FileNet
Team Collaboration Manager

Installation Guide

Release 3.5.0

August 2005

FileNet Corporation
3565 Harbor Boulevard
Costa Mesa, California 92626
800.FILENET (345.3638)
Outside the U.S., call:
1.714.327.3400
www.filenet.com

Notices

For notices regarding this documentation, refer to Help Directory > Notices in the FileNet P8 online documentation.

Typographical Conventions

This document uses the conventions in the following table to distinguish elements of text.

Convention	Usage
UPPERCASE	Environment variables, status codes, and utility names.
Bold	Paths and file names, program names, clickable user-interface elements (such as buttons), and selected terms such as command parameters or environment variables that require emphasis.
Italic	User-supplied variables and new terms introduced in text.
<*italic*>	User-supplied variables that replace everything between and including the angle bracket delimiters (< and >).
`Monospace`	Code samples, examples, display text, and error messages.

NOTE The following procedures contain pathnames for both UNIX and Windows. If there is no difference in directory structure, a forward slash (/) will be used to separate the elements of a pathname for both UNIX and Windows.

Table of Contents

Notices . . . 2

Typographical Conventions . . . 2

Table of Contents . . . 3

About this document . . . 5

Planning . . . 5
- TCM components . . . 5
- Auxiliary documentation . . . 6
- Installing TCM . . . 7
- Object Stores and Teamspaces . . . 7
- TCM roles and security . . . 8
- Security information required during the TCM installation . . . 8
- Authentication Considerations . . . 11
- Operating System and Application Server Considerations . . . 11
- FileNet P8 Platform Considerations . . . 12
- Collaboration Mail Server . . . 12
- Ports used by TCM . . . 13
- Network Considerations . . . 13
- Upgrade . . . 13
- TCM and high availability . . . 13

Prerequisite Tasks . . . 14
- Install TCM documentation . . . 15
- Prepare Process Engine for TCM . . . 18
- Configure Symmetric Encryption . . . 19

Installation Tasks . . . 23
- Install the Content Engine Integration . . . 24
- Install the TCM Application . . . 31
- Deploy the TCM Application . . . 40
- Deploy the TCM Application (JBoss/Tomcat) . . . 41
- Deploy the TCM Application (WebLogic) . . . 46
- Deploy the TCM Application (WebSphere) . . . 49
- Configure Workflow for TCM use . . . 53
- Install the Collaboration Engine . . . 59
- Install the Collaboration Mail Server . . . 64

Configuration/Startup Tasks . . . 69
- Install unlimited strength .jar files . . . 70
- (Optional) Manually Configure TCM . . . 71
- Start Team Collaboration Manager . . . 78
- (Optional) Setup TCM SSL security . . . 82

Software Reconfiguration and Removal Tasks 84

Appendixes 87

(HP-UX only) Enable Java Service Wrapper 88

FileNet TCM Port Numbers 90

Index 91

About this document

Every effort has been made to provide you with complete installation instructions. If information became available after the creation of the documentation CD from which you accessed this guide, we have provided an updated version of the guide on the FileNet CSS web site (http://www.css.filenet.com).

As a general rule, you should refer to the CSS web site to obtain the most current version of the installation guide.

Planning

The FileNet Team Collaboration Manager (TCM) Installation Guide describes the prerequisites for installing TCM, as well as the steps to install and configure TCM.

This section lists details that will help you prepare your environment for FileNet TCM. In many cases, the items you see listed will be links to more detailed information, which will help you plan a system roll out. Please review this information thoroughly before you start to set up FileNet TCM.

NOTES

- The TCM setup program does *not* install any of the core components of the FileNet P8 suite of products and requires that the three core components, namely Content Engine (CE), Process Engine (PE), and Application Engine (AE) must be installed and configured before starting the TCM installation. We strongly recommend that you install the FileNet P8 documentation also.
- The FileNet Team Collaboration Manager Installation Guide is intended for use by a FileNet Certified Professional (FCP) Technician or a Certified Technical Service Provider (TSP). To learn more about the FCP Certification program, please refer to the FileNet Worldwide Customer Support web site (http://www.css.filenet.com), Products > Services & Support. At least 10 working days prior to the installation, the FCP Technician or TSP must schedule the installation with the FileNet Upgrade/ Installation Assurance Team and access the team's latest list of current scheduling procedures, which is available at http://www.css.filenet.com/install.asp.

TCM components

You install TCM as a separate functional expansion of the FileNet P8 platform. TCM consists of the following components, which can be installed on a single server or distributed across servers:

- Collaboration documentation - integrates with the FileNet P8 platform documentation to provide specific information on the TCM features.
- TCM Application - installs the web-based user interface for TCM. The TCM Application is a web application that is deployed and run on an application server such as JBoss, WebLogic, or WebSphere.
- Collaboration Java API - provides complete access to the FileNet P8 Collaboration capabilities to developers for creating their own collaborative applications or for customizing the out-of-the-box TCM capabilities. The Collaboration Java API is installed with the TCM Application, but can also be installed separately.
- Collaboration Engine - handles all of the behind-the-scenes activities of the Collaboration application, such as maintaining access rights on documents and folders, and handling event notification emails.

- Collaboration Mail Server - provides email notification, and receipt of messages for archiving.

During the installation process you will also make updates to the:

- Content Engine to provide the ability to generate an object store that contains the necessary features to support the TCM environment.
- Process Engine region to provide workflow capabilities within TCM. The components required for this functionality are installed on the Application Engine.

In addition, the following components must exist in your environment:

- Corporate mail server – The Collaboration Mail Server handles mail sent in and out of TCM, but relies on an external corporate mail server for external email communications.
- An application server - The TCM Application runs on an application server such as WebSphere, WebLogic, or JBoss.
- FileNet P8 platform documentation – The documentation must be installed on an application server to enable context sensitive help from within the TCM application. This guide also extensively links to information on the FileNet P8 platform help site and PDFs.

Auxiliary documentation

Review the following documents found on the FileNet Worldwide Customer Support web site (http://www.css.filenet.com):

- FileNet TCM 3.5.0 Release Notes. This document provides details on new features, known issues, and resolved problems for the TCM product.
- FileNet P8 3.5.0 Platform Release Notes. This document provides details on new features, known issues, and resolved problems for the FileNet P8 Platform.
- FileNet P8 3.5.0 Platform Installation and Upgrade Guide. This document contains the installation instructions for the FileNet P8 platform, and is referenced from this document.
- FileNet P8 3.5.0 Hardware and Software Requirements. This document provides details for all FileNet P8 system components, as well as the minimum supported levels of third-party software components. The information throughout the FileNet TCM Installation Guide assumes you have met all applicable requirements listed in that document.
- FileNet P8 Platform user and group security help. For more information, go to *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Enterprise-wide Administration > Security > Users and groups. This help topic provides a complete list of the user and group roles, accounts, and responsibilities required to install, configure, and maintain a FileNet P8 system.
- FileNet P8 3.5.0 Platform Security Questionnaire. This document provides a list of security-related questions that, when answered for your site, can provide valuable feedback to the FileNet Upgrade/Installation Assurance Team that will install and deploy your FileNet P8 system.
- FileNet P8 Platform Shutdown and Startup documentation. For more information, go to *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Enterprise-wide Administration > Shutdown and Startup. This topic describes how to shut down and restart FileNet P8 Platform components and some functional expansions. Manual, command line, and some sample batch file procedures are provided.
- FileNet P8 3.5.0 Platform High Availability Technical Notice. This document provides details on how to set up your FileNet P8 system using clusters, farms, and other high-availability software and hardware.

- FileNet P8 Platform Troubleshooting Guide. This document provides troubleshooting information on all aspects of the product.

Installing TCM

Guidelines for distributing TCM components

The installation instructions provided in this guide explain how to install and configure the Team Collaboration Manager on separate servers. However, the TCM components can be collocated. There are no restrictions on which TCM components can be collocated. In addition, TCM components can also be collocated with other FileNet P8 components to optimize performance and system resources. For example, you can collocate the TCM Application with the Application Engine.

Using the custom installation option

If you plan to collocate TCM components on a server, select Custom in the setup screen of the TCM setup wizard to install multiple components simultaneously. The setup wizard merges the required screens; please refer to the individual installation instructions for each component for descriptions of the screens.

Installation Order

The TCM components should be installed, configured, and started in the order outlined in this guide.

Read the “Prerequisite Tasks” on page 14, “Installation Tasks” on page 23, and “Configuration/Startup Tasks” on page 69 to become familiar with the tasks you will perform when setting up your FileNet TCM software.

Configuration information

During the installation process you will be prompted for information. If you do not know the requested information, you can complete the installation process using the placeholder information that is displayed on the installation screens. After you have completed the installation process and gathered the required information, you can manually update the TCM configuration files with the information.

If your environment changes after the initial installation, (for example, if a new Content Engine is added) you can edit the TCM configuration files with updated information to enable TCM to continue functioning. For more information, see “(Optional) Manually Configure TCM” on page 71.

Object Stores and Teamspaces

A central concept to TCM is the teamspace. A teamspace is a work area that is accessible only to specific users who have been identified as members of a team or as a collaboration administrator. Each teamspace can contain documents, folders, workflows, polls, forums and discussions. The structure of a teamspace and its associated security and content are stored in an object store.

For more information, go to *Documentation for FileNet P8 Platform* help and navigate to Functional Expansions > Team Collaboration Manager > Concepts > Teamspaces.

Each TCM environment supports only one object store; however, the object store can support multiple teamspaces in addition to being used as a document content repository for other applications. To support the TCM functionality, several Collaboration “addOn” files must be added to the object store. Once an

object store has been configured with the Collaboration addOns, the object store is referred to as a Collaboration object store.

Any object store can become a Collaboration object store. When installing and configuring TCM, you can choose to create a new object store for use as the Collaboration object store or you can choose to update an existing object store. Becoming a Collaboration object store does not prevent an object store from supporting other FileNet P8 applications or from being used as a document management repository.

TCM roles and security

TCM uses the concept of security roles to control what a user can do within a teamspace. Within each teamspace, a user is assigned a specific role. That role determines what activities the user can participate in, and controls which objects they can create or modify. The definition of security roles can occur after TCM is installed.

For more information, go to *Documentation for FileNet P8 Platform* help and navigate to Functional Expansions > Team Collaboration Manager > Security.

Security information required during the TCM installation

During the installation there are two types of security information you must be aware of:

- The user privileges needed to run a specific portion of the installation.
- The user information that must be supplied during the installation process.

You do not have to create any new users to install and run TCM, all assignments can be performed with existing users. After installation, the user assignments can be updated.

User Privileges required to complete the TCM Installation

The following table identifies the user privileges required to complete the TCM installation.

TCM Component	User Privileges Required
TCM Documentation	Read and write access to the folder where the FileNet P8 platform documentation is installed. Application server rights to deploy the documentation.
Content Engine Integration installation	Local system administrator. If using a Windows LDAP server, GCD Administrator. If a non-Windows LDAP server is in use, the installer will prompt for GCD account information.
Collaboration Object Store	For a new object store: Content Engine Administrator. For an existing object store: Object Store administrator.
TCM Application installation	Read and write access to the folder where the TCM Application will be installed. Application server administrator rights to deploy the TCM Application.
Workflow Integration	Process Engine Administrator rights to stop and start the Process Services on the Process Engine. Workplace Site Administrator rights with the ability to: • Access the Process Administrator in Workplace. • Add a folder to the Collaboration object store. • Add a workflow via the Browse page. • Transfer a workflow. • Create workflow subscriptions via Workplace.
Collaboration Engine	Read and write access to the installation directory. Root user rights to configure the daemon to start automatically on reboot.
Collaboration Mail Server	Read and write access to the installation directory. Root user rights to configure the daemon to start automatically on reboot.

User information required during the installation process

The following table identifies where in the installation process you will be prompted for user information.

TCM Component	Information Requested	Minimum Requirements
Content Engine		
Security Script wizard	Collaboration Administrators	Include object store and Process Engine administrators.
	Collaboration Users	Include any users that will be customizing TCM.
Collaboration Enterprise Security Definitions.xml	Sysadmin-Rights access role	Provide a user or group that has object store and Process Engine administrator rights. You will also need to supply the username and password for one these accounts during other parts of the installation process.
	Required teamspace template security	Initially accept the default of all authenticated users.
Workflow Integration		
	JAAS Credentials	The account must have the following rights: • Object store administrator. • Process Engine administrator.
	Collaboration Queue security rights	Collaboration Administrator.
	Component Manager	Process Engine administrator.
Collaboration Engine	Content Engine username and password	Provide a Content Engine Administrator account that was also identified as a SysAdmin user in the Collaboration Enterprise Security Definitions.xml file.
Collaboration Mail Server	Content Engine username and password	Provide a Content Engine Administrator account that was also identified as a SysAdmin user in the Collaboration Enterprise Security Definitions.xml file.

Authentication Considerations

To secure user information as it is passed between components in the TCM environment, you are required to use:

- User tokens

  This authentication requires that a copy of the UTCryptoKeyFile.properties file that exists on the Application Engine be copied to the TCM application server, Collaboration Engine, and the Collaboration Mail server.

- Encryption between the Collaboration Engine, Collaboration Mail Server, and TCM application server.

  A TCMCryptoKeyFile.properties file is generated by the TCM Application installation and must then be copied to the Collaboration Engine and Collaboration Mail Server.

Additionally, you can also choose to use Symmetric encryption between the Application Engine and the Content Engine, and between the TCM application server and the Content Engine. To enable this layer of symmetric encryption you must:

1. Configure Workplace to use Symmetric Encryption.
2. Copy the CryptoKeyFile.properties file generated by the Application Engine installation from the Application Engine to the TCM application server, Collaboration Engine, and Collaboration Mail Server.

For more information on symmetric encryption and user tokens, refer to the FileNet P8 online help. For more information on how to configure TCM to support the authentication methods mentioned above, see “Configure Symmetric Encryption” on page 19

Operating System and Application Server Considerations

There are some specific steps that must be taken if your installation includes any of the following:

- Installing the Collaboration Engine or the Collaboration Mail Server on an HP-UX server.
- Installing the TCM Application on a Linux server or if you are using a JBoss application server.

Enable Java Service Wrapper on HP-UX

If you are installing the Collaboration Engine or Collaboration Mail Server on an HP-UX server, you must enable the Java Service Wrapper by:

- Installing Binutils 2.15 and GCC 3.4.3.
- Creating a symbolic link between the directory that contains the libgcc_s.sl file—from the GNU Compiler Collection (GCC)—and the /sww/lib directory.

For more information, see “(HP-UX only) Enable Java Service Wrapper” on page 88.

Linux Operating system considerations

To install the TCM Application on Linux, several legacy libraries are required. Add the compat-libstdc++-7.3-2.96.122.i386.RPM located on Disc 3 of the Red Hat AS 3.0 install media to your installation.

JBoss Application Server considerations

If you plan to collocate the TCM Application with another application such as Workplace, you must set the JBoss web loader attribute to false.

For more information, see "To collocate the TCM Application with other applications on JBoss" on page 45.

FileNet P8 Platform Considerations

User name display setting

In TCM user names can be displayed using either short format (user id) or long format (display name). This setting is originally applied when you install the FileNet P8 Platform. Changes made to this setting apply only to Teamspaces and other objects created after the change.

For more information on how to change the user name display setting, go to the *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Enterprise-wide Administration > Process Task Manager > Process Engine > Process Service > Configure the Process Service > Configure the LDAP connection > Advanced properties.

Also see To create or join a FileNet P8 domain on pages 76 or 91 in the *FileNet P8 3.5.0 Platform Installation and Upgrade Guide*.

Collaboration Mail Server

The collaboration mail server is used to archive mail that is sent explicitly to a teamspace. The archived mail is stored in the Collaboration object store. In order for the Collaboration Mail Server to receive email, it must be recognized by the corporate mail server.

If the teamspace will receive email from internal users only and if the corporate mail server and the Collaboration mail server are in the same DNS domain, no additional configuration steps are needed. However, if email will be sent to the teamspace from outside of the corporate network, external mail servers must be able to resolve the Collaboration mail server DNS name. Typically, this is done by adding a mail exchange (MX) record to the corporate DNS server.

For example, if the DNS name for the:

- Collaboration Mail Server is `MyCollabMail.filenet.com`.
- Corporate mail server is `CorporateMail.filenet.com`.

Add an MX record of format similar to the following to your DNS server:

```
MyCollabMail.filenet.com IN MX 10 CorporateMail.filenet.com
```

The Collaboration Mail Server must be configured to use port 25.

For more information, refer to your organization's documentation for DNS configuration and mail servers.

The Java Apache Mail Enterprise Server provides the foundation for the email archive capability. For more information about the Java Apache Mail Enterprise Server, see http://james.apache.org/. If your environment does not have access to a corporate mail server, you can use the Java Apache Mail Enterprise Server to provide general email access for the FileNet P8 environment.

Required Collaboration Mail Server ports

TCM requires that the Collaboration Mail Server uses ports 25 and 110. If you are experiencing communication problems verify that this port is available and is not being used by other applications. For example

- On Windows, if the server on which you are the installing Collaboration Mail Server is running IIS, ensure that the Simple Mail Transport Protocol (SMTP) service is stopped and disabled, or that it is configured to use a port other than 25.
- On Unix, if the server on which you are installing the Collaboration Mail Server is using the sendmail daemon, ensure that the sendmail daemon is stopped and will not restart after a reboot, or configure the daemon to use a different port.

For more information see "SMTP port" on page 67 and "FileNet TCM Port Numbers" on page 90.

Ports used by TCM

Several port numbers are required by FileNet P8 components. For a composite list, see "FileNet TCM Port Numbers" on page 90 and *FileNet Port Numbers* in the FileNet P8 3.5.0 Platform Installation and Upgrade Guide.

Network Considerations

Verify that you can access all other FileNet P8 servers and TCM servers from the servers on which you will be installing the TCM components.

Upgrade

Upgrade from TCM 3.0.0 to TCM 3.5.0 is not supported. If TCM 3.0.0 is currently installed, you must:

- Uninstall all the TCM software prior to running the TCM 3.5.0 installation program.
- Designate a new object store for use with TCM 3.5.0 or remove all TCM objects from the existing Collaboration object store.

TCM and high availability

If you plan to set up a web farm or clustered environment, in addition to these instructions read and follow the instructions in FileNet P8 Platform 3.5.0 High Availability Technical Notice available from the FileNet Worldwide Customer Support web site (http://www.css.filenet.com).

Prerequisite Tasks

To set up and configure prerequisite software for TCM components

1. Install TCM documentation. Do Task 1 on page 15.
2. Prepare Process Engine for TCM. Do Task 2 on page 18.
3. Configure Symmetric Encryption. Do Task 3 on page 19.

Task 1: Install TCM documentation

CAUTION NOTES

- You must install the documentation on an application server if you intend to configure it for online help functionality in the FileNet P8 software.
- The application server must be Java-enabled to use the help's Search functionality (e.g., IBM WebSphere or BEA WebLogic).
- Users must have Java Script support enabled on their web browsers to use some of the features in the help (such as Search and the tables of content). The help files are contained in a folder called "ecm_help."
- Updates to the documentation are provided periodically. Please check the FileNet Worldwide Customer Support web site for updates.

To refresh the documentation on the application server

1. Ensure that you have the latest version of the FileNet P8 Platform 3.5.0 documentation installed on your application server. See the FileNet P8 3.5.0 Platform Installation and Upgrade Guide for more information.
2. Refer to your application server documentation. Complete any initial steps that might be necessary before updating the ecm_help files. For example, on a WebLogic server, you must undeploy the ecm_help application.
3. Copy the **ecm_help** folder on the FileNet TCM Documentation CD to the application server where the FileNet P8 documentation is installed.

   For example, on a WebLogic 7.x server running on Windows:

   C:\bea\user_projects\<*myDomain*>\ecm_help.

   ### NOTES

   - If you downloaded updated TCM documentation from the FileNet Worldwide Customer Support web site, install the updated version instead of the version on the TCM CD. Note, however, that the TCM documentation must be installed *after* you install version 3.5.0 of the FileNet P8 Platform documentation.
   - The FileNet P8 Platform help includes placeholder files for functional expansions that are released on different schedules. As a result, when you install the documentation for the various components in the prescribed order, you might see warning messages about overwriting newer files and folders. Ignore the messages and allow the overwrites to occur. By doing so the actual functional expansion help files will replace the placeholder files.
   - If you later install a version of the FileNet P8 Platform documentation that is newer than **3.5.0**, you must refresh the TCM documentation on the application server.

4. Update the installation guide PDFs.

   After you copy the TCM documentation, download and replace the installation PDF files under the Installation directory with the latest files from FileNet Worldwide Customer Support web site. These files are released independently of the FileNet P8 Platform 3.5.0 documentation and FileNet TCM Documentation; the installation files on the CSS site might be more current than the ones included in the documentation builds.

On the FileNet Worldwide Customer Support web site, navigate to **Product Tech Info > Products >**...

Business Process Manager (BPM) > Product Documentation > 3.5.0x Documentation > FileNet P8 Platform 3.5.0 Installation and Upgrade Guide.

and

Team Collaboration Manager (TCM) > Product Documentation > 3.5.0x Documentation > FileNet Team Collaboration Manager 3.5.0 Installation Guide.

5. Refer to your application server documentation. Complete any additional steps that might be necessary after updating the ecm_help files.

   For example, on a WebLogic server, you must redeploy the ecm_help application.

Update the Search Index

Once you've installed the TCM help, you should update the search index files. Unless you complete this step, the documentation search function will not find the TCM content.

NOTES

- If you're installing more than one FileNet P8 functional expansion, update the search index *after* all the functional expansions have been installed. If you install another functional expansion later, update the search index again by following the procedure below.
- When you update the Search Help index, a backup of the files in the existing **.../ecm_help/search/index/core** subdirectory will be copied automatically to an **.../ecm_help/search/index/indexOld** subdirectory. To return to the previous indexed state, reapply these backed-up files to the **core** subdirectory (after first removing the new files created there).
- If you have already deployed or installed the FileNet P8 help as a web application, undeploy or uninstall it before proceeding.

  NOTE For WebSphere you must deploy the original ecm_help.war file, execute it, and then stop WebSphere. Next, copy the files to the deployed location, update the search, and then restart WebSphere.

To update the Help Search index

1. Ensure that you have copied the FileNet P8 Platform help and all your functional expansions to a designated application server. See Step 1 and Step 3 on page 15.
2. Edit the search-indexing script file that launches the Java-based indexer:

   ...\ecm_help\search\indexFiles.bat (Windows)

   .../ecm_help/search/indexFiles.sh (UNIX)
3. Modify the JAVA_HOME variable in the script file with the path to your JRE installation (version 1.3 or later).

   The defaults are:

   ```
   SET JAVA_HOME=c:/j2sdk1.4.2 (Windows)
   JAVA_HOME="/usr/java/j2sdk1.4.1_02" (UNIX)
   ```
4. Save your changes.
5. Run the updated search-indexing script file.

To deploy and verify the documentation web site

1. Deploy or install the copied FileNet P8 documentation as a web application. Use the appropriate instructions provided with your application server.
2. Verify that the application server and the new **ecm_help** documentation web site are running, as follows:

   a. From your web browser, access the **_start_here.htm** page in the top-level **ecm_help** directory.

   b. The documentation Help Directory should open.

   c. Click the **Search** link on the Help Directory toolbar. The documentation Search page should open.

   NOTE Use the following URL to configure the online help location for the various FileNet P8 components either while running Setup programs or later via site preferences settings:

   `http://<docserver>:<port#>/<ecm_help>/`

   where:

   <*docserver*> is the name of the Java web server.

   <*port#*> is the port number.

   <*ecm_help*> is the root folder of the documentation website. You can use multi-part root folders (e.g., / docs/ ecm_help) if your application server supports them.

Task 2: Prepare Process Engine for TCM

TCM relies on the email notification mechanism provided by the Process Engine. If you haven't configured email notification as part of the FileNet P8 Platform installation, follow the procedure below.

To configure the Process Engine email notification

Complete this task on the Process Engine using a Process Administrator account.

1. Launch the Process Task Manager on the Process Engine.
2. If any routers are running on this server, stop them using the appropriate tool: Process Services Administrator for Content Engine routers, and the Process Task Manager for Process Engine or Application Engine routers.
3. Stop the PPM.
4. Stop the Process Service.
5. Select **Process Service**.
6. In the right pane, select the **Notification** tab.
7. Ensure that a valid SMTP Host has been configured.

   For more information on completing this screen, refer to the *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Enterprise-wide Administration > Process Task Manager > Process Engine > Process Service > Configure the Process Service > Email notification.
8. After all the parameters have been entered, click **Apply**.
9. Restart the Process Service.
10. Restart the PPM.
11. Restart the routers.

Task 3: Configure Symmetric Encryption

The use of symmetric encryption between the TCM servers and the FileNet P8 servers requires cryptographic keys. These are stored in three configuration files on the TCM servers.

Team Collaboration Manager uses three types of cryptographic keys:

- (Optional) User Credentials encryption, stored in the **CryptoKeyFile.properties** file.

  These cryptographic keys are used to provide symmetric encryption when signing in to TCM. Encryption protects user credentials passed between the TCM servers and the Content Engine. The Application Engine installer creates this file, and you must copy it to the TCM servers.

- (Required) User Token cryptographic keys, stored in the **UTCryptoKeyFile.properties** file.

  All FileNet P8 applications must use the same User Token cryptographic keys. The Application Engine installer creates this file, and you must copy it to the TCM servers.

  For information, go to the *Documentation for FileNet P8 Platform* help and navigate to Developer Help > Workplace Integration and Customization Introduction > User Tokens > Configuring Applications to Use Tokens.

- (Required) TCM cryptographic keys, stored in the **TCMCryptoKeyFile.properties** file.

  The installer creates this file on the TCM Application server.

  This file is used to encrypt:

  – (TCM Application) TCM meeting vendor credentials.

  – (Collaboration Engine server) The Collaboration Engine administrative user's password in the collabEngineConfig.properties file.

  – (Collaboration Mail Server) The Collaboration Mail Server administrative user's password in the config.xml file.

NOTE To use symmetric encryption with your TCM system you must copy the files listed above to the correct directories on your TCM servers, see "Copy the cryptographic key files." on page 20.

To configure symmetric encryption

1. Create the folder structure on your TCM servers.

   On each TCM server (TCM Application, Collaboration Engine, Collaboration Mail Server) do the following.

   a. Log in to the server.

   b. Create the folder structure where you plan to store your cryptographic key files.

      The default location is:

      ***<TCM_install_path>*/FileNet/Authentication**

      Where ***<TCM_install_path>*** is the directory you select to have the installer add the TCM source files, for example, see "Directory Name" on page 32.

CAUTION

If you select to create a folder structure other than the default, make sure you browse for and select the files when you install TCM; if you select the default CryptoKeyFile.properties location value in the installer, the TCM setup will not be correctly configured.

If you collocate any of the TCM components with the Content Engine, you may want to use the folder where Content Engine stores the CryptoKeyFile.properties file for your cryptographic key files rather than the default location above:

Content Engine Authentication folder:

<*CE_install_path*>\FileNet\Content Engine\JavaAPIListener\Authentication

2. Copy the cryptographic key files.

   a. (Optional) Copy the User Credentials cryptographic key file.

   If you selected symmetric encryption during Application Engine setup, the setup program generated an encryption key file called **CryptoKeyFile.properties** in the following default location on the Application Engine server:

   <*AE_install_path*>/FileNet/Authentication

   Copy this file to the newly created Authentication folder on your servers.

   NOTE Instead of using the Application Engine cryptographic keys you can create TCM specific cryptographic keys, see "(Optional) Manually create the CryptoKeyFile.properties file for TCM" on page 21.

   b. Copy the User Token cryptographic key file.

   During Application Engine setup, the setup program generated an encryption key file called **UTCryptoKeyFile.properties** in the following default location on the Application Engine server:

   <*AE_install_path*>/FileNet/Authentication

   Copy this file to the newly created Authentication folder on your servers.

   c. Copy the TCM cryptographic key file.

   NOTE Perform this step *after* you have installed the TCM Application. For more information, see "Install the TCM Application" on page 31. You will be directed back to this step from that procedure.

   During the TCM Application installation the installer generates an encryption key file called **TCMCryptoKeyFile.properties** in the following default location (or in a location of your choice) on the TCM Application server:

   <*TCM_install_path*>/FileNet/Authentication

   Copy this file to the newly created Authentication folder on your Collaboration Engine and Collaboration Mail Server servers.

   CAUTION As the installer uses this cryptographic key to encrypt the passwords entered during installation this file *must* exist on the Collaboration Engine server and Collaboration Mail Server *before* you run the installer on these servers.

3. (Application servers using JRE1.3 only) On the TCM Application server, modify the java.security file.

CAUTION If the TCM Application is collocated with AE you have already added com.sun.crypto.provider.SunJCE to the configuration. You should not add it a second time.

a. Use a text editor to open the java.security file used by WebLogic and typically stored in the following location:

   ***<JRE_dir>*/jre/lib/security**

b. Add the following line, specifying a preference order that does not conflict with an existing entry:

   ```
   security.provider.n=com.sun.crypto.provider.SunJCE
   ```

   where n is the preference order value.

   For example, in the example below, you can specify a preference order value of 3 or higher. The following is an example from the JRE 1.3 java.security file:

   ```
   #
   # List of providers and their preference orders (see above):
   #
   security.provider.1=sun.security.provider.Sun
   security.provider.2=com.sun.rsajca.Provider
   security.provider.3=com.sun.crypto.provider.SunJCE
   ```

c. Save and close the java.security file.

(Optional) Manually create the CryptoKeyFile.properties file for TCM

If user credentials symmetric encryption is not enabled on the Application Engine--or if you want unique cryptographic keys for TCM--you can manually create a unique CryptoKeyFile.properties file for TCM.

Depending on if there is an existing CryptoKeyFile.properties file on the Content Engine or not, you can either copy this file to the Authentication folder on that server or edit the existing file and add the new keys.

NOTE This procedure only pertains to the CryptoKeyFile.properties and the cryptographic keys stored in this file. For User Token encryption and Collaboration Web Application security you should always use the UTCryptoKeyFile.properties file created by the Application Engine installer, and the TCMCryptoKeyFile.properties created by the TCM Application installer respectively.

To manually create the CryptoKeyFile.properties file:

1. Create cryptographic keys for TCM.

   The TCM installer does not create the user credentials cryptographic keys. To create additional keys, use the Content Java API class, **MakeCryptoKeys**.

   For information, go to the *Documentation for FileNet P8 Platform* help and navigate to Developer Help > Content Java API > Security > Working with Security > Creating Cryptographic Keys for Symmetric Encryption.

2. Add the newly created cryptographic keys to the Content Engine.

   Depending on your setup, use either of the following two methods.

   - If symmetric encryption is not used by the Application Engine and no CryptoKeyFile.properties file exists on the Content Engine server:

     i. Copy the **CryptoKeyFile.properties** file to the following folder on the Content Engine(s):

        C:\Program Files\FileNet\Content Engine\JavaAPIListener\Authentication

NOTES

If the **Authentication** folder listed in the path above doesn't exist on the Content Engine server, create it.

We recommend copying the file over a secure link.

ii. If you copy the file to a location on the Content Engine other than the one listed above.

Modify the Content Engine's registry to match the new name or path; the Content Engine installation adds the registry key **CryptoKeyFile**, with a value that defines the name of the file and the default path.

CAUTION Back up your registry before making any changes.

To change the value, open the registry and navigate to:

HKEY_LOCAL_MACHINE\SOFTWARE\FileNet\ECM\Content Engine\JavaAPIListener\Authentication

Change the data value of CryptoKeyFile to the new path and filename.

- If symmetric encryption is used by the Application Engine and a CryptoKeyFile.properties file exists on the Content Engine.

  i. (On the Content Engine) Open up the existing **CryptoKeyFile.properties** file for editing:

  C:\Program Files\FileNet\Content Engine\JavaAPIListener\Authentication\CryptoKeyFile.properties

  ii. Append the contents of the newly created **CryptoKeyFile.properties** file to the content of the Content Engine file.

3. Copy the newly created CryptoKeyFile.properties file to the Authentication folder on your TCM servers, see "(Optional) Copy the User Credentials cryptographic key file." on page 20.

Installation Tasks

To install the TCM components

1. Install the Content Engine Integration. Do Task 4 on page 24.
2. Install the TCM Application. Do Task 5 on page 31.
3. Deploy the TCM Application.
   - Deploy the TCM Application (JBoss/Tomcat). Do Task 6a on page 41.
   - Deploy the TCM Application (WebLogic). Do Task 6b on page 46.
   - Deploy the TCM Application (WebSphere). Do Task 6c on page 49.
4. Configure Workflow for TCM use. Do Task 7 on page 53.
5. Install the Collaboration Engine. Do Task 8 on page 59.
6. Install the Collaboration Mail Server. Do Task 9 on page 64.

Task 4: Install the Content Engine Integration

In order for Team Collaboration Manager to work with a FileNet P8 system, you must update the Content Engine for TCM use.

CAUTION

Before you run the TCM installer to add the Content Engine Integration on a Content Engine for a second or consecutive time, you must first manually stop and restart the three Content Engine services: Content Engine Content Cache Service, Content Engine File Store Service, and Content Engine Object Store Service. For more information on how to stop and restart a Windows service, see Windows documentation.

To check GCD permissions

Complete the following steps on the Content Engine using the FileNet Enterprise Manager.

1. On the Content Engine, launch FileNet Enterprise Manager.
2. Right-click the **Enterprise Manager** node and select **Properties**.
3. Select the **Security** tab.
4. Verify that the user you are currently accessing the FileNet Enterprise Manager with has a Security level of “Full Control” and that it applies to “This object and all its children.”

   If the current user account does not have the required privileges, identify a user that does. You will need to supply information about this account during the Content Engine Integration Installation.
5. Close the Enterprise Manager

To install the Content Engine Integration

1. Log in to the Content Engine server as a local administrator. If possible, this should also be a user with Content Engine GCD Administrator privileges.

   If your FileNet P8 environment uses a directory service other than Active Directory, log in as a local administrator. You will be prompted for the GCD Administrator user name and password when running the installer, see “GCD Administrator user information” on page 25.
2. Verify that the Content Engine Object Store and Content Engine File Store services are running.
   a. Open **Start > Settings > Control Panel > Administrative Tools > Services**.
   b. Locate the Content Engine Object Store and Content Engine File Store services.
   c. Verify that their Status is **Started**.
3. Start the TCM Setup wizard:

   Insert the Windows TCM CD. If Autorun is enabled, the setup program will start. Otherwise, navigate to the **CD-ROM** drive and execute:

   Win32_filenet_TCM_setup.exe.
4. Complete the Setup screens as follows:

In this screen...	Perform this action...
License Agreement	Review and accept the FileNet End User Software License Agreement, and then click **Next**.

In this screen...	Perform this action...
Directory Name	For the Directory Name field, enter or browse to the location where you want to install the TCM software (***<TCM_install_path>***), or accept the default location: **C:\Program Files** Click **Next**. The installation program creates a **FileNet** directory at the selected location, and installs the TCM software in this directory: ***<TCM_install_path>*/FileNet/Collaboration**
Choose the Setup Type	Select **Content Engine Integration**, and click **Next**.
Verify Upgrade **NOTE** This screen *only* appears if you try to install TCM on a system that has a previous version of TCM installed.	The setup wizard detects previous version of TCM is installed on your system. Before you continue with the installation you must first uninstall the TCM component(s). For uninstallation information, see FileNet Team Collaboration Manager Installation Guide Release 3.0.0, Software Reconfiguration and Removal Tasks.
Ready to Install	Read the summary and click **Next** to install the Content Engine Integration components.
GCD Administrator user information	(Non-Active Directory FileNet P8 environments only) Provide the GCD Administrator user information. a. Enter the GCD Administrator ID, and click **OK**. b. Enter the GCD Administrator Password, and click **OK**.
Completing the setup wizard	Click **Finish** to complete the installation.

5. Verify that the installation was successful.

   The following file should contain no errors.

   ***<TCM_install_path>*/FileNet/TCM_install_log_35.txt**

6. Configure an object store for use with TCM.

   To use an object store with TCM you must first configure it. You can either create an object store for TCM use, adding the Team Collaboration Manager add-ons at the end of the process, or configure an existing object store for TCM use.

   - Create an object store for TCM use.

     To create an object store, follow the instructions in the FileNet P8 3.5.0 Platform Installation and Upgrade Guide, Task 10: Create an object store and verify the Content Engine installation.

     i. Do Steps 1 through 7 to input the information required to create the object store.

     CAUTION Do *not* click Finish to create the object store.

ii. In the final screen of the Object Store Wizard, click **Advanced** to open the Auto Install Components dialog.

iii. Check the three components listed below, and click **OK**.

- TeamCollaborationManagerAddOn
- TeamCollaborationManagerAddOn2
- TeamCollaborationManagerAddOn3

iv. Click **Finish** to create the Collaboration Object Store.

v. Click **OK** to exit the wizard.

- Configure an existing object store for TCM use.

  If you plan to use an existing object store with TCM you must install the Team Collaboration Manager addons using FileNet Enterprise Manager.

  i. On the Content Engine, launch the FileNet Enterprise Manager.

  ii. Right-click the object store you want to configure for TCM use, and select **All Tasks > Install AddOn**.

  iii. Check the three components listed below, and click **Install**.

  - TeamCollaborationManagerAddOn
  - TeamCollaborationManagerAddOn2
  - TeamCollaborationManagerAddOn3

  iv. In the AddOn Installation Status window, click **OK**.

  v. Right-click the object store, and select **Refresh**.

7. Configure Collaboration Object Store security

   After configuring the Collaboration object store, you must modify the security settings of several TCM-specific folders as follows:

   a. Launch FileNet Enterprise Manager.

   b. Right-click the Collaboration object store you configured in Step 6 on page 25.

   c. Select **All Tasks > Run Security Script Wizard**.

   d. On the Welcome screen, click **Next**.

   e. On the Select security script information file screen, click **Browse...**

   f. Browse for the **Content Engine** directory.

      Default:

      C:\Program Files\FileNet\Content Engine.

   g. Select the **CollaborationImportSecurity.xml** file, and click **Open**.

   h. Click **Next**.

   i. Set Collaboration Administrators.

      Add the users and groups that you want to designate as Collaboration Administrators.

j. Set Collaboration Users.

Add the users and groups that you want to designate as Collaboration Users.

k. Click **Finish** to complete the configuration.

l. On the verification screen, click **OK** to exit the wizard.

If, at a later date, you need to add additional users as Collaboration Administrators or Collaboration Users, rerun the Security Script Wizard.

8. Configure Full Text Indexing on the Collaboration object store.

NOTE To configure Full Text Indexing the object store must have at least one File Store.

a. Right click on the Collaboration object store and select **All Tasks > Configure Full Text Indexing**.

b. From the **Task Menu**, select **Create Filestore Indexes**.

c. Create at least two indexes, and select the appropriate language for your locale.

d. Click **Create Indexes**, then click **Close**.

e. From the **Task Menu**, select **Create Database Indexes**.

f. Select at least two indexes.

g. Click **Create Indexes**, then click **Close**.

h. From the Task Menu, select **Property Level Indexing**.

i. In the tree view,

i. Expand **Class Definitions > Document > Indexable Properties**.

ii. Index **Document Title**.

iii. Expand **Class Definitions > Document > Subclasses > Collaboration Document > Subclasses > Collaboration Meeting Proxy Document > Indexable Properties**.

iv. Index **Agenda**.

v. Expand **Class Definitions > Document > Subclasses > Collaboration Document > Subclasses > Collaboration Teamspace Proxy Document > Indexable Properties**.

vi. Index **Collaboration Description**.

j. Click **Apply Changes**, then click **Close**.

k. Click **Yes** when prompted to index properties now; click **OK** when informed that the indexing will occur as a background task, then click **Close**.

General information about content-based retrieval can be found in *Documentation for FileNet P8 Platform* help; navigate to FileNet P8 Administration > Content Engine Administration > Content-based retrieval > How to... > Prepare for CBR.

9. Update the Collaboration Enterprise Security Definitions.xml file to designate a user or group to be associated with the SysAdmin role.

a. Using FileNet Enterprise Manager, navigate to **Root Folder > Collaboration Store** in the Collaboration object store.

b. Check out the Collaboration Enterprise Security Definitions.xml file by right-clicking the document, and selecting **Exclusive Check Out**.

c. Save the file to the local machine.

d. Open the file for editing using a toll such as Notepad.

Initially the file looks as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<collaboration-enterprise-security>
    <required-teamspace-security>
        <enterprise-subject>
        <name>Administrator</name>
        <type>user</type>
        <accessalias>sysadmin-rights</accessalias>
        </enterprise-subject>
    </required-teamspace-security>
    <required-teamspace-template-security>
        <enterprise-subject>
        <name>#AUTHENTICATED-USERS</name>
        <type>group</type>
        <accessalias>view-rights</accessalias>
        </enterprise-subject>
    </required-teamspace-template-security>
</collaboration-enterprise-security>
```

e. Update the user information in the <required-teamspace-security> area (shown in italics) to provide the fully-qualified user name of an account or group that is defined as a Collaboration Administrator and that is an Object Store and Process Engine administrator.

If you supply a group name, then update the <type> to Group.

When installing the Collaboration Engine and Collaboration Mail Server, you will be prompted for the username and password of an account that you designate as being associated with the SysAdmin role.

Format examples for fully-qualified names:

- Novell eDirectory: cn=Administrator,ou=Engineering,dc=company,o=novell
- SunOne LDAP: uid=Administrator,ou=Engineering,dc=server,dc=company,dc=com
- Windows LDAP: Administrator@domainname.company.com

For example, to update the file such that the group CE Admins@filenet.com is assigned the SysAdmin role, change the Enterprise Security Definitions.xml file to the following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<collaboration-enterprise-security>
    <required-teamspace-security>
        <enterprise-subject>
        <name>CE Admins@filenet.com</name>
        <type>group</type>
        <accessalias>sysadmin-rights</accessalias>
        </enterprise-subject>
    </required-teamspace-security>
    <required-teamspace-template-security>
        <enterprise-subject>
        <name>#AUTHENTICATED-USERS</name>
        <type>group</type>
        <accessalias>view-rights</accessalias>
        </enterprise-subject>
    </required-teamspace-template-security>
</collaboration-enterprise-security>
```

f. (Optional) Provide information about other access roles or about the users who should have rights to use the TCM templates.

These additional refinements can be made at any time and do not need to be made during the initial installation and configuration of TCM.

For more information on the access roles and the use of the TCM templates, refer to the TCM online help.

g. Save your changes.

h. Check the document back in as a major version.

10. Update the Collaboration Applications.xml file.

NOTE This file can be updated after the other components of TCM are installed.

a. Using FileNet Enterprise Manager navigate to the **Root Folder > Collaboration Store** folder.

b. Check out the Collaboration Applications.xml file by right-clicking the document and selecting **Exclusive Check Out**.

c. Save the file to the local machine.

d. Open the file for editing using a tool such as Notepad.

e. The following table indicates the changes that need to be made to this file. Search on the word “example” to find all the entries that need to be edited.

Item to be replaced	Change to be made	Number of Occurrences	Notes
Clbmail.example.com	Collaboration mail server DNS name.	1	The fully-qualified DNS name of the server on which the TCM Collaboration Mail Server will be installed.
Example.com	The corporate mail domain	2	The domain name of the corporate mail server.
www.example.com:8080	The internet domain and port of the TCM application	5	Update the domain and the port.Do not type Http:// at the start of the entry.
Secure.example.com:9090	The internet domain and port of the secure TCM server	2	Update the domain and the port.Do not type Https:// at the start of the entry. If you are not using SSL with your environment, leave the default values in place.
Example/timezone	The time zone for the Collaboration mail server.	1	Use a standard abbreviation such as PST, or provide the Country/Major City; for example America/Los Angeles.

f. Save your changes.

g. Check in the document as a major version.

Task 5: Install the TCM Application

This task includes TCM Application installation instructions for all supported application servers, for UNIX and Windows platforms.

CAUTION

(Linux only) To install the TCM Application on Linux, several legacy libraries are required. Add the compat-libstdc++-7.3-2.96.122.i386.RPM located on Disc 3 of the Red Hat AS 3.0 install media to your installation.

(HP-UX only) Enable the Java Service Wrapper prior to installing the TCM application. For more information, refer to "(HP-UX only) Enable Java Service Wrapper" on page 88.

To install the TCM Application

1. Log on to the application server:

   UNIX - logon as a user with *write* access to the **/bin** directory and *read*, *write*, and *execute* access to the directory where you plan to install Application Engine.

   Windows - log on as a member of the local Administrators group or a user with equivalent permissions.

2. Start the TCM Setup wizard:

   AIX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **AIX_filenet_TCM_setup.bin**.

   HP-UX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **HP11_filenet_TCM_setup.bin**.

   Linux - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **Linux_filenet_TCM_setup.bin**.

   Solaris - Insert and mount the TCM CD. Navigate to **/cdrom/cdrom0/** and execute **Solaris_filenet_TCM_setup.bin**.

   Windows - Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, navigate to the **CD-ROM** drive and execute **Win32_filenet_TCM_setup.exe**.

3. Complete the Setup screens as follows:

In this screen...	Perform this action...
License Agreement	Review and accept the FileNet End User Software License Agreement, and then click **Next**.
Directory Name	For the Directory Name field, enter or browse to the location where you want to install the TCM software (***<TCM_install_path>***), or accept the default location: UNIX - **/opt** Windows - **C:\Program Files** Click **Next**. The installation program creates a **FileNet** directory at the selected location, and installs the TCM software in this directory: ***<TCM_install_path>*/FileNet/Collaboration**
Choose the Setup Type	Select **Web Application**, and click **Next**. **NOTE** Installing the Web Application will also install the Collaboration Java API. To install the Collaboration Java API only, use the **Custom** installation option.
Choose an application server	Choose the appropriate application server for your installation. Click **Next**.
Content Engine Java API Configuration	Configure the Content Engine Java API. • Content Engine server name – Enter the Content Engine server's full machine name or IP address. • Content Engine server port – Enter the port number for the Content Engine's listening port. (Default: 8080) Click **Next**.

In this screen...	Perform this action...
Application Engine User Security	This screen lets you set the path to the folder that holds the CryptoKeyFile.properties file. This file holds the cryptographic keys that secure the communication between TCM and the Content Engine. Use the same encryption configuration as Workplace. If Workplace is using symmetric encryption, enable symmetric encryption for TCM. Otherwise, use the Clear setting. a. Select credentials protection, the encryption method to protect stored logon credentials passed between TCM and the Content Engine: • Clear - encodes credentials using base 64 encoding. • Symmetric - uses cryptographic keys to encrypt and decrypt user credentials. b. (If you selected Symmetric encryption) Browse for an existing CryptoKeyFile.properties file or accept the default path. Default: **<TCM_install_path>/FileNet/Authentication/CryptoKeyFile.properties** If you are installing the TCM application on the same server as Workplace, the file is located as follows: ***<AE_install_path>*/FileNet/Authentication/CryptoKeyFile.properties** **CAUTION** If you are using JDK 1.4 and use maximum strength keys you must install Unlimited Strength Jurisdiction Policy Files before logging in to the TCM Application. For information, see "Install unlimited strength .jar files" on page 70. **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Create the folder structure on your TCM servers." on page 19 and "(Optional) Copy the User Credentials cryptographic key file." on page 20 for more information. c. Click **Next**.

In this screen...	Perform this action...
User Token Security	This screen lets you select the UTCryptoKeyFile.properties file. a. Browse for an existing UTCryptoKeyFile.properties file or accept the default path. The default location for the UTCryptoKeyFile.properties file is: ***<TCM_install_path>*/FileNet/Authentication/** For multiple FileNet applications to pass user tokens between one another, each participating application must use the same encryption key file. If you are installing the TCM application on the same server as Workplace, the file is located as follows: ***<AE_install_path>*/FileNet/Authentication/CryptoKeyFile.properties** If this is not a collocated system, then after the setup program completes, copy the **UTCryptoKeyFile.properties** file installed with Application Engine to the TCM Application server. If you are using JDK 1.4 and use unlimited strength keys you must install Unlimited Strength Jurisdiction Policy Files before logging in to the TCM Application. For information, see "Install unlimited strength .jar files" on page 70. b. Click **Next**.

In this screen...	Perform this action...
Collaboration Web Application Security	This screen lets you browse to the folder where the installer creates the TCMCryptoKeyFile.properties file used to encrypt web meeting login information. The default location for the TCMCryptoKeyFile.properties file is: **<*TCM_install_path*>/FileNet/Authentication/ TCMCryptoKeyFile.properties** a. (Optional) Check the box if you want to create maximum strength keys. By default, the installer creates limited strength (128-bit) keys; if you check the box, the installer creates maximum strength (448-bit) keys. **CAUTION** If you are using JDK 1.4 and use unlimited strength keys you must install the Unlimited Strength Jurisdiction Policy Files before logging in to the TCM Application. For information, see "Install unlimited strength .jar files" on page 70. b. Select the default location or browse to a folder where the installer will create the TCMCryptoKeyFile.properties file. **CAUTION** In the browser the **Open** button selects the current or highlighted folder. To navigate between folders double-click a folder to open it. To select a folder highlight it and click **Open**. The browser selects folder path and appends TCMCryptoKeyFile.properties to it. c. Click **Next**. **NOTES** The installer creates the cryptographic key file, and places it in the directory specified above. If a TCMCryptoKeyFile.properties file already exists in the directory, that file will be used. The installer will *not* create a new file.

In this screen...	Perform this action...
P8 Process Router Configuration	Enter the following information for the router running on the Application Engine. If a router is not yet configured or running on the Application Engine, it can be set up after the TCM setup program completes. a. Process router system. Enter the full computer name or the IP address of the server the router is running on. b. Process Router Port Enter the process router port. (Default: 32771) c. Process Router Name Enter the name of the process router. (Default: vwrouter)

In this screen...	Perform this action...
P8 Workplace Configuration	Provide the following information: a. Collaboration Object Store name Enter the name of the Object Store that contains the TCM Application AddOns. For more information, refer to "Install the Content Engine Integration" on page 24. b. Workplace server Enter the full machine name or IP address used by clients to access Workplace. c. Workplace port number Enter the port number of the Workplace application. **NOTE** Enter 0 If you don't have to specify a port number when accessing Workplace. d. Workplace Application Name Enter the name of the Application Engine application (Default: Workplace). e. Secure Workplace server Enter the full machine name or IP address used by clients to access Workplace on the secure server. If SSL is not being used, leave the default values. f. Secure Workplace port number Enter the secure port number of the Workplace application. If SSL is not being used, leave the default values. **NOTE** Enter 0 If you don't have to specify a port number when accessing Workplace.

In this screen...	Perform this action...
Documentation Configuration	For the documentation URL, enter the Documentation Server URL, which is where the FileNet P8 Platform Documentation is installed, then click **Next**. Your entry must be in the following format: `http://<docserver>:<port#>/<ecm_help>/` where: <*docserver*> is the name of the Java web server. <*port#*> is the port number. <*ecm_help*> is the root folder of the documentation website. You can use multi-part root folders (e.g., /docs/ecm_help) if your application server supports them. See "Install FileNet P8 Platform documentation" on page 65 for more information. **NOTE** For information on how to reconfigure the Documentation URL, go to the *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Application Engine Administration > Key configuration files and logs > Bootstrap properties.
Upload Directory	Select the Upload Directory, then click **Next**. The Upload Directory is the directory used by TCM Application to store temporary copies of files uploaded to Workplace. Leave the default option or browse for a directory to hold the temporary upload files. **CAUTION** Using a UNC admin share (ex: **\\server\C$**) for a shared upload directory location is not supported. An ordinary share may be used.
Download Directory	Select the Download Directory, then click **Next**. The Download Directory is the directory used by the TCM Application to store temporary copies of files downloaded from Workplace. Leave the default option or browse for a directory to hold the temporary download files. **CAUTION** Using a UNC admin share (ex: **\\server\C$**) for a shared download directory is not supported. An ordinary share may be used.
Ready to Install	Verify your selections, and click **Next** to install the TCM Application.
Completing the setup wizard	Click **Finish** to complete the installation.

4. Verify that the installation was successful.

   The following file should contain no errors.

   <*TCM_install_path*>/FileNet/TCM_install_log_35.txt

5. Copy the TCMCryptoKeyFile.properties file to the Collaboration Engine server and the Collaboration Mail Server server. For more information, see “Copy the TCM cryptographic key file.” on page 20.

   CAUTION You must copy the TCMCryptoKeyFile.properties file to the Collaboration Engine server and to the Collaboration Mail Server before you run the installer on these servers.

Deploy the TCM Application

After you have installed the TCM application, you need to deploy it. The following topics contain deployment instructions for the application servers supported by TCM.

To deploy the TCM Application

- Deploy the TCM Application (JBoss/Tomcat). Do Task 6a on page 41.
- Deploy the TCM Application (WebLogic). Do Task 6b on page 46.
- Deploy the TCM Application (WebSphere). Do Task 6c on page 49.

Task 6a: Deploy the TCM Application (JBoss/Tomcat)

This topic covers the deployment of the TCM application (TCM) on JBoss/Tomcat.

CAUTION If you are collocating the TCM Application with another web application such as Workplace, follow the instructions in "To collocate the TCM Application with other applications on JBoss" on page 45.

To deploy the TCM Application

1. (JBoss using JRE 1.4.x) Move .jar files.
   a. If it doesn't exist, create the following directory on your application server:

      ***<JRE_dir>*/lib/endorsed**

      NOTE If the folder already exists, back up all jars in the folder.

   b. Move the following three .jar files.

      - xercesImpl.jar
      - xml-apis.jar
      - xalan.jar

      Move the files from:

      ***<TCM_install_path>*/FileNet/Collaboration/TCM/WEB-INF/lib**

      to:

      ***<JRE_dir>*/lib/endorsed**

2. (JBoss using JRE 1.3.x) Configure JCE.

   CAUTION If the TCM Application is collocated with another application you may have already added the required .jar files and the com.sun.crypto.provider.SunJCE to the configuration. If this is the case, continue with the next step.

   a. Copy the following .jar files from the installed ***<TCM_install_path>*/FileNet/Collaboration/lib2** folder to the ***<JRE_dir>*/lib/ext folder**:

      - jce1_2_2.jar
      - sunjce_provider.jar
      - local_policy.jar
      - US_export_policy.jar

   b. Modify the java.security file.

      i. Use a text editor to open the java.security file used by the application server, and typically stored in the following location:

         ***<JRE_dir>*/lib/security**

ii. Add the following line, specifying a preference order that does not conflict with an existing entry:

```
security.provider.n=com.sun.crypto.provider.SunJCE
```

where n is the preference order value. In the example below, you can specify a preference order value of 3 or higher.

NOTE If you want to use a JCE provider other than SunJCE, make sure it is compatible with the JDK version in use and supports the Blowfish algorithm in ECM mode. Follow the JCE vendor's instructions for installation.

The following is an example from the JRE 1.3.x java.security file:

```
#
# List of providers and their preference orders (see above):
#
security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.rsajca.Provider
security.provider.3=com.sun.crypto.provider.SunJCE
```

iii. Save and close the java.security file.

3. (JBoss 3.x using JRE 1.3.x *or* JBoss using JRE 1.3.x with a WebEx URL that begins with https) Configure JSSE.

CAUTION If the TCM Application is collocated with another application you may have already added the required .jar files and the com.sun.net.ssl.internal.ssl.Provider to the configuration. If this is the case, continue with the next step.

a. Copy the following .jar files from the installed ***<TCM_install_path>*/FileNet/Collaboration/lib2** folder to the ***<JRE_dir>*/lib/ext** folder:

- jsse.jar
- jnet.jar
- jcert.jar

b. Modify the java.security file.

i. Use a text editor to open the java.security file used by the application server. The file is typically stored in the following location:

***<JRE_dir>*/lib/security**

ii. Add the following line, specifying a preference order that does not conflict with an existing entry:

```
security.provider.n=com.sun.net.ssl.internal.ssl.Provider
```

where n is the preference order value. In the example below, we have specified a preference order value of 4.

The following is an example from the JDK 1.3.x java.security file:

```
#
# List of providers and their preference orders (see above):
#
security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.rsajca.Provider
security.provider.3=com.sun.crypto.provider.SunJCE
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
```

iii. Save and close the java.security file.

4. (JBoss 3.x using JRE 1.3.x) Set the JBoss web loader attribute to false.
   a. Stop JBoss.
   b. On the JBoss server, open the jboss-service.xml file available in the ***<JBoss_HOME>*/server/default/deploy/jbossweb-tomcatNN.sar/META-INF** folder, where NN is the version of JBoss you are running.
   c. Change the value of the `UseJBossWebLoader` attribute in the jboss-service.xml file to **false**.
   d. Save and close the jboss-service.xml file.
   e. Start JBoss.
5. (JBoss 3.x using JRE 1.3.x) Update .jar files.
   a. Delete the following .jar files:
      - ***<JBoss_HOME>*/lib/xercesImpl.jar**
      - ***<JBoss_HOME>*/lib/xml-apis.jar**
      - ***<JBoss_HOME>*/server/all/lib/xalan.jar**
      - ***<JBoss_HOME>*/default/lib/xalan.jar**
   b. Copy the following files from ***<TCM_install_path>*/WEB-INF/lib** to ***<JBoss_HOME>*/lib**:
      - xercesImpl.jar
      - xml-apis.jar
   c. Copy the following file from ***<TCM_install_path>*/WEB-INF/lib** to ***<JBoss_HOME>*/server/all/lib**:
      - xalan.jar
   d. Copy the following file from ***<TCM_install_path>*/WEB-INF/lib** to ***<JBoss_HOME>*/default/lib**:
      - xalan.jar
6. Configure the application server

   JBoss

   a. On the JBoss server, copy the **/TCM** folder from:

      ***<TCM_install_path>*/FileNet/Collaboration/**

      to:

      ***<JBoss_HOME>*/server/default/deploy/**

   b. Append the extension .war to the TCM folder:

      ***<JBoss_HOME>*/server/default/deploy/TCM.war**

   Tomcat

   a. On the Tomcat server, copy the **/TCM** folder from:

      ***<TCM_install_path>*/FileNet/Collaboration/**

      to:

      ***<Tomcat_HOME>*/webapps/**

7. (Optional) Disable JBoss logging.

   In development mode JBoss creates a large amount of Server log and HTTP access log messages. This can cause unexpected behavior in the deployed FileNet software. To turn logging off, follow the procedure below.

   NOTE With logging turned off error messages will still be displayed in the JBoss console.

   To disable JBoss logging

   a. Edit the log4j.xml file (**<*JBoss_HOME*>/server/default/conf/log4j.xml**).

      i. Change all threshold values and priority values from "INFO", "DEBUG", or "TRACE" to "ERROR".

      ii. Delete or comment out the "Preserve messages in a local file" to turn off the server log.

   b. Edit the jboss-service.xml file (**<*JBoss_HOME*>/server/default/deploy/jbossweb-tomcatNN.sar/META-INF**), where NN is the version of JBoss you are running.

      Delete or comment out the "Access logger" section to turn off HTTP access logging.

   c. Edit the transaction-service.xml (**<*JBoss_HOME*>/server/default/deploy**).

      Change the value of the "Debug" attribute from true to false, to turn off JCA debugging.

   d. Edit the web.xml (**<*JBoss_HOME*>/server/default/deploy/jbossweb-tomcatNN.sar**), where NN is the version of JBoss you are running.

      Change the logVerbosityLevel to "FATAL".

8. Set permissions for the user running the application server.

   If the user that will be running the application server is different from the user that installed the TCM Application, you must give the user read/write permissions on the following folders:

   JBoss:

   UNIX

   <*JBoss_HOME*>/server/default/deploy/TCM.war

   <*TCM_install_path*>/FileNet/

   Windows (only required for NTFS formatted partitions):

   <*JBoss_HOME*>\server\default\deploy\TCM.war

   <*TCM_install_path*>\FileNet

   Tomcat:

   Windows (only required for NTFS formatted partitions):

   <*Tomcat_HOME*>\webapps\TCM

   <*TCM_install_path*>\FileNet

9. Restart the application server.

10. Logon to the application server console to confirm that the application server is running.

To collocate the TCM Application with other applications on JBoss

If you plan to collocate the TCM Application with another application such as Workplace, you must set the JBoss web loader attribute to false.

1. Stop JBoss.
2. On the JBoss server, open the jboss-service.xml file available in the **<*JBoss_HOME*>/server/default/deploy/jbossweb-tomcatNN.sar/META-INF** folder, where NN is the version of JBoss you are running.
3. Change the value of the `UseJBossWebLoader` attribute in the jboss-service.xml file to **false**.
4. Save and close the jboss-service.xml file.
5. Start JBoss.

Task 6b: Deploy the TCM Application (WebLogic)

This topic covers the deployment of the TCM web application (TCM) on WebLogic.

To deploy the TCM Application

1. (WebLogic using JRE 1.3) Configure JCE.

   CAUTION If the TCM Application is collocated with another application you may have already added the required .jar files and the com.sun.crypto.provider.SunJCE to the configuration. If this is the case, continue with the next step.

   a. Copy the following .jar files from the installed ***<TCM_install_path>*/FileNet/Collaboration/lib2** folder to the ***<TCM_install_path>*/FileNet/Collaboration/TCM/WEB-INF/lib** folder:

      - jce1_2_2.jar
      - sunjce_provider.jar
      - local_policy.jar
      - US_export_policy.jar

   b. Modify the java.security file.

      i. Use a text editor to open the java.security file used by the application server, and typically stored in the following location:

         ***<JRE_dir>*/lib/security**

      ii. Add the following line, specifying a preference order that does not conflict with an existing entry:

         ```
         security.provider.n=com.sun.crypto.provider.SunJCE
         ```

         where n is the preference order value. In the example below, you can specify a preference order value of 3 or higher.

         NOTE If you want to use a JCE provider other than SunJCE, make sure it is compatible with the JDK version in use and supports the Blowfish algorithm in ECM mode. Follow the JCE vendor's instructions for installation.

         The following is an example from the JRE 1.3 java.security file:

         ```
         #
         # List of providers and their preference orders (see above):
         #
         security.provider.1=sun.security.provider.Sun
         security.provider.2=com.sun.rsajca.Provider
         security.provider.3=com.sun.crypto.provider.SunJCE
         ```

      iii. Save and close the java.security file.

2. (WebLogic using JRE 1.3 and using a WebEx URL that begins with https) Configure JSSE.

   CAUTION If the TCM Application is collocated with another application you may have already added the required .jar files and the com.sun.net.ssl.internal.ssl.Provider to the configuration. If this is the case, continue with the next step.

a. Copy the following .jar files from the installed ***<TCM_install_path>*/FileNet/Collaboration/lib2** folder to the ***<TCM_install_path>*/FileNet/Collaboration/TCM/WEB-INF/lib** folder:

   - jsse.jar
   - jnet.jar
   - jcert.jar

b. Modify the java.security file.

   i. Use a text editor to open the java.security file used by the application server, and typically stored in the following location:

      ***<JRE_dir>*/lib/security**

   ii. Add the following line, specifying a preference order that does not conflict with an existing entry:

      ```
      security.provider.n=com.sun.net.ssl.internal.ssl.Provider
      ```

      where n is the preference order value. In the example below, we have specified a preference order value of 4.

      The following is an example from the JDK 1.3 java.security file:

      ```
      #
      # List of providers and their preference orders (see above):
      #
      security.provider.1=sun.security.provider.Sun
      security.provider.2=com.sun.rsajca.Provider
      security.provider.3=com.sun.crypto.provider.SunJCE
      security.provider.4=com.sun.net.ssl.internal.ssl.Provider
      ```

   iii. Save and close the java.security file.

3. Create a new Web Application.

   - WebLogic 7.x

      i. If it's not already running, start the WebLogic server. Wait until the WebLogic console displays the message "Server started in RUNNING mode" before continuing.

      ii. Start the WebLogic Server Console.

      iii. Specify the username and password for logging on to WebLogic. The Welcome page of the WebLogic server displays.

      iv. From the WebLogic Server Console, under ***<mydomain>*** expand **Deployments**, and click **Web Applications**.

      v. Click **Configure a new Web Application**.

      vi. From the right pane of the WebLogic Server Console, browse to the Collaboration folder:

         ***<TCM_install_path>*/FileNet/Collaboration/**

         Click **Select** to select **TCM**.

      vii. Select ***<myserver>*** from **Available Servers** and click the right-arrow button so that ***<myserver>*** becomes the target server. Verify that the **Application Name** is **TCM**.

      viii. Click **Configure and Deploy**.

NOTE To verify that the deployment was successful, expand **Deployments** and **Web Application Modules**. The web application TCM will be listed.

ix. Click the **Other** sub-tab. Check **Prefer Web Inf Classes**, and click **Apply**.

- WebLogic 8.1.x

  i. If it's not already running, start the WebLogic server. Wait until the WebLogic console displays the message "Server started in RUNNING mode" before continuing.

  ii. Start the WebLogic Server Console.

  iii. Specify the username and password for logging on to WebLogic. The Welcome page of the WebLogic server displays.

  iv. Click the **Deploy a new Web Application Module** link. The Deploy a Web Application Module page displays.

  v. Navigate to the folder **<*TCM_install_path*>/FileNet/Collaboration**.

  vi. Select the radio button next to TCM.

  vii. Click **Target Module**.

  viii. Click **Deploy**.

  ix. When the deployment completes successfully, stop and restart the WebLogic domain.

Task 6c: Deploy the TCM Application (WebSphere)

This topic covers the deployment of the TCM application (TCM) on WebSphere.

To deploy the TCM Application

1. Set JVM memory settings.
   a. From the WebSphere Administrative Console, expand **Servers**, and click **Application Servers**.
   b. Click ***<server name>***.
   c. (WebSphere 5.1) Under “Additional Properties”, select **Process Definition**.
   d. (WebSphere 6.0) Under “Server Infrastructure”, select **Java and Process Management** and then **Process Definition**.
   e. Select **Java Virtual Machine**.
   f. Enter the numbers for the Initial and Maximum Heap Size.

      NOTE Please refer to your application server vendor's recommendation for Initial and Maximum heap size values.

   g. Click **Apply**.
2. Set UTF-8 encoding.
   a. From the WebSphere Administrative Console, expand **Servers**, and click **Application Servers**.
   b. Click ***<server name>***.
   c. (WebSphere 5.1) Under “Additional Properties”, select **Process Definition**.
   d. (WebSphere 6.0) Under “Server Infrastructure”, select **Java and Process Management** and then **Process Definition**.
   e. Select **Process Definition** and then select **Java Virtual Machine**.
   f. Click **Custom Properties**.
   g. Click **New**.
   h. In the **Name** field, enter

      ```
      client.encoding.override
      ```

   i. In the **Value** field, enter

      ```
      UTF-8
      ```

   j. Click **Apply**, **Save**, then **Save** to save changes to the Master Configuration.
3. (WebSphere 5.1) Install the Enterprise Application (TCM).

   NOTE If you are running WebSphere 6.0, follow the instructions in “(WebSphere 6.0) Install the Enterprise Application (TCM).” on page 51.

   a. Verify that the collaboration_application.war file was created before you continue.

      The default path is:

      ***<TCM_install_path>*/FileNet/Collaboration/TCM**

b. From the Administrative Console, expand **Applications**. Click **Install New Application**. The “Preparing for the application installation” dialog opens.

c. (If the Administrative Console is running *locally*) Select **Local Path** and enter or browse to the location of the **collaboration_application.war** file created by the setup program. Do not enter the machine name.

d. (If the Administrative Console is *remote*) Select **Server path** and enter the fully-qualified path name to the **collaboration_application.war** file. Do not enter the machine name.

e. Enter the context root:

   Enter **TCM** and click **Next** to proceed to deploying a new application.

   NOTE The context root is the name of the application you log in to using the web interface, e.g. `http://<TCMServerName>:<port#>/<Context Root>`.

f. On the “Preparing for the application installation” screen, leave the defaults, and click **Next**.

g. On the “Application Security Warning” screen, click **Continue**.

h. At “Install New Application”, Step 1, specify the application name.

   Enter **TCM**, or the name you chose to call the application, and then click **Next**.

i. At “Install New Application”, Step 2, specify the **Virtual Host** for the virtual host that you are planning to use. Check **TCM** and keep the default virtual host (default_host), click **Next**.

j. At “Install New Application”, Step 3, configure your application server, and then click **Next**.

k. At “Install New Application”, Step 4, verify your configuration and click **Finish**. Once the configuration is saved, click **Save to Master Configuration**.

l. Configure the Classloader settings.

   i. From the Administrative Console, expand **Applications**. Click **Enterprise Applications**, and click your application (default TCM).

   ii. From the **Configuration** tab, set Classloader Mode to **PARENT_LAST**.

   iii. Verify that the **WAR Classloader Policy** is set to **Module**.

      NOTE You do this only for the specific web application. There are similar settings for the entire application server. Do not change these.

m. Configure the Web Module Classloader setting.

   i. From the Administrative Console, expand **Applications**. Click **Enterprise Applications**, and click your application (default TCM). Under Related Items, click **Web Modules**. Click **collaboration_application.war**.

   ii. From the **Configuration** tab, set Classloader Mode to **PARENT_LAST**.

      NOTE Do this only for the specific web application. There are similar settings for the entire application server. Do not change these.

n. Click **Apply**, **Save**, then **Save changes to the Master Configuration**.

o. Regenerate the web server plug-in.

   From the Administrative Console, expand **Environment**. Click **Update Webserver Plugin**, then click **OK**.

p. Continue with "Stop and restart the application server, (and restart the HTTP server, if installed)." on page 160.

4. (WebSphere 6.0) Install the Enterprise Application (TCM).

   a. Verify that the collaboration_application.war file was created before you continue.

      The default path is:

      ***<TCM_install_path>*/FileNet/Collaboration/TCM**

   b. From the WebSphere Administrative Console, expand **Applications**. Click **Install New Application**. The "Preparing for the application installation" dialog opens.

   c. (If the Administrative Console is running *locally*) Select **Local Path** and enter or browse to the location of the **collaboration_application.war** file created by the setup program. Do not enter the machine name.

   d. (If the Administrative Console is *remote*) Select **Remote File System** and enter the fully-qualified path to the **collaboration_application.war** file. Do not enter the machine name.

   e. Enter the context root:

      Enter **TCM** and click **Next** to proceed to deploying a new application.

      NOTE The context root is the name of the application you log in to using the web interface, e.g. `http://<TCMServerName>:<port#>/<Context Root>`.

   f. On the "Preparing for the application installation" screen, leave the defaults, and click **Next**.

   g. On the "Application Security Warning" screen, click **Continue**.

   h. At "Install New Application", Step 1, specify the application name.

      Enter **TCM**, or the name you chose to call the application, and then click **Next**.

   i. At "Install New Application", Step 2, Map modules to servers, specify the **WebServer** you are planning to use. Check **TCM** and click **Next**.

   j. At "Install New Application", Step 3, Map virtual hosts for Web Modules, check **TCM** and keep the default virtual host (default_host), click **Next**.

   k. At "Install New Application", Step 4, verify your configuration and click **Finish**. Once the configuration is saved, click **Save to Master Configuration**.

   l. Configure the Classloader settings.

      i. From the Administrative Console, expand **Applications**. Click **Enterprise Applications**, and click your application (default TCM).

      ii. From the **Configuration** tab, set Classloader Mode to **PARENT_LAST**.

      iii. Verify that the **WAR Classloader Policy** is set to **Module**.

      NOTE Do this only for the specific web application. There are similar settings for the entire application server. Do not change these.

   m. Click **Apply**, **Save**, then **Save changes to the Master Configuration**.

   n. Configure the Web Module Classloader setting.

i. From the Administrative Console, expand **Applications**. Click **Enterprise Applications**, and click your application (default TCM). Under Related Items, click **Web Modules**. Click **collaboration_application.war**.

ii. From the **Configuration** tab, set Classloader Mode to **PARENT_LAST**.

NOTE You do this only for the specific web application. There are similar settings for the entire application server. Do not change these.

o. Click **Apply**, **Save**, then **Save changes to the Master Configuration**.

5. Start the Enterprise Application.

   From the Administrative Console, expand **Applications**. Click **Enterprise Application**. Check the box to the left of the **TCM** application (or whatever you named it), and click **Start**.

6. Set permissions for the user running the application server.

   If the local user that will be running the application server is different from the user that installed TCM, you must give the user read/write permissions on the following (default) folders:

   UNIX:

   <*WAS_HOME*>/profiles/default/installedApps/<*node_name*>/collaboration_application_war.ear/collaboration_application.war

   <*TCM_install_path*>/FileNet/

   Windows (only required for NTFS formatted partitions):

   <*WAS_HOME*>\profiles\default\installedApps\<*node_name*>\collaboration_application_war.ear\collaboration_application.war

   <*TCM_install_path*>\FileNet

Task 7: Configure Workflow for TCM use

To use the special Collaboration Component Integrator steps (Create Teamspace, Create Teamspace from Template, and Create Task) you must:

1. Configure the workflow region.
2. Add and transfer workflows.
3. Create workflow subscriptions that utilize the workflows added in step 2.

To configure Workflow settings on the Application Engine

1. Verify that your FileNet P8 environment, including TCM, is up and running.
2. Log in to the Application Engine server.

   UNIX - logon as a user with *write* access to the **/bin** directory and *read*, *write*, and *execute* access to the directory where you plan to install the TCM components.

   Windows - log on as a member of the local Administrators group or a user with equivalent permissions.
3. Ensure that the router you specified during the TCM application installation is configured and running.
4. Start the TCM Setup wizard:

   AIX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **AIX_filenet_TCM_setup.bin**.

   HP-UX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **HP11_filenet_TCM_setup.bin**.

   Linux - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **Linux_filenet_TCM_setup.bin**.

   Solaris - Insert and mount the TCM CD. Navigate to **/cdrom/cdrom0/** and execute **Solaris_filenet_TCM_setup.bin**.

   Windows - Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, navigate to the **CD-ROM** drive and execute **Win32_filenet_TCM_setup.exe**.

5. Complete the Setup screens as follows:

In this screen...	Perform this action...
License Agreement	Review and accept the FileNet Software License Agreement, and then click **Next**.
Directory Name	For the Directory Name field, enter or browse to the location where you want to install the TCM software (***<TCM_install_path>***), or accept the default location: UNIX - **/opt** Windows - **C:\Program Files** Click **Next**. The installation program creates a **FileNet** directory at the selected location, and installs the TCM software in this directory: ***<TCM_install_path>*/FileNet/Collaboration**
Choose the Setup Type	Select **Workflow Integration**, and click **Next**.
Ready to Install	Read the summary and click **Next** to install the Workflow Integration.
Completing the setup wizard	Click **Finish** to complete the installation.

6. Verify that the installation was successful.

   The following file should contain no errors.

   ***<TCM_install_path>*/FileNet/TCM_install_log_35.txt**

7. Launch the Process Configuration Console.

   a. Launch Workplace from the Application Engine or from an alternate location if the Application Engine browser does not support the use of Java applets.

   b. Log on with an account that is a member of the PWConfiguration access role and has Collaboration Administrator privileges.

   c. Select the **Admin** tab.

   d. Launch the Process Configuration Console.

   e. Right-click the router name and select **Connect**.

   f. If the process region has not yet been initialized, right-click on the router name and select **Initialize Isolated Region**.

8. Import the TCM workflow configuration file.

   a. From the Process Configuration Console, right-click the router and select **Import from XML file**.

   b. Click **Browse** and select the CollaborationWorkflowConfiguration.xml file. This file is available in the ***<TCM_install_path>*/FileNet/Collaboration/Workflow** folder on the Application Engine server.

c. Select the **Merge** option.

d. Click **Import**, then click **Yes** to proceed with the import.

e. Once the screen indicates Success, click **Close**.

9. Update the adaptor settings for the Collaboration_Operations component queue.

   a. From the Process Configuration Console, expand the Server 0 node for the router you are using.

   b. Expand the Component Queues node.

   c. Right-click **Collaboration_Operations** and select **Properties**.

   d. Select the Operations tab and verify that the following operations exist:

      - createTeamspace
      - createTeamspaceFromTemplate
      - createTask
      - createTeamspaceWithMembers

   e. Select the **Adaptor** tab.

   f. In the JAAS credentials field, enter the user name and password of a person who is both a Collaboration Administrator and a PE Administrator.

   g. In the Configure Content text box, type **CELogin**.

   h. Click **OK**.

   i. Right-click on the router name and select **Commit Changes**.

      The Process Configuration Console dialog box displays.

   j. Click **Continue**.

   k. When the changes have been saved, click **Close**.

10. Assign users and groups to the Collaboration_Wait work queue.

    By assigning users and groups to this queue you specify who can view, and if necessary, process work queue items. In generally tasks in this queue are handled automatically and no manual intervention is required.

    a. From the Process Configuration Console, expand **Server0 > Work Queues**.

    b. Right-click the **Collaboration_Wait** queue.

    c. Select **Properties**.

    d. Select the **Security** tab.

    e. Add users and groups who should have visibility to this queue.

    f. Click **OK**.

11. Configure the CollaborationIntegration workflow.

    The TCM Workflow Integration component copies the following workflow definition (.pep) file to the ***<TCM_install_path>*/FileNet/Collaboration/Workflow** folder:

    ```
    CollaborationIntegration.pep
    ```

    To make this workflow available to TCM users you must complete the following three steps:

    1. Add the workflow to the Collaboration object store.
    2. Transfer the workflow to the Process Engine.
    3. Create subscriptions that will enable the workflow to be launched from within the TCM application.

    Complete the following steps from a browser that has access to the CollaborationIntegration.pep file.

    To add the Workflow to the Collaboration object store

    a. Log on to Workplace as a user with Site Administrator and Process Engine administrator rights.

    b. Add a folder to the Collaboration object store.

    c. Navigate into the new folder and select **Add Document**.

       The Add Document wizard displays.

    d. Select the **Workflow Definition** document class.

    e. Click **Next**.

    f. Enter a name of your choice in the Document Title field.

    g. Set **Add as a Major Version** to **Yes**.

    h. Click **Next**.

    i. If appropriate, update the security settings and then click **Next**.

    j. Browse to and select CollaborationIntegration.pep from:

       ***<TCM_install_path>*/FileNet/Collaboration/Workflow**

    k. Click **Finish**.

       The Workplace Browse window displays.

    To transfer the Workflow to the Process Engine

    a. In the Workplace Browse window, right-click on the new document and select **Transfer Workflow**.

    b. When the Workflow definition has been successfully transferred, click **OK**.

    To create Workflow Subscriptions

    In order to launch workflows from the TCM application, you must create workflow subscriptions.

    The following procedure enables TCM Application users to launch workflows from the Teamspace Overview tab.

    a. Log on to Workplace as a user with Site Administrator and object store administator rights for the Collaboration object store.

    b. Go to **Authoring > Advanced Tools**.

c. Click **Add Workflow Subscription**.

d. Select the Collaboration object store.

e. Select **Folder > Collaboration Folder** as the Target Type.

f. Click **Next**.

g. Click the **Browse/Search for Workflow Definition** link.

h. Navigate to the workflow you added in the preceding procedure.

i. Click on the **Select from Versions** link that is displayed the workflow definition name.

j. Click **Select** under the desired version and then click **Next**.

For a new installation, there is only one version. If you edit the workflow definition and retransfer the workflow, you must update the subscription to point to the new version.

k. Give a name to your Workflow Subscription.

l. Check the **Initial State Enabled** box.

m. Set the **Enable Manual Launch** to Yes.

n. Click **Next**.

o. Click **Next** on the Event Expression Builder screen.

p. Click **Next** on the Property Mapping screen.

q. Set the appropriate security for the subscription and click **Finish**.

To enable launching of workflows the TCM document and folder Detail views, create Workflow Subscriptions with Target Types of

- Document
- Folder

12. Configure Component Manager.

Complete the following steps on the Application Engine.

a. If not already running, start Process Task Manager.

b. Stop the Component Manager, if running.

c. Select the Required Libraries tab.

Click the document icon and add the following libraries:

- ***<TCM_install_path>*/FileNet/Collaboration/Workflow/lib/bsoclb.jar**
- ***<TCM_install_path>*/FileNet/Collaboration/Workflow/lib/bsoclb_res.jar**
- ***<TCM_install_path>*/FileNet/Collaboration/Workflow/lib/bsoutil.jar**
- ***<TCM_install_path>*/FileNet/Collaboration/Workflow/lib/bsoutil_res.jar**
- ***<TCM_install_path>*/FileNet/Collaboration/Workflow/lib/CollaborationOperations.jar**
- ***<TCM_install_path>*/FileNet/Collaboration/Workflow/lib/CollaborationOperations_res.jar**

d. Click **Apply**.

e. Start Component Manager.

Task 8: Install the Collaboration Engine

The Collaboration Engine will be installed as a Windows service or a UNIX daemon. You will start Collaboration engine in “Start Collaboration Engine.” on page 78.

To install Collaboration Engine

CAUTION (HP-UX only) Enable the Java Service Wrapper prior to installing the Collaboration Engine. For more information, refer to “(HP-UX only) Enable Java Service Wrapper” on page 88.

1. Log in to the Collaboration Engine server as a user with read/write privileges on the folder where you will install the Collaboration Engine.
2. Start the TCM Setup wizard:

   AIX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **AIX_filenet_TCM_setup.bin**.

   HP-UX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **HP11_filenet_TCM_setup.bin**.

   Linux - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **Linux_filenet_TCM_setup.bin**.

   Solaris - Insert and mount the TCM CD. Navigate to **/cdrom/cdrom0/** and execute **Solaris_filenet_TCM_setup.bin**.

   Windows - Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, navigate to the **CD-ROM** drive and execute **Win32_filenet_TCM_setup.exe**.
3. Complete the Setup screens as follows:

In this screen...	Perform this action...
License Agreement	Review and accept the FileNet Software License Agreement, and then click **Next**.
Directory Name	For the Directory Name field, enter or browse to the location where you want to install the TCM software (**<*TCM_install_path*>**), or accept the default location: UNIX - **/opt** Windows - **C:\Program Files** **NOTE** The directory must exist; the installer will not create a directory for you. Click **Next**. The installation program creates a **FileNet** directory at the selected location, and installs the TCM software in this directory: **<*TCM_install_path*>/FileNet/Collaboration**
Choose the Setup Type	Select **Collaboration Engine**. Click **Next**.

In this screen...	Perform this action...
Content Engine Java API Configuration	Enter the Content Engine Java API information. • Content Engine's name – Enter the Content Engine server's full machine name or IP address. • Port Number – Enter the port number for the Content Engine's listening port (Default: 8008).
Application Engine User Security	This screen lets you select the CryptoKeyFile.properties file. This file holds the cryptographic keys that secure the communication between TCM and the Content Engine. a. Select credentials protection, the encryption method to protect stored logon credentials passed between Collaboration Engine and the Content Engine: • Clear - encodes credentials using base 64 encoding. • Symmetric - uses cryptography keys to encrypt and decrypt user credentials. b. (If you selected Symmetric encryption) Browse for an existing CryptoKeyFile.properties file or accept the default path. **<TCM_install_path>/FileNet/Authentication** **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Create the folder structure on your TCM servers." on page 19 and "(Optional) Copy the User Credentials cryptographic key file." on page 20 for more information. c. Click **Next**.

In this screen...	Perform this action...
User Token Security	This screen lets you select the UTCryptoKeyFile.properties file. a. Browse for an existing UTCryptoKeyFile.properties file or accept the default path. **<TCM_install_path>/FileNet/Authentication/** **CAUTION** For multiple FileNet applications to pass user tokens between one another, each participating application must use the same encryption key file. Copy the **UTCryptoKeyFile.properties** file installed with Application Engine to all servers that are hosting a token-sharing application. **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Create the folder structure on your TCM servers." on page 19 and "(Optional) Copy the User Credentials cryptographic key file." on page 20 for more information. b. Click **Next**.
Collaboration Web Application Security	This screen lets you browse for the TCMCryptoKeyFile.properties file used to encrypt user login information stored on the Collaboration Engine server. a. Browse for an existing TCMCryptoKeyFile.properties file or accept the default path. The default location for the TCMCryptoKeyFile.properties file is: **<*TCM_install_path*>/FileNet/Authentication/** **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Configure Symmetric Encryption" on page 19 for more information. **CAUTION** If you are using JDK 1.4 and use maximum strength TCM cryptographic keys (see "(Optional) Check the box if you want to create maximum strength keys." on page 35) you must install Unlimited Strength Jurisdiction Policy Files (see "Install unlimited strength .jar files" on page 70), and then manually configure the Collaboration Engine password after you complete the installation (see "Collaboration Engine Configuration" on page 74). b. Click **Next**.

In this screen...	Perform this action...
P8 Process Router Configuration	Enter the following information for the router running on the Application Engine. If a router is not yet configured or running on the Application Engine, it can be set up after the Collaboration Engine setup program completes. a. Process router system. Enter the full computer name or the IP address of the server the router is running on. b. Port Enter the process router port. (Default: 32771) c. Name Enter the name of the process router. (Default: vwrouter)
Collaboration Engine Configuration	Enter the information for the Collaboration Engine Object Store used to store the Collaboration Engine preferences. a. Object Store Enter the name of the object store that has been configured for use with TCM. b. User ID Enter the user ID of that was assigned to the sysadmin role in the Collaboration Applications.xml file. For more information, refer to “Sysadmin-Rights access role” on page 10. c. Password Enter the password for the user. **CAUTION** If you are using JDK 1.4 and use maximum strength TCM cryptographic keys you must install Unlimited Strength Jurisdiction Policy Files, see “Install unlimited strength .jar files” on page 70, and then manually configure the Collaboration Engine password after you complete the installer, see “Collaboration Engine Configuration” on page 74. d. Click **Next**.
Ready to Install	Verify your selections, and click **Next** to install Collaboration Engine.
Completing the setup wizard	Click **Finish** to complete the installation.

4. Verify that the installation was successful.

   The following file should contain no errors.

   <*TCM_install_path*>/FileNet/TCM_install_log_35.txt

CAUTION If you are using JDK 1.4 and use maximum strength TCM cryptographic keys there will be errors in this file indicating that there were problems performing encryption. This does not mean that the installation failed. To complete your configuration you must install Unlimited Strength Jurisdiction Policy Files, see “Install unlimited strength .jar files” on page 70, and then manually configure the Collaboration Engine password, see “Collaboration Engine Configuration” on page 74.

Task 9: Install the Collaboration Mail Server

To have TCM archive email messages in the Collaboration object store, you must install and configure the Collaboration Mail Server. The Collaboration Mail Server archives email sent to the teamspace into the Collaboration object store.

The Collaboration Mail Server is installed as a Windows service or a UNIX daemon.

To install the Collaboration Mail Server server

CAUTION (HP-UX only) Enable the Java Service Wrapper prior to installing the Collaboration Mail Server. For more information, refer to "(HP-UX only) Enable Java Service Wrapper" on page 88.

1. Log in to the Collaboration Mail Server server as a user with read/write permissions on the folder where you will install the Collaboration Mail Server.
2. (HP-UX only) Verify that have enabled the Java Service Wrapper on the server on which you plan to install Collaboration Mail Server. For more information, see "(HP-UX only) Enable Java Service Wrapper" on page 88.
3. Start the TCM Setup wizard:

   AIX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **AIX_filenet_TCM_setup.bin**.

   HP-UX - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **HP11_filenet_TCM_setup.bin**.

   Linux - Insert and mount the TCM CD. Navigate to **/<*mount_point*>/** and execute **Linux_filenet_TCM_setup.bin**.

   Solaris - Insert and mount the TCM CD. Navigate to **/cdrom/cdrom0/** and execute **Solaris_filenet_TCM_setup.bin**.

   Windows - Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, navigate to the **CD-ROM** drive and execute **Win32_filenet_TCM_setup.exe**.

4. Complete the Setup screens as follows:

In this screen...	Perform this action...
License Agreement	Review and accept the FileNet Software License Agreement, and then click **Next**.
Directory Name	For the Directory Name field, enter or browse to the location where you want to install the TCM software (***<TCM_install_path>***), or accept the default location: UNIX - **/opt** Windows - **C:\Program Files** Click **Next**. The installation program creates a **FileNet** directory at the selected location, and installs the TCM software in this directory: ***<TCM_install_path>*/FileNet/Collaboration**
Choose the Setup Type	Select **Collaboration Mail Server**. Click **Next**.
Content Engine Java API Configuration	Enter the Content Engine Java API information. • Content Engine's name – Enter the Content Engine server's full machine name or IP address. • Port Number – Enter the port number for the Content Engine's listening port (Default: 8008).
Application Engine User Security	This screen lets you select the CryptoKeyFile.properties file. This file holds the cryptographic keys that secure the communication between TCM and the Content Engine. a. Select credentials protection, the encryption method to protect stored logon credentials passed between TCM and the Content Engine: • Clear - encodes credentials using base 64 encoding. • Symmetric - uses cryptography keys to encrypt and decrypt user credentials. b. (If you selected Symmetric encryption) Browse for an existing CryptoKeyFile.properties file or accept the default path. **<TCM_install_path>/FileNet/Authentication/** **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Create the folder structure on your TCM servers." on page 19 and "(Optional) Copy the User Credentials cryptographic key file." on page 20 for more information. c. Click **Next**.

In this screen...	Perform this action...
User Token Security	This screen lets you select the UTCryptoKeyFile.properties file. a. Browse for an existing UTCryptoKeyFile.properties file or accept the default path. **<TCM_install_path>/FileNet/Authentication/** **CAUTION** For multiple FileNet applications to pass user tokens between one another, each participating application must use the same encryption key file. Copy the **UTCryptoKeyFile.properties** file installed with Application Engine to all servers that are hosting a token-sharing application. **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Create the folder structure on your TCM servers." on page 19 and "(Optional) Copy the User Credentials cryptographic key file." on page 20 for more information. b. Click **Next**.
Collaboration Web Application Security	This screen lets you browse for the TCMCryptoKeyFile.properties file used to encrypt user login information stored on the Collaboration Engine server. a. Browse for an existing TCMCryptoKeyFile.properties file or accept the default path. **<*TCM_install_path*>/FileNet/Authentication/ TCMCryptoKeyFile.properties** **NOTE** If you select the default location make sure you have created the folder structure and copied the cryptographic key file to the Authentication folder, see "Configure Symmetric Encryption" on page 19 for more information. **CAUTION** If you are using JDK 1.4 and use maximum strength TCM cryptographic keys (see "(Optional) Check the box if you want to create maximum strength keys." on page 35) you must install Unlimited Strength Jurisdiction Policy Files (see "Install unlimited strength .jar files" on page 70), and then manually configure the Collaboration Engine password after you complete the installation (see "Collaboration Engine Configuration" on page 74). b. Click **Next**.

In this screen...	Perform this action...
Collaboration Mail Server Configuration	Enter the following information to configure your Collaboration Mail Server. a. Object Store Enter the name of the object store that has been configured for use with TCM. b. User ID Enter the user ID of a user that is both a Collaboration Administrator and has been assigned the sysadmin role in the Collaboration Applications.xml file. For more information, refer to "Sysadmin-Rights access role" on page 10. c. Password Enter the password for the user ID. d. Mail domain This entry must match the email domain name in the Collaboration Applications.xml file that is in the Collaboration object store. For more information, see "Install the Content Engine Integration" on page 24. **CAUTION** The fully-qualified name should contain only alphanumeric characters, hyphens(-) or periods(.). DNS names that contain other characters can cause communication issues. e. SMTP port Enter the SMTP port used by the Collaboration Mail Server (default 25). **CAUTION** Verify that no other application is using the SMTP port. For more information, see "Required Collaboration Mail Server ports" on page 13. f. Click **Next**.
Ready to Install	Verify your selections, and click **Next** to install the Collaboration Mail Server.
Completing the setup wizard	Click **Finish** to complete the installation.

5. Verify that the installation was successful.

   The following file should contain no errors.

   <*TCM_install_path*>/FileNet/TCM_install_log_35.txt

CAUTION If you are using JDK 1.4 and use maximum strength TCM cryptographic keys there will be errors in this file indicating that there were problems performing encryption. This does not mean that the installation failed. To complete your configuration you must install Unlimited Strength Jurisdiction Policy Files, see “Install unlimited strength .jar files” on page 70, and then manually configure the Collaboration Engine password, see “Collaboration Mail Server Configuration” on page 76.

Configuration/Startup Tasks

To configure and start the TCM components

1. Install unlimited strength .jar files. Do Task 10 on page 70.
2. (Optional) Manually Configure TCM. Do Task 11 on page 71.
3. Start Team Collaboration Manager. Do Task 12 on page 78.
4. (Optional) Setup TCM SSL security. Do Task 13 on page 82.

Task 10: Install unlimited strength .jar files

Perform this task on the Collaboration Engine server, the TCM Application server, and the Collaboration Mail Server after you have installed the TCM applications.

CAUTION You will need a tool such as WinZip to extract the compressed files you will be downloading. Make sure you have installed this tool before you download the files.

You must install the unlimited strength jar files if:

- You are using JDK 1.4 or higher

  and

- You have selected the *Create maximum strength keys* option in the security steps of the installer

  and/or

- You are using maximum strength keys from the Application Engine for login and/or user token security.

Failure to perform the step will cause EncryptionException messages or other errors indicating that a Java Security API provider for Blowfish is not available. The EncryptionException is caused by the wrong versions of (or absence of) required .jar files that provide unlimited strength security policy files in a Sun JDK 1.4 or higher environment.

For more information, go to the *Documentation for FileNet P8 Platform* website and navigate to Developer Help > Content Java API > Security > Working with Security > Creating Cryptographic Keys for Symmetric Encryption. Scroll down for the *Configuring a Security Provider for a J2EE Application Server Environment section*.

To install unlimited strength .jar files

1. Obtain the unlimited strength .jar files.
   - Sun JDK 1.4 - Obtain the Sun unlimited strength policy files from the Sun product web site (http://java.sun.com/products/jce).
   - IBM JDK 1.4 - Obtain the IBM unlimited jurisdiction policy files from the IBM web site (http://www.ibm.com/developerworks/java/jdk/security).
2. Install the files into the following folders by replacing files with the same names.
   - TCM Application - ***<JRE_dir>*/lib/security**

     This is the location that the application server (for example WebSphere, WebLogic, JBoss) loads its JRE.
   - Collaboration Engine - ***<TCM_install_path>*/FileNet/Collaboration/_jvm/lib/security**
   - Collaboration Mail Server - ***<TCM_install_path>*/FileNet/Collaboration/_jvm/lib/security**
3. Restart the TCM Application server.

Task 11: (Optional) Manually Configure TCM

If you run the TCM installer without providing any configuration data, or if you need to update configuration information after the installation is complete, you must manually configure the components for TCM to work properly.

Complete the editing tasks in this section using a standard text editor such as Notepad.

Running the Encrypt Password tool

TCM uses encrypted passwords in a number of configuration files. If you manually configure the configuration files or when you need to change a password, you must use the password encryption tool provided with TCM.

The TCM installer installs this tool on the Collaboration Engine and the Collaboration Mail Server.

CAUTION If you are using JDK 1.4 and use maximum strength keys in your TCMCryptoKeyFile.properties file you must install unlimited strength .jar files before running the Encrypt Password tool. For information, see "Install unlimited strength .jar files" on page 70.

To run the password encryption tool

1. Log in to the Collaboration Engine or Collaboration Mail Server.
2. Open a command window.
3. Run the encryption tool.
   - UNIX
     - Collaboration Engine

       Navigate to:

       <*TCM_install_path*>/FileNet/Collaboration/Collaboration/Engine/

       Run:

       ```
       ./EncryptPassword.sh <password>
       ```

     - Collaboration Mail Server

       Navigate to:

       <*TCM_install_path*>/FileNet/Collaboration/JamesMailServer/

       Run:

       ```
       ./EncryptPassword.sh <password>
       ```

   - Windows
     - Collaboration Engine

       Run the EncryptPassword.bat file:

       ```
       C:\PROMPT>
       <TCM_install_path>\FileNet\Collaboration\Collaboration\Engine\EncryptPass
       word.bat <password>
       ```

– Collaboration Mail Server

Run the EncryptPassword.bat file:

```
C:\PROMPT>
<TCM_install_path>\FileNet\Collaboration\JamesMailServer\EncryptPassword.
bat <password>
```

4. If prompted, type in the password you want to be encrypted.
5. The tool returns the encrypted password.
6. Open the appropriate configuration file and copy the encrypted password to the required location.

Configure the TCM servers

CAUTION To perform the manual configuration steps you must have read/write permissions on the TCM installation folder on each server.

The following files are created and configured by the TCM installer. If you choose to do a “default” installation you must edit these files with the actual values for your planned TCM system. These values are described in detail in the following procedures.

- Collaboration Engine server:
  - collabEngineConfig.properties (**<*TCM_install_path*>/FileNet/Collaboration/Engine**)
  - WcmApiConfig.properties (**<*TCM_install_path*>/FileNet/Collaboration/Engine**)
- TCM Application server:
  - BsoApiConfig.properties (**<*TCM_install_path*>/FileNet/Collaboration/TCM/WEB-INF/classes**)
  - config.properties (**<*TCM_install_path*>/FileNet/Collaboration/TCM/WEB-INF**)
  - WcmApiConfig.properties (**<*TCM_install_path*>/FileNet/Collaboration/TCM/WEB-INF**)
  - web.xml (**<*TCM_install_path*>/FileNet/Collaboration/TCM/WEB-INF**)
- Collaboration Mail Server server:
  - config.xml (**<*TCM_install_path*>/FileNet/Collaboration/JamesMailServer/apps/james/SAR-INF**)
  - WcmApiConfig.properties (**<*TCM_install_path*>/FileNet/Collaboration/JamesMailServer**)

To manually configure TCM

The following steps highlight the configuration files and corresponding values that need to be set before starting TCM. The numbered steps all correspond to TCM installer screens with the same names. The examples are taken from a Windows installation.

CAUTION Make sure you have backup copies of any files before you edit them. Also, make sure you save the files with the correct extension.

1. Content Engine Java API Configuration

   Set the values on the following servers:

   - TCM Application server
   - Collaboration Engine
   - Collaboration Mail Server server

   Edit the following values (bold in the example below):

   - Content Engine Server
   - Content Engine listening port

   Edit the following file:

   - WcmApiConfig.properties

   ```
   RemoteServerUrl =http://appserver.example.com:8008/ApplicationEngine/xcmisasoap.dll
   RemoteServerUploadUrl =http://appserver.example.com:8008/ApplicationEngine/doccontent.dll
   RemoteServerDownloadUrl =http://appserver.example.com:8008/ApplicationEngine/
   doccontent.dll
   ```

2. Application Engine User Security

   Set the values on the following servers:

   - TCM Application server
   - Collaboration Engine server
   - Collaboration Mail Server server

   Edit the following file:

   - WcmApiConfig.properties

   Edit the following values (bold in the example below):

   - Credentials protection (Clear or Symmetric)
   - Cryptographic key file location

   ```
   CredentialsProtection =Clear
   CryptoKeyFile =C:\\Program Files\\FileNet\\Authentication\\CryptoKeyFile.properties
   ```

   NOTE The installer does not create the cryptographic key file or folder structure, see “Configure Symmetric Encryption” on page 19.

3. User Token Security

   Set the values on the following servers:

   - TCM Application server
   - Collaboration Engine server
   - Collaboration Mail Server server

   Edit the following file:

   - WcmApiConfig.properties

Edit the following values (bold in the example below):

- Cryptographic key file location

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

NOTE The installer does not create the cryptographic key file or folder structure, see "Configure Symmetric Encryption" on page 19.

4. TCM Security

   Set the values on the following servers:

   - TCM Application server
   - Collaboration Engine server
   - Collaboration Mail Server server

   Edit the following files (with values bold in the examples below):

   - BsoApiConfig.properties (TCM Application server)

     ```
     TCMCryptoKeyFile=C:\\Program Files\\FileNet\\Authentication\\TCMCryptoKeyFile.properties
     ```

   - collabEngineConfig.properties (Collaboration Engine server)

     ```
     cryptoKeyFile=C:\\Program Files\\FileNet\\Authentication\\TCMCryptoKeyFile.properties
     ```

   - config.xml (Collaboration Mail Server server)

     ```
     <cryptoKeyFile>C:\\Program Files\\FileNet\\Authentication\\TCMCryptoKeyFile.properties</
     cryptoKeyFile>
     ```

     NOTE The installer creates the cryptographic key file and folder structure on the TCM Application server only. For more information, see "Configure Symmetric Encryption" on page 19.

5. P8 Process Engine Configuration

   Set the values on the following servers:

   - TCM Application server
   - Collaboration Engine server

   Edit the following values:

   - Process router system
   - Process router port
   - Process router name

   Edit the following files (with values bold in the examples below):

   - config.properties (TCM Application)

     ```
     processRouter=eprocess.example.com:32771/vwrouter
     ```

   - collabEngineConfig.properties (Collaboration Engine)

     ```
     processRouter=eprocess.example.com:32771/vwrouter
     ```

6. Collaboration Engine Configuration

   Set the values on the following server:

- Collaboration Engine server

Edit the following values:

- User ID - Enter the user ID that was assigned to the sysadmin role in the Collaboration Applications.xml file. For more information, refer to "Sysadmin-Rights access role" on page 10.
- Password - Encrypted, see "Running the Encrypt Password tool" on page 71.
- Object Store name

Edit the following file (with values bold in the example below):

- collabEngineConfig.properties

```
user=Administrator
password=<encrypted>
...
configObjectStore=Collaboration
```

7. P8 Workplace Configuration

   Set the values on the following server:

   - TCM Application server

   Edit the following values:

   - Object Store name - Enter the name of the Object Store where the TCM Application configuration files are stored.
   - Workplace server - Enter the full machine name or IP address used by clients to access Workplace.
   - Workplace port number - Enter the port number of the Workplace application.

     NOTE Enter 0 If you don't have to specify a port number when accessing Workplace.

   - Secure Workplace server - Enter the full machine name or IP address used by clients to access Workplace.
   - Secure Workplace port number - Enter the port number of the Workplace application.

     NOTE Enter 0 If you don't have to specify a port number when accessing Workplace.

   Edit the following file (with values bold in the example below):

   - config.properties

```
workplaceHTTPAppRoot=http://workplace.example.com:8080/Workplace
workplaceHTTPSAppRoot=https://workplace.example.com:8090/Workplace
defaultObjectStore=Collaboration
```

8. Documentation Configuration

   Set the values on the following server:

   - TCM Application server

   Edit the following values:

   - Documentation URL, see "To deploy and verify the documentation web site" on page 17.

Edit the following file (with values bold in the example below):

- config.properties

```
documentationServer=http://appserver.example.com:8080/ecm_help
```

9. Upload and Download Directory

   Set the values on the following server:

   - TCM Application server

   Edit the following values:

   - Upload Directory. For more information, see “Upload Directory” on page 38.
   - Download Directory. For more information, see “Download Directory” on page 38.

   Edit the following file (with values bold in the example below):

   - web.xml

```
- <context-param id="ContextParam_6">
  <param-name>uploadDir</param-name>
  <param-value>C:\Program Files\FileNet\Collaboration\TCM\upload</param-value>
  </context-param>
- <context-param id="ContextParam_7">
  <param-name>downloadDir</param-name>
  <param-value>C:\Program Files\FileNet\Collaboration\TCM\download</param-value>
```

10. Collaboration Mail Server Configuration

    Set the values on the following server:

    - Collaboration Mail Server server

    Edit the following values:

    - Object Store name - Enter the name of the Object Store used for Collaboration Mail Server configuration.
    - User ID - Enter the user ID of a user that is both a Collaboration Administrator and has been assigned the sysadmin role in the Collaboration Applications.xml file. For more information, refer to “Sysadmin-Rights access role” on page 10.
    - Password - Encrypted, see “Running the Encrypt Password tool” on page 71.
    - Mail domain - Enter the full DNS name for the server on which you have installed the Collaboration Mail Server.

      CAUTION The domain name should contain only alphanumerical characters, hyphens(-) or periods(.). Make sure this domain name is identical to the one entered in the Collaborations Applications.xml file. For more information, see “Clbmail.example.com” on page 30.

      If you plan to use the Collaboration Mail Server for mail archiving with a mail server that is open to outside email, you must set up your email domain for this. For more information, see “Collaboration Mail Server” on page 12.

- SMTP port - Enter the SMTP port used by the mail server (default 25).

  CAUTION Verify that no other application is using the SMTP port. For more information, see “Required Collaboration Mail Server ports” on page 13.

Edit the following file (with values bold in the example below):

- config.xml

```
<!-- Collaboration processing -->
…
<user>Administrator</user>
<password><encrypted></password>
<objectStore>Collaboration</objectStore>

<!--  Configuration file for the ASF James server -->
…
<servername>collab.example.com</servername>
```

Sharing the config.properties file among multiple TCM Applications

By default the TCM Application stores the config.properties configuration file in the following directory on the TCM Application server:

***<TCM_install_path>*/FileNet/Collaboration/TCM/WEB-INF**

If you want to store this configuration file in another location, such as a shared folder, you can configure the TCM Applications to look for it there using a servlet parameter.

To share configuration files between TCM Applications

1. Create a shared folder accessible by both TCM Application servers.
2. Install and configure one TCM application.
3. Copy the config.properties file from the ***<TCM_install_path>*/FileNet/Collaboration/WEB-INF** directory to the shared folder.
4. Configure the TCM Applications to share configuration files:
   a. On each of the TCM Application servers open the ***<TCM_install_path>*/FileNet/Collaboration/WEB-INF/web.xml** file for editing.
   b. Add the following to the file at the end of the context-param section:

```
<context-param id="ContextParam_6">
    <param-name>tcm.configDir</param-name>
    <param-value>\\<Server>\<shared_directory></param-value>
</context-param>
```

      Where param-value contains the full path to your the directory you want to use for your configuration files. TCM accepts local and UNC paths.

   c. Save the web.xml file.
5. Redeploy the TCM Application.

- “Deploy the TCM Application (JBoss/Tomcat)” on page 41.
- “Deploy the TCM Application (WebLogic)” on page 46.
- “Deploy the TCM Application (WebSphere)” on page 49.

Task 12: Start Team Collaboration Manager

This topic contains instructions on how to start TCM and how to configure automatic startup of the Collaboration Engine and Collaboration Mail Server on UNIX.

For complete startup/shutdown procedures, go to *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Enterprise-wide Administration > Shutdown and Startup.

To start Team Collaboration Manager

Start the TCM environment in the following order:

1. Start the FileNet P8 environment, including Content Engine, Process Engine, and Application Engine.
2. Verify that the router used by TCM is running.
3. Verify that Component Manager is running.
4. Start the Collaboration Mail Server.

   The Collaboration Mail Server is installed as a Windows service/UNIX daemon. The Windows service will automatically start when your server is rebooted. To configure the UNIX daemon for automatic restart, see "(UNIX only) Configure Collaboration Engine and Collaboration Mail Server daemons to automatically restart on reboot" on page 79.

   (UNIX) Start the Collaboration Service daemon.

   i. Open a terminal window.

   ii. Navigate to **<*TCM_install_path*>/FileNet/Collaboration/JamesMailServer/bin**

   iii. Run **./MailServer.sh start** to start the Collaboration Service daemon.

   NOTE To verify that the Collaboration Service daemon started correctly, see the service log:

   <*TCM_install_path*>/FileNet/Collaboration/JamesMailServer/logs/wrapper.log

   (Windows) Start the Collaboration Mail Server Windows service.

   i. Open **Start > Settings > Control Panel > Administrative Tools > Services**.

   ii. Locate and right-click the **Collaboration Mail Server service**.

   iii. Select **Start**.

   (Windows, command line) Start the Collaboration Mail Server Windows service.

   i. Open a command line window.

   ii. Execute:

   ```
   C:\ Prompt>net start "Collaboration Mail Server"
   ```

5. Start Collaboration Engine.

   The Collaboration Engine is installed as a Windows service/UNIX daemon. The Windows service will automatically start when your server is rebooted. To configure the UNIX daemon for automatic restart, see "(UNIX only) Configure Collaboration Engine and Collaboration Mail Server daemons to automatically restart on reboot" on page 79.

   (UNIX) Start the Collaboration Service daemon.

   i. Open a terminal window.

ii. Navigate to ***<TCM_install_path>*/FileNet/Collaboration/ManagedServices/bin**

iii. Run **./Engine.sh start** to start the Collaboration Service daemon.

NOTE To verify that the Collaboration Service daemon started correctly, see the service log:

***<TCM_install_path>*/FileNet/Collaboration/ManagementService/logs/engine.log**

(Windows) Start the Collaboration Engine Windows service.

i. Open **Start > Settings > Control Panel > Administrative Tools > Services**.

ii. Locate and right-click the **Collaboration Engine service**.

iii. Select **Start**.

(Windows, command line) Start the Collaboration Engine Windows service.

i. Open a command line window.

ii. Execute:

```
C:\ Prompt>net start "Collaboration Engine"
```

6. Verify that the TCM Application has been deployed and that the application server is running.

(UNIX only) Configure Collaboration Engine and Collaboration Mail Server daemons to automatically restart on reboot

The following procedures describe how to configure the Collaboration Service daemons to automatically reboot if the server is rebooted.

1. (Collaboration Mail Server) Configure Collaboration Service daemon to automatically start on reboot.

   Use the ConfigureStartOnReboot.sh script to configure the Collaboration Service daemon to automatically restart on reboot.

   CAUTION You *must* run this script as root.

   a. Login to the Collaboration Engine server as root.

   b. (Optional) Modify the startup and shutdown sequence order.

      The Collaboration Services should start after the core UNIX services and the PE server (if installed on the system). The service should shut down in the opposite order of startup.

      Example:

      If a service has a startup/shutdown order of twenty (20), then the Collaboration Service startup order should be set to more than twenty (for example 21) and the shutdown order less than twenty (for example 19).

      CAUTION If Collaboration Engine and Collaboration Mail Server are collocated, the Collaboration Mail Server daemon should be started before the Collaboration Engine daemon.

      i. Edit the ConfigureStartOnReboot.sh script, located in:

         ***<TCM_install_path>*/FileNet/Collaboration/JamesMailServer/bin**

      ii. Change the STARTUP_ORDER and SHUTDOWN_ORDER numbers.

      Example:

```
# Multi-user run level startup / shutdown order
STARTUP_ORDER="70"
SHUTDOWN_ORDER="70"
```

iii. Save the ConfigureStartOnReboot.sh script.

c. Run the ConfigureStartOnReboot.sh script.

i. Navigate to:

***<TCM_install_path>*/FileNet/Collaboration/JamesMailServer/bin**

ii. Run the script:

```
./ConfigureStartOnReboot.sh register
```

d. Reboot the server.

The Collaboration Service daemon should start automatically upon reboot. Use the wrapper.log file to verify that the daemon started, and that no errors were recorded.

The log file is written to:

***<TCM_install_path>*/FileNet/Collaboration/JamesMailServer/logs**

2. (Collaboration Engine) Configure Collaboration Service daemon to automatically start on reboot.

Use the ConfigureStartOnReboot.sh script to configure the Collaboration Service daemon to automatically restart on reboot.

CAUTION You *must* run this script as root.

a. Login to the Collaboration Engine server as root.

b. (Optional) Modify the startup and shutdown sequence order.

The Collaboration Service daemon should start after the core UNIX services and the PE server (if installed on the system). The service should shut down in the opposite order of startup.

Example:

If a service has a startup/shutdown order of twenty (20), then the Collaboration Service startup order should be set to more than twenty (for example 21) and the shutdown order less than twenty (for example 19).

CAUTION If Collaboration Engine and Collaboration Mail Server are collocated, the Collaboration Engine daemon should be started after the Collaboration Engine daemon.

i. Edit the ConfigureStartOnReboot.sh script, located in:

***<TCM_install_path>*/FileNet/Collaboration/ManagementService/bin**

ii. Change the STARTUP_ORDER and SHUTDOWN_ORDER numbers.

Example:

```
# Multi-user run level startup / shutdown order
STARTUP_ORDER="70"
SHUTDOWN_ORDER="70"
```

iii. Save the ConfigureStartOnReboot.sh script.

c. Run the ConfigureStartOnReboot.sh script.

i. Navigate to:

<*TCM_install_path*>/FileNet/Collaboration/ManagementService/bin

ii. Run the script:

```
./ConfigureStartOnReboot.sh register
```

d. Reboot the server.

The Collaboration Service daemon should start automatically upon reboot. Use the wrapper.log file to verify that the daemon started, and that no errors were recorded.

The log file is written to:

<*TCM_install_path*>/FileNet/Collaboration/ManagementService/logs

Task 13: (Optional) Setup TCM SSL security

This topic describes how to configure TCM to work with or direct sign-ins through an SSL (https) connection. It assumes that TCM has already been installed and that you specified the appropriate SSL ports and URLs when prompted. If this is not the case, refer to "(Optional) Manually Configure TCM" on page 71 for information on how to update the appropriate configuration files.

FileNet TCM supports the following methods of configuring an SSL environment:

- Full SSL support - A single-TCM server, where all of the software is running under SSL.
- One server SSL redirect - One server setup to redirect logon attempts on the non-SSL port to the SSL port.
- Two server SSL redirect - Two TCM servers, where one is SSL-enabled, and the other redirects users to the SSL-enabled TCM server to log on.

To set up full SSL support on a single TCM server

1. Enable full SSL support on the TCM Application server (see your application server vendor SSL documentation).
2. Test the SSL connection by signing in to the TCM server using one of the following URLs:
   - `https://<server_name>:<SSL port>/TCM`

     The SSL-enabled host will handle the entire session.
   - `https://<IP_address>:<SSL port>/TCM`

     The entire session will be handled by the SSL-enabled host.

To set up SSL redirect on one TCM server

1. Enable SSL on the TCM Application server (see your application server vendor SSL documentation).
2. Stop the TCM Application, if running.
3. Open the file ***<TCM_install_path>*/WEB-INF/config.properties**.

   Look for the following line:

   ```
   sslInfo=
   ```

   Replace it with host name and port of the SSL enabled server:

   ```
   sslInfo=<SSL host>:<SSL port>
   ```

   CAUTION Do not add the protocol part of the URL.

   NOTES

   The host name can be either the full server name or the IP address of the server and must be resolvable by the client.

   For a list of default port numbers, see "FileNet TCM Port Numbers" on page 90.
4. Start the TCM Application.
5. Test the SSL connection by signing in to the TCM server using the following URL:

   `http://<TCM_server>:<port>/TCM`

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 off), and then TCM will display.

To set up SSL redirect on two TCM servers

1. Install the TCM Application on both computers so that both use the same config.properties file, see "Sharing the config.properties file among multiple TCM Applications" on page 77.
2. Enable SSL on the TCM server that you will be using as the SSL-enabled host (see your SSL documentation).
3. Log on to the non-SSL enabled TCM server.
4. Stop the application server, if running.
5. Open the file **<*TCM_install_path*>/WEB-INF/config.properties**.

   Look for the following line:

   ```
   sslInfo=
   ```

   Replace it with host name and port of the SSL enabled server:

   ```
   sslInfo=<SSL host>:<SSL port>
   ```

   CAUTION Do not add the protocol part of the URL.

   NOTES

   The host name can be either the full server name or the IP address of the SSL enabled server and must be resolvable by the client.

   For a list of default port numbers, see "FileNet TCM Port Numbers" on page 90.
6. Start the application server and launch the TCM Application.
7. Test the SSL connection by signing in to the TCM server using the following URL:

   ```
   http://<TCM_server>:<port>/TCM
   ```

   You will be redirected to the SSL-enabled host for sign in, then back to the non-SSL enabled computer 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 off), and then TCM will display.

Software Reconfiguration and Removal Tasks

Follow the instructions below to remove the Team Collaboration Manager components from your FileNet P8 Environment. To reconfigure your TCM installation, follow the instructions in "(Optional) Manually Configure TCM" on page 71.

NOTE On systems where two or more TCM components are collocated, running the uninstaller will result in all TCM components being removed from the server.

Content Engine Integration

To remove Content Engine Integration

1. Log on to the Content Engine server as a user with Administrative rights.
2. Use Add/Remove Programs from the Control Panel to remove FileNet Team Collaboration Manager.
3. Delete the Collaboration folder under the ***<TCM_install_path>*/FileNet** folder.

Collaboration Engine

(UNIX only) To prevent the Collaboration Service daemon from starting at boot

NOTE This step is only required if you have previously set up the Collaboration Engine service to automatically restart upon reboot. For more information, see "(UNIX only) Configure Collaboration Engine and Collaboration Mail Server daemons to automatically restart on reboot" on page 79.

1. Login to the Collaboration Engine server as root.
2. Run the ConfigureStartOnReboot.sh script.
   a. Navigate to:

      ***<TCM_install_path>*/FileNet/Collaboration/ManagementService/bin**

   b. Run the script to unregister the service.

      ```
      ./ConfigureStartOnReboot.sh unregister
      ```

To remove the Collaboration Engine

1. Log on to the Collaboration Engine server as a user with Administrative rights.
2. Navigate to the **_uninst** folder under the Collaboration Engine installation location.
   - UNIX - **/opt/**
   - Windows - **C:\Program Files**
3. Run the uninstall program:
   - UNIX - ***<Platform>*_filenet_TCM_uninstall.bin**
   - Windows - **Win32_filenet_TCM_uninstall.exe**

   NOTE For Windows, you can also use Add/Remove Programs from the Control Panel to remove FileNet Team Collaboration Manager.

4. If you have more than one FileNet component installed on the server, delete the Collaboration folder under the ***<TCM_install_path>*/FileNet** folder; if Collaboration Engine is the only FileNet component on your server, delete the FileNet folder.

TCM Application

To remove the TCM Application

1. Log on to the TCM Application server as a user with Administrative rights.
2. Undeploy the TCM Application.

   Follow the instructions provided by your application server vendor to undeploy the TCM Application.
3. Navigate to the **_uninst** folder under the Collaboration Engine installation location.
   - UNIX - **/opt/**
   - Windows - **C:\Program Files**
4. Run the uninstall program:
   - UNIX - ***<Platform>*_filenet_TCM_uninstall.bin**
   - Windows - **Win32_filenet_TCM_uninstall.exe**

   NOTE For Windows, you can also use Add/Remove Programs from the Control Panel to remove FileNet Team Collaboration Manager.
5. If you have more than one FileNet component installed on the server, delete the Collaboration folder under the ***<TCM_install_path>*/FileNet** folder; if the TCM Application is the only FileNet component on your server, delete the FileNet folder.

Collaboration Mail Server

(UNIX only) To unregister the Collaboration Service daemon from starting at boot

NOTE This step is only required if you have previously set up the Collaboration Mail Server service to automatically restart upon reboot. For more information, see "(UNIX only) Configure Collaboration Engine and Collaboration Mail Server daemons to automatically restart on reboot" on page 79.

1. Login to the Collaboration Engine server as root.
2. Run the ConfigureStartOnReboot.sh script.
   a. Navigate to:

      ***<TCM_install_path>*/FileNet/Collaboration/JamesMailServer/bin**

   b. Run the script to unregister the service.

      ```
      ./ConfigureStartOnReboot.sh unregister
      ```

To remove the Collaboration Mail Server

1. Log on to the Collaboration Mail Server server as a user with Administrative rights.

2. Navigate to the **_uninst** folder under the Collaboration Engine installation location.
   - UNIX - **/opt/**
   - Windows - **C:\Program Files**
3. Run the uninstall program:
   - UNIX - ***<Platform>*_filenet_TCM_uninstall.bin**
   - Windows - **Win32_filenet_TCM_uninstall.exe**

   NOTE For Windows, you can also use Add/Remove Programs from the Control Panel to remove FileNet Team Collaboration Manager.
4. If you have more than one FileNet component installed on the server, delete the Collaboration folder under the ***<TCM_install_path>*/FileNet** folder; if Collaboration Mail Server is the only FileNet component on your server, delete the FileNet folder.

Workflow Integration/Application Engine

To remove Workflow integration module

1. Log on to the Application Engine server as a user with Administrative rights.
2. Navigate to the **_uninst** folder under the Collaboration Engine installation location.
   - UNIX - **/opt/**
   - Windows - **C:\Program Files**
3. Run the uninstall program:
   - UNIX - ***<Platform>*_filenet_TCM_uninstall.bin**
   - Windows - **Win32_filenet_TCM_uninstall.exe**

   NOTE For Windows, you can also use Add/Remove Programs from the Control Panel to remove FileNet Team Collaboration Manager.
4. Delete the Collaboration folder under the ***<TCM_install_path>*/FileNet** folder.

Appendixes

This appendixes section contains the following major topics:

- "(HP-UX only) Enable Java Service Wrapper" on page 88.
- "FileNet TCM Port Numbers" on page 90.

(HP-UX only) Enable Java Service Wrapper

To enable the Java Service Wrapper to work on HP-UX on the Collaboration Engine and Collaboration Mail Server, you must install the Binutils 2.15 and GCC 3.4.3 packages on those servers, and create a symbolic link between the directory holding the libgcc_s.sl file (from the GNU Compiler Collection (GCC)) and the /sww/lib directory.

NOTE These steps must be taken before you install the TCM 3.5.0 Collaboration Engine and Collaboration Mail Server.

To install Binutils and GCC

CAUTION You must first install Binutils, and then GCC.

1. (On each server) Check to see if the packages are already installed.
   a. Open a terminal window.
   b. Use the following command to verify the existence of the package:

      ```
      # swlist <Package name>
      ```

      where:

      <Package name> is the name of the package you are installing (binutils or gcc)

      Example: If GCC is installed, the command swlist gcc* returns:

      ```
      # Initializing...
      # Contacting target "hq-cfghp8"...
      #
      # Target: hq-cfghp8:/
      #
      # gcc 3.4.3
      gcc.gcc
      ```

   c. If the packages are already installed, no further actions are required; proceed with "Installation Tasks" on page 23.
2. (If the packages are not installed) Downloaded Binutils and GCC to the server(s) on which you are planning to install Collaboration Engine and Collaboration Mail Server.

   The following web site contains the install packages:

   http://h21007.www2.hp.com/dspp/tech/tech_TechSoftwareDetailPage_IDX/1,1703,547,00.html

   Packages:

   - HP-UX 11i v1 (PA-RISC) binutils 2.15
   - HP-UX 11i v1 (PA-RISC) GCC 3.4.3
3. (On each server) Install the packages.

   CAUTION You must first install Binutils, and then GCC.

   a. Open a terminal window.
   b. Use the following command to install the package:

      ```
      # swinstall -s <System name>:<Package path>/<Package name>.depot
      ```

Where:

<*System name*> is the name of your HP-UX server.

<*Package path*> is the path to the location where you downloaded the package.

<*Package name*> is the name of the package you are installing (binutils or gcc)

4. (On each server) Create the symbolic link.
   a. If it doesn't exist, create a /sww/bin directory:

      ```
      # mkdir -p /sww/bin
      ```

   b. Create a symbolic link to /usr/local/lib:

      ```
      # ln -s /usr/local/lib /sww/lib
      ```

FileNet TCM Port Numbers

The table below lists the port numbers used by the TCM components. For a complete list of the FileNet P8 port numbers, see FileNet P8 Port Numbers in the *FileNet P8 3.5.0 Platform Installation and Upgrade Guide*,

TCM Ports	
Clients / SSL	80 / 443
WebSphere / WebSphere SSL	9080 / 443
WebLogic / WebLogic SSL	7001 / 7002
JBoss / JBoss SSL	8080 / 8443
Tomcat / Tomcat SSL	8080 / 8443
Collaboration Mail Server	25 110 (Pop3)

Index

C

Collaboration Applications.xml 29
Collaboration Engine
  install 59
  remove 84
Collaboration Enterprise Security Definitions.xml 27
Collaboration Mail Server
  install 64
  remove 85
collocate 7
configuration/startup tasks 69
configure
  Collaboration Applications.xml 29
  Collaboration Enterprise Security Definitions.xml 27
  email notification 18
  manual 71
  manually 12
  Object store security 26
  share config.properties among multiple TCM Applications 77
  symmetric encryption 19
  tasks 69
Content Engine
  CryptoKeyFile.properties location 21
  prepare 24
Content Engine Components
  remove 84
Content Engine GCD Administrator
  log in as 24
create cryptographic key 21
CryptoKeyFile.properties 19
custom installation 7

D

documentation
  install 15
  Install TCM
    WebSphere 38
  update the search index 16

E

email notification 18
encryption tool 71

F

FileNet P8 Platform documentation 15

H

high availability 13

I

install
  Collaboration Engine 59
  Collaboration Mail Server 64
  custom 7
  deploy TCM Application on WebLogic 46
  documentation 15
  TCM Application 31

M

manual configuration 71
Manually configure TCM 12

O

Object store
  full text indexing 27
  security 26

P

passwords 71
port numbers
  required 13
  TCM default 90
prepare
  Content Engine 24
  Process Engine 18
prerequisite tasks 14
Process Engine
  prepare 18

R

remove
  Collaboration Engine 84
  Collaboration Mail Server 85
  Content Engine Components 84
  software 84
  TCM Application 85
required port numbers 13

S

security
  security roles 8
security roles 8
share configuration files 77
SSL

setup SSL security 82
start TCM 78
symmetric encryption
configure 19
create cryptographic key 21
CryptoKeyFile.properties 19
CryptoKeyFile.properties Content Engine location 21
password encryption 71
TCMCryptoKeyFile.properties 19
unlimited strength .jars 70
UTCryptoKeyFile.properties 19

T

TCM Application
deploy on WebLogic 46
install 31
remove 85
TCM default ports 90
TCMCryptoKeyFile.properties 19

U

Unlimited strength encryption
symmetric encryption 70
user name display setting 12
User Token
Crypto key file path
WebLogic 34, 35, 61, 66
UTCryptoKeyFile.properties 19
UTF- 8 encoding
WebSphere 49

V

virtual host configuration
WebSphere TCM deployment 50

W

web server plug-in
regenerate, WebSphere TCM deployment 50
Web Sphere
UTF-8 encoding 49
WebLogic
deploy TCM Application 46
WebSphere
regenerate web server plug-in 50
virtual host configuration 50