FileNet Team Collaboration Manager

Installation Guide

Release 3.0.0

December 2004

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 Notices in the FileNet P8 online documentation.

Table of Contents

Table of Contents . . . 3

About the Installation Guide . . . 4

Planning . . . 5
- Installation Planning Considerations . . . 5
- General Requirements for all FileNet P8 Systems . . . 5
- P8 Platform Considerations . . . 6
- TCM and high availability . . . 6
- Content Engine . . . 6
- TCM Application server . . . 7
- Mail Server . . . 7
- TCM roles and security . . . 7
- Assigning users/groups for TCM security . . . 7
- Installation Permissions . . . 12
- Network Security Considerations . . . 12
- Authentication Security Considerations . . . 13
- Using the custom installation option . . . 13

Prerequisite Tasks . . . 14
- Install TCM documentation . . . 15
- Prepare Content Engine for TCM . . . 18
- Prepare Process Engine for TCM . . . 25
- Configure Symmetric Encryption . . . 26

Installation Tasks . . . 30
- Install the TCM Application . . . 31
- Deploy the TCM Application (WebLogic) . . . 35
- Install the Collaboration Engine . . . 36
- Install the Mail Server . . . 39

Configuration/Startup Tasks . . . 42
- Install unlimited strength .jar files . . . 43
- (Optional) Manually Configure TCM . . . 44
- (Optional) Setup TCM SSL security . . . 50
- Start Team Collaboration Manager . . . 53
- Configure Workflow for TCM use . . . 54

Software Reconfiguration and Removal Tasks . . . 58

FileNet TCM Port Numbers . . . 60

Index . . . 61

About the Installation Guide

The FileNet P8 Team Collaboration Manager Installation Guide is provided in Adobe Portable Document Format (PDF). If you do not have the Adobe Reader installed, download it from Adobe's web site (http://www.adobe.com). You can view this guide online, or you can print it.

If you view this guide using Adobe Reader, you can use the following search and navigation features to help you find information quickly:

- Adobe Acrobat Reader's Search tool that retrieves information based on your search criteria.
- Links to reference topics and procedures.

Most links display an Installation Guide topic in the same PDF file. In some cases, a link displays a topic in the FileNet P8 Platform help system, or on the FileNet Customer Support website. To continue viewing the PDF file, switch your active application back to Adobe Reader.

Planning

Before you begin to install FileNet Team Collaboration Manager (TCM):

- Verify that your FileNet P8 Platform environment has been successfully installed and configured for content and workflow management.

  NOTE In addition to this you must configure Process Engine email notification for use by TCM, see "Prepare Process Engine for TCM" on page 25. This is an optional task during the FileNet P8 Platform installation.

- Retrieve updates to FileNet P8 documentation, TCM documentation, and software from the FileNet Worldwide Customer Support web site (http://www.css.filenet.com).

- Review the "Installation Planning Considerations" on page 5 for a list of auxiliary documentation you should gather and a list of the tasks you should perform before installing FileNet TCM software.

- Read the "Prerequisite Tasks" on page 14, "Installation Tasks" on page 30, and "Configuration/Startup Tasks" on page 42 to become familiar with the tasks you will perform when setting up your FileNet TCM software.

Installation Planning Considerations

This section lists details that will help you prepare your environment for the installation of 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 P8 TCM or required third-party software.

IMPORTANT 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.

General Requirements for all FileNet P8 Systems

Gather auxiliary documentation

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

- FileNet P8 Platform Release Notes. This document provides details on new features, known issues, and resolved problems.
- FileNet P8 Platform Installation Guide This document contains the installation instructions for the FileNet P8 platform, and is referenced from this document.
- FileNet P8 3.0.0 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 P8 Platform Installation Guide assumes you have met all applicable requirements listed in that document.

- FileNet P8 Platform user and group security help found at: 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 Platform Security Questionnaire. This document provides a list of security-related questions that, when answered by 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 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. In so doing, the document also provides related disaster recovery information.
- FileNet P8 Performance Tuning Technical Notice. This document provides recommended configuration changes that can be applied to improve the performance and stability of the various components of the P8 system. These settings have proven beneficial in FileNet's performance test lab.

P8 Platform Considerations

Manually Configure TCM

You can run the installer using the default information provided by the installer. By clicking your way through the installer, you will install a "default" version of the TCM components on your servers. After installing, but before launching TCM, you must manually configure the components. For more information, see "(Optional) Manually Configure TCM" on page 44.

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 Process Engine > Process Task Manager > Process Service > Configuring Process Service > Configuring the LDAP connection > Advanced properties.

Also see *To create a new FileNet P8 domain* on pages 64 or 71 in the *P8 Platform Installation Guide*,.

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 3.0.0 High Availability Technical Notice available from the FileNet Worldwide Customer Support web site (http://www.css.filenet.com).

Content Engine

Enabling DTC and COM+ access

(Windows 2003 only) Verify that Content Engine is configured to support installation of P8 Add-ons by enabling DTC and COM+ access. For more information, see *FileNet P8 Platform Installation Guide*, Task 3: Configure Content Engine and SQL Servers for Windows 2003.

Running the TCM installer multiple times

If you run and complete the TCM Installer to add the Content Engine Integration on the Content Engine more than once, the **CIbCEEventHandler.dll** will fail to register properly. This will cause the Object Store creation to fail when using the TeamCollaborationManagerAddOns.

Before you run the TCM installer to add the Content Engine Integration on a Content Engine for the second or consecutive time you must manually unregister the **CIbCEEventHandler.dll**. For more information on how to unregister the .dll, see your Windows documentation.

TCM Application server

Verify that you the server where you plan to install the TCM Application has a WebLogic application server with a WebLogic domain.

Mail Server

If the server you are installing Mail Server on is running IIS, and it is set up to listen on the same port you select for the Mail server, make sure the Simple Mail Transport Protocol (SMTP) service is stopped and disabled. The Mail server uses port 25 (default). For more information see "SMTP port" on page 41 and "FileNet TCM Port Numbers" on page 60.

The Mail Server uses port 110 (pop3). Do not collocate the Mail Server with any other application that uses this port.

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 what objects they can create or modify.

Before you employ TCM in a production environment or where sensitive data may be exchanged, be sure to review the sections on Security carefully. Then create your own security roles for the different types of users that you anticipate.

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

Assigning users/groups for TCM security

In addition to the TCM roles discussed above, you have to assign TCM security on a number of folders in the Collaboration object store, assign permissions for non-TCM users to have access to teamspace objects, and assign (or create) specific users to run the Collaboration Engine, Mail Server, and Workflow integration.

NOTE The Collaboration Engine, Mail Server, and JAAS user can be the same user. This can be any existing user, or you can create a dedicated user for this purpose.

You do not have to create any new users to install and run TCM, all assignments below can be performed with existing users. For more detailed information about the users listed below, see the table "Summary of required user assignments for TCM" on page 9.

1. Users assigned during Collaboration object store creation.

   You will assign the following users/groups when you create the Collaboration object store.

   - Initial object store Administrator account(s)
   - Object store Users account(s)

   For more information, see "Specify the Collaboration Object Store administrator." on page 19.

2. Users assigned using the security script.

   You will run a security script when you configure the Collaboration object store. This script defines two sets of enterprise users and their permissions on the Collaboration object store.

   - Collaboration Administrators
   - Collaboration Users

   For more information, see "Set Collaboration Administrators." on page 20 and "Set Collaboration Users." on page 20.

3. Users assigned in the CollaborationEngineSecurityDefinition.xml file.

   Add domain users that should have access to the teamspace objects regardless of if they are members of the teamspace or not. The CollaborationEngineSecurityDefinition.xml file contains security settings for all objects created in all Teamspaces.

   The file contains two sections, each controlling one folder and its content.

   - Users with <required-teamspace-security>
   - Users with <required-teamspace-template-security>

   For more information, see "Update the Collaboration Enterprise Security Definitions.xml file." on page 22.

4. Users assigned when running the installer.

   You will assign these component users when you run the installer on the TCM servers. You can use the same user for all components, or have separate users for each component.

   - <*Collaboration Engine user*>
   - <*Mail Server user*>
   - <*JAAS User*>

   For more information, see "Configure the Collaboration Engine." on page 37, "Configure Mail Server." on page 40, and "Enter JAAS (Java Authentication and Authorization Service) Credentials." on page 55 respectively. In addition, see "(Optional) Manually Configure TCM" on page 44

Summary of required user assignments for TCM

Role/Tasks/Account	Description
Initial object store Administrator account(s) Assigned during object store creation.	The user or group added as the object store administrator has full control of all folders and objects in the object store. Add the FileNet P8 Domain groups and users that should have administrative access to the Collaboration object store. **IMPORTANT** To successfully configure TCM you have to be an Object store administrator for the Collaboration object store. Only members of the Initial object store Administrator accounts have access to the Collaboration Store folder and the configuration files therein. **NOTE** For the Object store administrator users to have access to Teamspaces and their sub-folders you have to add the administrator users to the Collaboration Administrators set below and to the <required-teamspace-security> with view or sysadmin-rights.
Object store Users account(s) Assigned during object store creation.	Add the FileNet P8 Domain groups that are likely to need basic non-administrative access to the object store.
(Collaboration Administrators) Assigned when running the security script on the Collaboration object store.	Add the users(s) you have selected to run the Collaboration Engine, the Mail Server, and the JAAS user to Collaboration Administrators. Collaboration Administrators have security rights set to be able to work with TCM on the following folders and their subfolders: • Teamspaces - To be able to work with the teamspaces the user is assigned to. • Collaboration Store/Teamspace Templates - To create and use teamspace templates. • Collaboration Store/Meeting Connection Templates/WebEx Online Meeting - To be able to connect to a WebEx conference. In addition Collaboration Administrators have class permissions needed to successfully run Collaboration Engine.

Role/Tasks/Account	Description
(Collaboration Users) Assigned when running the security script on the Collaboration object store.	Add all enterprise users that will be using TCM to Collaboration Users to provide them with the necessary permissions to create teamspaces and participate in teamspace activities Collaboration Users have security rights set to be able to work with TCM on the following folders and their subfolders: • Teamspaces - To be able to work with the teamspaces the user is assigned to. • Collaboration Store/Teamspace Templates - To create and use teamspace templates. • Collaboration Store/Meeting Connection Templates/WebEx Online Meeting - To be able to connect to a WebEx conference.
(User with <required-teamspace-security>) Assigned when modifying the Collaboration Enterprise Security Definitions.xml file.	The users/groups you add to this section will have permissions set on all objects in the Teamspaces folder and subfolders according to the accesalias you give them, see accessalias for more information. **IMPORTANT** The users(s) you have selected to run the Collaboration Engine, the Mail Server, and the JAAS user all have to be added to this section with sysadmin-rights
(User with <required-teamspace-template-security>) Assigned when modifying the Collaboration Enterprise Security Definitions.xml file.	The users/groups you add to this section will have permissions set on all objects in the Teamspace Templates folder according to the accesalias you give them, see accessalias for more information.
<*Collaboration Engine user*> Assigned when running the installer.	This user runs the Collaboration Engine processes, and is used to access the necessary objects and configuration files on the Content Engine. The <*Collaboration Engine User*> can be any existing user, or you can create a dedicated Collaboration Engine user for this purpose. This user can be the same as the <*Mail Server user*> and the <*JAAS user*>. To have the correct permissions set on the Collaboration object store the user selected must: • Belong to Collaboration Administrators. • Be added to the <required-teamspace-security> with sysadmin-rights.

Role/Tasks/Account	Description
<Mail Server user> Assigned when running the installer.	This user runs the Mail Engine processes, and is used to access the necessary objects and configuration files on the Content Engine. The *<Mail Server User>* can be any existing user, or you can create a dedicated Mail Server user for this purpose. This user can be the same as the *<Collaboration Engine user>* and the *<JAAS user>*. To have the correct permissions set on the Collaboration object store the user selected must: • Belong to Collaboration Administrators. • Be added to the <required-teamspace-security> with sysadmin-rights.
<JAAS user> Assigned when running the installer.	This user is used to access the component queues on the Process Engine, and needs to have access the necessary objects and configuration files on the Content Engine. The *<JAAS User>* can be any existing user, or you can create a dedicated JAAS user for this purpose. This user can be the same as the *<Collaboration Engine user>* and the *<Mail Engine user>*. To have the correct permissions set on the Collaboration object store the user selected must: • Belong to Collaboration Administrators. • Be added to the <required-teamspace-security> with sysadmin-rights. • Have system administrator rights on the Process Engine. • Has Content Engine GCD Administrator rights on the Collaboration object store. For more information about this type of user, see *Task 4: Create groups and users required for FileNet P8 installation*, in the FileNet P8 Platform Installation Guide . • Have Query & Process access to the component queue, as defined in the Process Configuration Console.

Installation Permissions

Content Engine

To install and configure the TCM components on the Content Engine you must log in as a user with Content Engine GCD Administrator permissions. For more information about this type of user, see *Task 4: Create groups and users required for FileNet P8 installation*, in the FileNet P8 Platform Installation Guide .

IMPORTANT (Installing in a non-Active Directory environment.) If your FileNet P8 environment uses a directory service other than Active Directory you will not be able to log in locally as the GCD Administrator user as required to complete Task 2: Prepare Content Engine for TCM. Instead, log in as a local administrator. The installer will prompt you for the GCD Administrator username and password, see Step 7 “(Non-Active Directory FileNet P8 environments only) Provide the GCD Administrator user information.” on page 18.

To check GCD permissions:

1. On the Content Engine, launch FileNet Enterprise Manager.
2. Right-click on the **root domain**.
3. From Enterprise Manager Domain Root Properties, select the **Security** tab.
4. Verify that the user you plan to use to install the Content Engine Components has Full control of the root domain.

TCM Application server

To install the TCM Application you must log in as a user with permission to read and write to the directory where you plan to install TCM.

To deploy the TCM Application you must use the application server administrative account.

Collaboration Engine and Mail Server

To install Mail Server and Collaboration Engine you must log in as a user with permission to read and write to the directory where you plan to install TCM.

To configure Mail Server and Collaboration Engine you will need the user name and password of a Collaboration Administrator user, see “Set Collaboration Administrators.” on page 20.

Application Engine (Workflow configuration)

To configure Workflow on the Application Engine server you need the user name and password of a Collaboration Administrator user, see “Set Collaboration Administrators.” on page 20.

In addition to this you must log in to Workplace as a user with access to the Process Configuration Console in the Admin tab.

Network Security Considerations

- Verify TCP/IP configuration settings on all UNIX and Windows servers and FileNet Enterprise Manager clients.

- Several port numbers are required by FileNet P8 components. For a composite list, see "FileNet TCM Port Numbers" on page 60 and *FileNet Port Numbers* in the FileNet P8 Platform Installation Guide .
- Verify that you can access all other FileNet P8 servers and TCM servers from the server you are currently installing on.

Authentication Security Considerations

Symmetric Encryption

Verify that you have copies of the CryptoKeyfile.properties file (optional) and the UTCryptoKeyFile.properties file (required) from the Application Engine server. These files are used to configure symmetric encryption for the TCM system. See "Configure Symmetric Encryption" on page 26 for more information.

Maximum Strength Cryptographic Keys

If you are using JDK 1.4 and use maximum strength cryptographic keys you must install unlimited strength .jar files after you have run the installer.

You need to install the unlimited strength jar files if:

- You are using JDK 1.4 or higher.
- Either of the following files contain maximum strength cryptographic keys:
  - CryptoKeyFile.properties
  - UTCryptoKeyFile.properties
  - TCMCryptoKeyFile.properties.

    IMPORTANT As the installer encrypts passwords on the Mail Server and Collaboration Engine servers using the TCM cryptographic keys, you must manually encrypt the passwords post installation. For more information, see "Install unlimited strength .jar files" on page 43, "Collaboration Engine Configuration" on page 47, and "Mail Server Configuration" on page 48.

Using the custom installation option

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

Prerequisite Tasks

To set up and configure prerequisite software for TCM components

1. Install TCM documentation. Do Task 1 on page 15.
2. Prepare Content Engine for TCM. Do Task 2 on page 18.
3. Prepare Process Engine for TCM. Do Task 3 on page 25.
4. Configure Symmetric Encryption. Do Task 4 on page 26.

Task 1: Install TCM documentation

IMPORTANT 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 contents). 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 3.0.0 documentation installed on your application server. See the FileNet P8 Platform Installation Guide for more information.
2. Refer to your 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. Here's an example on a WebLogic server: **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 3.0.0 of the FileNet P8 Platform documentation.
   - During the copy, some FileNet TCM documentation files will overwrite existing files.
   - If you later install a version of the FileNet P8 Platform documentation that is newer than **3.0.0**, you must refresh the TCM documentation on the application server.
4. 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.
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.

IMPORTANT NOTES:

- If you're installing more than one FileNet P8 functional expansion, update the search 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.
- To update the Help Search index, you must specify the path to the JRE installation on the application server where you intend to install the FileNet P8 Help.
- 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).

To update the Help Search index

indexFiles.bat is a script that launches the Java-based indexer (indexFiles.sh for UNIX-based systems).

The script is located in this directory: **ecm_help/search.**

If you have already deployed or installed this 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, then stop WebSphere. Next, copy the files to the deployed location, update the search, and then restart WebSphere.

1. Ensure that you have copied the FileNet P8 Platform help and all your functional expansions to a designated application server.

   NOTE 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. Ignore the messages and allow the overwrites to occur. By doing so the actual functional expansion help files will replace the placeholder files.

2. Open a command prompt on the application server.
3. From the command line, navigate to the **search** subdirectory under your **ecm_help** root directory.
4. Using a text editor, open the search-indexing script file that is appropriate to your application server operating system:

   indexFiles.bat (Windows)

   indexFiles.sh (UNIX)

5. 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)

6. Save your changes and close the text editor.
7. Run the updated search-indexing script file.
8. By default, the script backs up the existing index files to **indexOld**, and then re-indexes all the help files starting from the root **ecm_help** directory, and writes the index to this directory:

   ecm_help/search/index/core.

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 Content Engine for TCM

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

IMPORTANT If you run and complete the TCM Installer to add the Content Engine Integration on the Content Engine more than once, the ClbCEEventHandler.dll will fail to register properly. This will cause the Object Store creation to fail when using the TeamCollaborationManagerAddOns.

Before you run the TCM installer to add the Content Engine Integration on a Content Engine for the second or consecutive time you must manually unregister the ClbCEEventHandler.dll. For more information on how to unregister the .dll, see your Windows documentation.

To prepare Content Engine for Team Collaboration Manager

1. Log in to the Content Engine as a user with Content Engine GCD Administrator privileges (see "Content Engine" on page 6) and read/write privileges on the Content Engine installation folder.

   IMPORTANT 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 username and password when running the installer, see Step 7 "(Non-Active Directory FileNet P8 environments only) Provide the GCD Administrator user information." on page 18.

2. Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, run the TCM installer Win32_filenet_TCM_setup.exe from the CD.

   NOTE There will be a slight delay after the initial InstallShield Wizard startup window closes before the Team Collaboration Manager Installer window appears.

3. Accept the license agreement. Click **Next**.

4. Accept the default installation location or select a directory to install TCM.

   In the Directory Name field, type the path to the installation directory, or browse to select one.

   NOTE The installation location, ***<TCM_install_path>***, is the directory where the installer will add the TCM source files. The directory must exist prior to installation, the installer will not create a directory for you.

5. Choose setup type.

   Select Content Engine Integration, and click **Next**.

6. Read the summary and click **Next** to install the Content Engine Integration.

7. (Non-Active Directory FileNet P8 environments only) Provide the GCD Administrator user information.

   a. Enter the GCD Administrator username, and click **OK**.

   b. Enter the GCD Administrator password, and click **OK**.

8. Click **Finish** to exit the installer.

9. Verify that the installation was successful.

   The following file should contain no errors.

   ***<TCM_install_path>*/FileNet/TCM_install_log_30.txt**

10. Create a Collaboration Object Store.

    Follow these instructions to create a basic object store for TCM use.

For more information, go to the *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Content Engine Administration > Content Engine Wizard Help > Create Object Store.

a. Launch FileNet Enterprise manager.

b. In the left pane, right-click **Object Stores** and select **New Object Store**.

c. Read the welcome screen, and click **Next**.

d. Give the Collaboration Object Store a Display Name, and click **Next**.

e. Select a SQL or Oracle database (for Oracle type the Database alias), and click **Next**.

f. Select Win2000 authentication or specify your Database engine information, click **Next**.

g. Select Create a New Database, and click **Next**.

h. Select Database Store or File Store, and click **Next**.

i. (File Store only) Select **Local** or **Remote Server** and click **Browse**.

j. (File Store only) Browse to the drive where you want to create the File Store and click **New Folder**.

k. (File Store only) Enter a folder name, and click **OK**.

l. (File Store only) Click **Yes** to share the folder, click **OK**.

m. (File Store only) Click **Next**.

n. (File Store only) If you want to create a Fixed File Store, check the box, and select Default Retention Period. Click **Next**.

   For more information, go to the *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Content Engine Administration > Content stores > Fixed file stores.

o. Specify the Collaboration Object Store administrator.

   Add the FileNet P8 Domain groups and users that should have administrative access to the Collaboration object store. For more information, see “Users assigned during Collaboration object store creation.” on page 8.

   i. Click **Add**.

   ii. On Select Users and Groups dialog, click **Find**.

   iii. Select the user or group you want to add, and click **OK**.

   iv. Repeat these steps for each administrative user/group you want to add.

p. Click **Next**.

q. Specify Initial User Groups.

   Add the FileNet P8 Domain groups that are likely to need basic non-administrative access to the object store. For more information, see “Users assigned during Collaboration object store creation.” on page 8.

   i. Click **Add**.

   ii. On Select Users and Groups dialog, click **Find**.

   iii. Select the group you want to add, and click **OK**.

   iv. Repeat these steps for each initial group you want to add.

r. Click **Next**.

s. Click **Advanced**.

t. The Auto Install Components dialog displays. Check the three components listed below, and click **OK**.

- TeamCollaborationManagerAddOn
- TeamCollaborationManagerAddOn2
- TeamCollaborationManagerAddOn3

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

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

11. Configure Collaboration Object Store security

After creating the Collaboration Object Store the security settings of several TCM-specific folders need to be modified as follows:

a. Launch FileNet Enterprise Manager.

b. Right-click the Collaboration Object Store you created in Step 10 on page 18.

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: **<*TCM_install_path*>/FileNet/Content Engine**.

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

h. Click **Next**.

i. Set Collaboration Administrators.

Add the users(s) you have selected to run the Collaboration Engine, the Mail Server, and the JAAS user to Collaboration Administrators. For more information, see "Users assigned using the security script." on page 8.

i. In the left pane of the Security Roles screen, select **Collaboration Administrators**.

ii. Click **Add**.

iii. On the Select Users and Groups screen, find and add all users and/or groups you want.

iv. Click **OK**.

NOTES

A Collaboration Administrator user must be used when configuring Collaboration Engine, Mail Server, and Workflow Integration. For more information, see "Configure the Collaboration Engine." on page 37, "Configure Mail Server." on page 40, and "Enter JAAS (Java Authentication and Authorization Service) Credentials." on page 55 respectively.

j. Set Collaboration Users.

Add all enterprise users that will be using TCM to Collaboration Users to provide them with the necessary permissions to create teamspaces and participate in teamspace activities. For more information, see "Users assigned using the security script." on page 8.

i. In the left pane of the Security Roles screen, select **Collaboration Users**.

ii. Click **Add**.

iii. On the Select Users and Groups screen, find and add all users and/or groups you want.

iv. Click **OK**.

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

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

12. Configure Full Text Indexing on the Collaboration Object Store.

a. (If you are using a Database Object Store) Create a File Store in the Collaboration Object Store

i. In FileNet Enterprise Manager, expand the Collaboration Object Store you just created, (see "Create a Collaboration Object Store." on page 18) right-click the File Stores folder, and select **New File Store**.

ii. Read the welcome screen, and click **Next**.

iii. Enter a display name for the File Store, and click **Next**.

iv. Select **Local** or **Remote Server** and click **Browse**.

v. Browse to the drive where you want to create the File Store and click **New Folder**.

vi. Enter a folder name, and click **OK**.

vii. Click **Yes** to share the folder, click **OK**.

viii. Click **Next**.

ix. If you want to create a Fixed File Store, check the box, and set the Default Retention Period. Click **Next**. For more information, go to the *Documentation for FileNet P8 Platform* help and navigate to FileNet P8 Administration > Content Engine Administration > Content stores > Fixed file stores.

x. Click **Finish**.

xi. Click **OK**.

b. Right-click the Collaboration Object Store.

c. Select **All tasks > Configure Full Text Indexing**.

d. Select **Task Menu > Create Filestore Indexes**.

e. Select two (2) indexes.

f. Select locale (en-us English/en-usx EnglishX).

g. Click **Create Indexes**.

h. Verify the message *Finished creating indexes successfully* displays, then click **Close**.

i. Select **Task Menu > Create Database Indexes**.

j. Specify two (2) indexes, click **Create Indexes**.

k. Click **Close**.

l. Select **Task Menu > Property Level Indexing**.

m. Double-click on the following recommended minimum set of Indexable properties to enable them:

- **Class Definitions > Document > Indexable Properties > *Document Title***
- **Class Definitions > Document > Subclasses > Collaboration Document > Subclasses > Collaboration Task > Indexable Properties > *Collaboration Description***
- **Class Definitions > Document > Subclasses > Collaboration Document > Subclasses > Collaboration Meeting Proxy Document > Indexable Properties > *Agenda***

n. Click **Apply Changes**.

o. Click **Close**.

p. To start indexing, click **Yes**.

q. Click **OK**.

r. Click **Close**.

For more information, go to *Documentation for FileNet P8 Platform* help; navigate to Functional Expansions > Team Collaboration Manager> Configuration > Configuring CBR to support searching the TCM application.

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

13. Update the Collaboration Enterprise Security Definitions.xml file.

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

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 desktop.

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

e. Update the users/groups under <required-teamspace-security>.

For more information, see "Users assigned in the CollaborationEngineSecurityDefinition.xml file." on page 8.

The users/groups added here will have access to all teamspace objects regardless of if they are members of the teamspace or not. The level of access is set by the <accessalias> tag.

Find the <required-teamspace-security> field, and append the following lines for each user/group you want to add.

```
<enterprise-subject>
    <name><name></name>
    <type><type></type>
    <accessalias><access alias></accessalias>
</enterprise-subject>
```

Where:

- <name> is a fully-qualified LDAP name of a user or group.

Format examples:

– Windows LDAP: *Administrator@server.company.com*

– SunOne LDAP: uid=*Administrator*,ou=*Engineering*,dc=*server*,dc=*company*,dc=*com*.

- <type> is USER or GROUP.
- <accessalias> is a string that contains a reference to an access alias element defined in the Collaboration Access Alias Definitions.xml file. Low-level access rights are defined there.

f. Update the users/groups under <required-teamspace-template-security>.

For more information, see "Users assigned in the CollaborationEngineSecurityDefinition.xml file." on page 8.

The users/groups added here will have access to all teamspace templates regardless of if they are members of the teamspace or not. The level of access is set by the <accessalias> tag.

Find the <required-teamspace-template-security> field, and append the following lines for each user/group you want to add.

```
<enterprise-subject>
    <name><name></name>
    <type><type></type>
    <accessalias><access alias></accessalias>
</enterprise-subject>
```

Where:

- <name> is a fully-qualified LDAP name of a user or group.

  Format examples:

  – Windows LDAP: *Administrator@server.company.com*

  – SunOne LDAP: uid=*Administrator*,ou=*Engineering*,dc=*server*,dc=*company*,dc=*com*.

- <type> is USER or GROUP.
- <accessalias> is a string that contains a reference to an access alias element defined in the Collaboration Access Alias Definitions.xml file. Low-level access rights are defined there.

g. Save the file.

h. Check the document back in.

IMPORTANT Make sure you check in the document using the *Collaboration Configuration* document class.

14. Update the Collaboration Applications.xml file.

a. Using FileNet Enterprise Manager or Workplace 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 desktop.

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

e. Update the Collabaoration email-domain.

Update the the Mail Server mail domain used to archive email to reflect the domain you will be using.

Default value:

clbmail.example.com

f. **IMPORTANT** This value must be identical to the DNS name for the server you enter during the Mail server installation. For more information, see "Mail domain" on page 41 (For manual configuration, see "Mail Server Configuration" on page 48.).

g. Update the email-domain.

Update the email-domain value with the corporate mail domain used to send email (the part to the right of the @) to reflect the domain you will be using.

Default value:

example.com

h. Update the web application URL.

Update all instances of the TCM Application URL to point to where the TCM Application will be installed.

Default value:

www.example.com:8080/TCM

NOTE If you give the web application a name other than *TCM*, make sure you update this file accordingly. See "Verify the Web Application name, or give it a new name." on page 35.

i. Update the web application SSL URL.

Update all instances of the SSL version of the TCM Application URL point to where the TCM Application will be installed.

Default value:

www.example.com:9090/TCM

NOTE If you give the web application a name other than *TCM*, make sure you update this file accordingly. See "Verify the Web Application name, or give it a new name." on page 35.

j. Update the time zone.

Update the sample value for the timezone to be used by the TCM Application

Default value:

example/timezone

k. Save the file.

l. Check the document back in.

IMPORTANT Make sure you check in the document using the *Collaboration Configuration* document class.

Task 3: Prepare Process Engine for TCM

If you haven't configured email notification as part of the P8 Platform installation, follow the procedure below.

To configure the Process Engine email notification.

Complete this task to configure the connection between the Process Engine and the FileNet P8 directory service.

1. In the Process Task Manager, stop Process Service, if running.
2. Select **Process Service**.
3. In the right pane, select the **Notification** tab.
4. Enter the appropriate value for each property. For property descriptions, go to the *Documentation for FileNet P8 Platform* help and navigate to Process Engine > Process Task Manager > Process Service > Configuring Process Service > Email notification.
5. After all parameters have been entered, click **Apply** and restart the Process Service when prompted.

Task 4: 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, stored in the UTCryptoKeyFile.properties file. 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.

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

To use symmetric encryption with your TCM system you must copy the files listed above to the correct directories on your TCM servers.

To configure symmetric encryption

1. Create the folder structure on your TCM servers.

   On each TCM server (TCM Application, Collaboration Engine, 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.

      IMPORTANT

      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 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 above:

Content Engine Authentication folder:

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

2. Copy the cryptographic key files.

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

   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:

   <*App_Engine_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 28.

   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:

   <*App_Engine_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, see "Install the TCM Application" on page 31.

   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 Mail Server and Collaboration Engine servers.

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

3. (Application servers using JDK1.3 only) On the TCM Application server modify the java.security file.

   a. Use a text editor to open the java.security file used by WebLogic and typically stored in the following location: <JDK_1.3_Home>/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 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
```

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 your own CryptoKeyFile.properties file.

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:

   a. 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 doesn't exist on the Content Engine server, create it.

      We recommend copying the folder 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.

b. 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. (On your TCM servers) Copy the newly created CryptoKeyFile.properties file to the Authentication folder on your TCM servers, see "Copy the User Credentials cryptographic key file (optional)" on page 27.

Installation Tasks

To install the TCM components

1. Install the TCM Application. Do Task 5 on page 31.
2. Deploy the TCM Application (WebLogic). Do Task 6 on page 35.
3. Install the Collaboration Engine. Do Task 7 on page 36.
4. Install the Mail Server. Do Task 8 on page 39.

Task 5: Install the TCM Application

To install the TCM Application:

1. Log in to the TCM Application server as user with read/write permission on the folder where you want to install the TCM Application.
2. Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, run the TCM installer Win32_filenet_TCM_setup.exe from the CD.

   NOTE There will be a slight delay after the initial InstallShield Wizard startup window closes before the Team Collaboration Manager Installer window appears.
3. Accept the license agreement. Click **Next**.
4. Accept the default installation location or select a directory to install TCM.

   In the Directory Name field, type the path to the installation directory, or browse to select one.

   NOTE The installation location, ***<TCM_install_path>***, is the directory where the installer will add the TCM source files. The directory must exist, the installer will not create a directory for you.
5. Select setup type.

   Select Web Application. Click **Next**.
6. Choose an application server.

   Select WebLogic Application Server.
7. 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.
8. Set Application Engine 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 Collaboration Engine 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.

      Default: **<TCM_install_path>\FileNet\Authentication\CryptoKeyFile.properties**

      IMPORTANT If you are using JDK 1.4 and use maximum strength keys you need to install unlimited strength .jar files before logging in to the TCM Application. For information, see “Install unlimited strength .jar files” on page 43.

      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 26 and "Copy the User Credentials cryptographic key file (optional)" on page 27 for more information.

c. Click **Next**.

9. Set 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

IMPORTANT

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.

If you are using JDK 1.4 and use unlimited strength keys you need to install unlimited strength .jar files before logging in to the TCM Application. For information, see "Install unlimited strength .jar files" on page 43.

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 26 and "Copy the User Credentials cryptographic key file (optional)" on page 27 for more information.

b. Click **Next**.

10. Set 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.

IMPORTANT If you are using JDK 1.4 and use unlimited strength keys you need to install unlimited strength .jar files before logging in to the TCM Application. For information, see "Install unlimited strength .jar files" on page 43.

b. Select the default location or browse to a folder where the installer will create the TCMCryptoKey-File.properties file.

IMPORTANT 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**.

NOTE The installer creates the cryptographic key file, and places it in the directory specified above.

11. Configure the P8 Process Router

Enter the following information for your Process Engine router.

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.

c. Name

   Enter the name of the process router.

12. Configure P8 Workplace

    Provide the following information to allow the TCM Application to access Workplace.

    a. Collaboration Object Store name

       Enter the name of the Object Store where the TCM Application configuration files are stored.

       NOTE Normally this would be the Object Store created in "Create a Collaboration Object Store." on page 18.

    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. Secure Workplace server

       Enter the full machine name or IP address used by clients to access Workplace on the secure server.

    e. Secure Workplace port number

       Enter the secure port number of the Workplace application.

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

13. For the documentation URL, enter the Documentation Server URL, which is where the FileNet P8 Platform Documentation is installed, see "To deploy and verify the documentation web site" on page 17.

    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.

14. Read the summary and click **Next** to install the TCM Application.

15. Click **Finish** to exit the installer.
16. Verify that the installation was successful.

    The following file should contain no errors.

    <*TCM_install_path*>/FileNet/TCM_install_log_30.txt

17. Copy the TCMCryptoKeyFile to the Mail Server and Collaboration Engine servers, see “Copy the TCM cryptographic key file” on page 27.

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

Task 6: Deploy the TCM Application (WebLogic)

To deploy the TCM Application:

1. Log on to the TCM Application server.
2. Start WebLogic if it not running.
3. Log in to the WebLogic console.
4. Navigate to Web Application Modules.
5. Click **Deploy New Web Application Module**.
6. Browse for the TCM folder.

   ***<TCM_install_path>*/FileNet/Collaboration/**
7. Select the radio button for the TCM folder and click **Target Module**.
8. Verify the Web Application name, or give it a new name.

   NOTE If you give the web application a name other than the default (TCM), make sure you update the Collaboration Applications.xml file with the correct name, see “Update the web application URL.” on page 24 and “Update the web application SSL URL.” on page 24.
9. Click **Deploy**.
10. Verify successful deployment.

Task 7: Install the Collaboration Engine

To install Collaboration Engine

1. Log in to the Team Collaboration Manager as a user with read/write privileges on the folder where you will install the Collaboration Engine.
2. Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, run the TCM installer Win32_filenet_TCM_setup.exe from the CD.

   NOTE There will be a slight delay after the initial InstallShield Wizard startup window closes before the Team Collaboration Manager Installer window appears.
3. Accept the license agreement. Click **Next**.
4. Accept the default installation location or select a directory to install TCM.

   In the Directory Name field, type the path to the installation directory, or browse to select one.

   NOTE The installation location, ***<TCM_install_path>***, is the directory where the installer will add the TCM source files. The directory must exist, the installer will not create a directory for you.
5. Select setup type.

   Select Collaboration Engine. Click **Next**.
6. 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.
7. Set Application Engine security.

   This screen lets select the CryptoKeyFile.properties file. This file holds the cryptographic keys that secure the communication between Collaboration Engine 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.

      Default: **<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 26 and "Copy the User Credentials cryptographic key file (optional)" on page 27 for more information.

   c. Click **Next**.
8. Set 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.

Default: **<TCM_install_path>\FileNet\Authentication**

IMPORTANT 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 26 and "Copy the User Credentials cryptographic key file (optional)" on page 27 for more information.

b. Click **Next**.

9. Set 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\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 26 for more information.

IMPORTANT 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 32) you must install unlimited strength .jar files (see "Install unlimited strength .jar files" on page 43), and then manually configure the Collaboration Engine password after you complete the installation (see "Collaboration Engine Configuration" on page 47).

b. Click **Next**.

10. Configure the P8 Process Router

Enter the following information for your Process Engine router.

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.

c. Name

Enter the name of the process router.

11. Configure the Collaboration Engine.

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 used to store the Collaboration Engine configuration files.

NOTE Normally this would be the Object Store created in "Create a Collaboration Object Store." on page 18.

b. User ID

Enter the user ID of a user that is both Collaboration Administrator and has sysadmin-rights on the objects in the Collaboration object store, see "<Collaboration Engine user>" on page 8.

c. Password

Enter the password for the user.

IMPORTANT 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 32) you need to install unlimited strength .jar files, see "Install unlimited strength .jar files" on page 43, and then manually configure the Collaboration Engine password after you complete the installer, see "Collaboration Engine Configuration" on page 47.

d. Click **Next**.

12. Read the summary and click **Next** to install the Collaboration Engine.
13. Click **Finish** to exit the installer.
14. Verify that the installation was successful.

The following file should contain no errors.

***<TCM_install_path>*/FileNet/TCM_install_log_30.txt**

IMPORTANT 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 .jar files, see "Install unlimited strength .jar files" on page 43, and then manually configure the Collaboration Engine password, see "Collaboration Engine Configuration" on page 47.

Task 8: Install the Mail Server

To have TCM retrieve and store emails and email attachments for the Teamspaces, you must install and configure the Java Apache Mail Enterprise Server using the TCM installer.

For information about Java Apache Mail Enterprise Server, see http://james.apache.org/.

To install the Mail Server:

1. Log in to the server you are installing Mail Server on as a user with read/write permissions on the folder where you will install the Mail server.
2. Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, run the TCM installer Win32_filenet_TCM_setup.exe from the CD.

   NOTE There will be a slight delay after the initial InstallShield Wizard startup window closes before the Team Collaboration Manager Installer window appears.
3. Accept the license agreement. Click **Next**.
4. Accept the default installation location or select a directory to install Mail Server.

   In the Directory Name field, type the path to the installation directory, or browse to select one.

   NOTE The installation location, ***<TCM_install_path>***, is the directory where the installer will add the TCM source files. The directory must exist, the installer will not create a directory for you.
5. Select setup type.

   Select Mail Server. Click **Next**.
6. Enter the Content Engine Java API information.
   - 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.
7. Set Application Engine security.

   This screen lets you select the CryptoKeyFile.properties file. This file holds the cryptographic keys that secure the communication between Collaboration Engine 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.

      Default: **<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 26 and “Copy the User Credentials cryptographic key file (optional)” on page 27 for more information.
8. Set 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.

Default: **<TCM_install_path>\FileNet\Authentication**

IMPORTANT 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 26 and "Copy the User Credentials cryptographic key file (optional)" on page 27 for more information.

b. Click **Next**.

9. Set 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\TCMCryptoKeyFile.properties

IMPORTANT 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 32), you must install unlimited strength .jar files (see "Install unlimited strength .jar files" on page 43), and then manually configure the Mail Server password after you complete the installation (see "Mail Server Configuration" on page 48).

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 26 for more information.

b. Click **Next**.

10. Configure Mail Server.

Enter the following information to configure your Mail Server.

a. Object Store

Enter the name of the Object Store used for Mail Server configuration.

NOTE Normally this would be the Object Store created in "Create a Collaboration Object Store." on page 18.

b. User ID

Enter the user ID of a user that is both Collaboration Administrator and has sysadmin-rights on the objects in the Collaboration object store, see "<Mail Server user>" on page 8.

c. Password

Enter the password for that user.

IMPORTANT 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 32) you need to install unlimited strength .jar files, see "Install unlimited strength .jar files" on page 43 and then manually configure the Mail Server password after you complete the installer, see "Mail Server Configuration" on page 48.

d. Mail domain

Enter the full DNS name for the server you are installing the Mail server on.

IMPORTANT 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, see "Update the email-domain." on page 24.

e. Post master email address

Enter the administrative email address for the mail server.

f. SMTP port

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

IMPORTANT

If your server is running IIS, and it is set up to listen on the same port you select for the Mail server, make sure the Simple Mail Transport Protocol (SMTP) service is stopped and disabled.

g. Click **Next**.

11. Read the summary and click **Next** to install the Mail Server.
12. Click **Finish** to exit the installer.
13. Verify that the installation was successful.

The following file should contain no errors.

<*TCM_install_path*>/FileNet/TCM_install_log_30.txt

IMPORTANT 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 .jar files, see "Install unlimited strength .jar files" on page 43, and then manually configure the Collaboration Engine password, see "Mail Server Configuration" on page 48.

Configuration/Startup Tasks

To configure the TCM components

1. Install unlimited strength .jar files. Do Task 9 on page 43.
2. (Optional) Manually Configure TCM. Do Task 10 on page 44.
3. (Optional) Setup TCM SSL security. Do Task 11 on page 50.
4. Start Team Collaboration Manager. Do Task 12 on page 53.
5. Configure Workflow for TCM use. Do Task 13 on page 54.

Task 9: Install unlimited strength .jar files

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

IMPORTANT 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 need to 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 Encryptiont. Scroll down for the *Configuring a Security Provider for a J2EE Application Server Environmen 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..

   NOTE These directories do not exist until after you have run the installer.

   - TCM Application - lib\security (In the location from which the Web Server loads its JRE.Normally, that is the location specified in the JAVA_HOME environment variable.

     Example, Weblogic:

     C:\bea\jdk141_05\jre\lib\security
   - Collaboration Engine - **<*TCM_install_path*>\FileNet\Collaboration_jvm\lib\security**
   - Mail Server - **<*TCM_install_path*>\FileNet\Collaboration_jvm\lib\security**
3. Restart the TCM Application server.

Task 10: (Optional) Manually Configure TCM

You can run the TCM installer without providing any configuration data. Performing a “default” installation--click through the installer without entering any values--will install unconfigured TCM components on your servers. After installing, but before launching TCM, you must manually configure the components for TCM to work properly.

NOTE All editing described below can be done using a standard text editor such as Notepad.

IMPORTANT The passwords stored in the configuration files are encrypted. To edit the password values you need to encrypt the passwords using the supplied command line application and then edit in the encrypted passwords in the configuration files described below. For more information, see “Running the Encrypt Password tool” on page 49.

Perform prerequisite tasks and run the TCM installer

Before you perform the manual configuration steps listed in the sections below, verify that you have performed the following “default” installation and configuration steps:

1. “Prepare Content Engine for TCM” on page 18. (“Default” installation)
2. “Configure Symmetric Encryption” on page 26. (Copy cryptographic key files to your servers)
3. “Install the TCM Application” on page 31. (“Default” installation)
4. “Copy the TCM cryptographic key file” on page 27. (Copy cryptographic key files to your servers)
5. “Install the Collaboration Engine” on page 36. (“Default” installation)
6. “Install the Mail Server” on page 39. (“Default” installation)
7. “Install unlimited strength .jar files” on page 43. (Optional configuration)

Create and configure Object Store for TCM

1. “Create a Collaboration Object Store.” on page 18.
2. “Configure Full Text Indexing on the Collaboration Object Store.” on page 21.
3. “Update the Collaboration Enterprise Security Definitions.xml file.” on page 22.
4. “Update the Collaboration Applications.xml file.” on page 23.
5. “Deploy the TCM Application (WebLogic)” on page 35. (Deploy application)

Configure the TCM servers

IMPORTANT To perform the following manual configuration steps you need to have read/write permissions on the TCM installation folder on each machine.

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:

- Collaboration Engine

  - collabEngineConfig.properties (**<*TCM_install_path*>\FileNet\Collaboration\Engine**)
  - WcmApiConfig.properties (**<*TCM_install_path*>\FileNet\Collaboration\Engine**)
- TCM Application
  - 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**)
- Mail 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.

IMPORTANT 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
   - Collaboration Engine
   - Mail 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
   - Collaboration Engine
   - Mail 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 =D:\\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 26.

3. User Token Security

   Set the values on the following servers:

   - TCM Application
   - Collaboration Engine
   - Mail Server

   Edit the following file:

   - WcmApiConfig.properties

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

   - Credentials protection (By default Symmetric, do not change)
   - cryptographic key file location

```
CredentialsProtection/UserToken =Symmetric
CryptoKeyFile/UserToken =D:\\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 26.

4. TCM Security

   Set the values on the following servers:

   - TCM Application
   - Collaboration Engine
   - Mail 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 (Mail 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, see "Configure Symmetric Encryption" on page 26.

5. P8 Process Engine Configuration

Set the values on the following servers:

- TCM Application
- Collaboration Engine

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

   Edit the following values:

   - User ID (Enter the user ID of a user that is both Collaboration Administrator and has sysadmin-rights on the objects in the Collaboration object store, see “<Collaboration Engine user>” on page 8.)
   - Password (Encrypted, see “Running the Encrypt Password tool” on page 49.)
   - 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

   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

   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. Mail Server Configuration

   Set the values on the following server:

   - Mail Server

   Edit the following values:

   - Object Store name - Enter the name of the Object Store used for Mail Server configuration.
   - User ID - Enter the user ID of a user that is both Collaboration Administrator and has sysadmin-rights on the objects in the Collaboration object store, see "<Mail Server user>" on page 8.
   - Password - Encrypted, see "Running the Encrypt Password tool" on page 49.
   - Mail domain - Enter the full DNS name for the server you are installing the Mail Server on.

     IMPORTANT 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, see "Update the email-domain." on page 24.
   - Postmaster email address
   - SMTP port - Enter the SMTP port used by the mail server (default 25).

     IMPORTANT If your server is running IIS, and it is set up to listen on the same port you select for the Mail server, make sure the Simple Mail Transport Protocol (SMTP) service is stopped and disabled.

   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>?
<postmaster>admin@collab.example.com</postmaster>
```

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 each of the TCM servers at the following location:

<*TCM_install_path*>/FileNet/Collaboration/.../EncryptPassword.bat

IMPORTANT If you are using JDK 1.4 and use maximum strength keys in your TCMCryptoKeyFile.properties file you need to install unlimited strength .jar files before running the Encrypt Password tool. For information, see “Install unlimited strength .jar files” on page 43.

To run the password encryption tool:

1. Log in to the server you want to configure.
2. Open a command window.
3. Run the encryption tool:

   ```
   PROMPT> <TCM_install_path>/FileNet/Collaboration/.../EncryptPassword.bat <password>
   ```

   NOTE You can run the tool with the password appended to the command line or have the tool prompt you for the password.
4. If prompted, type in the password you want to encrypt using the TCM cryptographic key.
5. The tool returns the encrypted password.
6. Open the configuration file and copy the encrypted password to the correct location.

Task 11: (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.

There are three 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 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 entire session will be handled by the SSL-enabled host.
   - `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 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>
   ```

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

   IMPORTANT Do not add the protocol part of the URL.
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 51.

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 WebLogic, 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>
   ```

   NOTE 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.

   IMPORTANT Do not add the protocol part of the URL.
6. Start WebLogic 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.

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. From the WebLogic console Redeploy the TCM Application.

Task 12: Start Team Collaboration Manager

The TCM environment should be started 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 your isolated region is initialized.
4. (If the Component Manager is already configured) Verify that Component Manager is running.

   NOTE The first time you start TCM the you will launch and configure the Component Manager as part of "Configure Workflow for TCM use" on page 54.

5. Start the Mail Server.

   Use the desktop shortcut--Start Collaboration Mail Server--to start the Mail Server.

6. Start Collaboration Engine.

   Use the desktop shortcut--Start Collaboration Engine--to start the Collaboration Engine.

7. Start TCM Application.

   Use the application server console to start the TCM Application.

Task 13: Configure Workflow for TCM use

To have Workflow work with the special Collaboration Component Integrator steps (Create Teamspace, Create Teamspace from Template, and Create Task) you must configure the Workflow settings on the Application Engine.

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 as a local administrator.
3. Verify that a router is configured and running on the Application Engine server.
4. Insert the TCM CD. If Autorun is enabled, the setup program will start. Otherwise, run the TCM installer Win32_filenet_TCM_setup.exe from the CD.

   NOTE There will be a slight delay after the initial InstallShield Wizard startup window closes before the Team Collaboration Manager Installer window appears.
5. Accept the license agreement. Click **Next**.
6. Accept the default installation location or select a directory to install TCM.

   In the Directory Name field, type the path to the installation directory, or browse to select one.

   NOTE The installation location, ***<TCM_install_path>***, is the directory where the installer will add the TCM source files. The directory must exist, the installer will not create a directory for you.
7. Select setup type.

   Select Workflow Integration, and click **Next**.
8. Read the summary and click **Next** to install the Workflow Integration components.
9. Click **Finish** to exit the installer.
10. Verify that the installation was successful.

    The following file should contain no errors.

    ***<TCM_install_path>*/FileNet/TCM_install_log_30.txt**
11. Create Collaboration Workflow queue.
    a. On the Application Engine server log in to Workplace as a user with access to the Process Configuration Console in the Admin tab.

       IMPORTANT You must log in to Workplace from the Application Engine server as the procedure below involves referencing files local to this server.

    b. Select the Admin tab.

    c. Select Process Configuration Console.

    d. Right-click your router and select **Connect**.

    e. Expand Server.

    f. Right-click **Component Queues** and select **New**

    g. Enter *Collaboration_Operations* for the Queue Name.

h. Click **Next**

i. Under Adapter, select **Java Component**. Click **Configure**.

j. Browse to and select the jar file path:

<*TCM_install_path*>\FileNet\Collaboration\Workflow\lib\CollaborationOperations.jar,

and click **Open**.

k. Click **OK**.

l. Under Adaptor Properties, set the polling rate (default 1000 = one second) to a value that suits your setup.

For information, go to the *Documentation for FileNet P8 Platform* help and navigate to *Adaptor configuration* under Workplace > Admin tools > Process Configuration Console > Queues > Configure component queues > Create a component queue.

m. Enter JAAS (Java Authentication and Authorization Service) Credentials.

i. Enter a user name and password for the Component Integrator queue you just created.

NOTE

Enter the user ID of a user that is both Collaboration Administrator, has system administrator rights on the Process Engine, and has Content Engine GCD Administrator rights on the objects in the Collaboration object store, see “<JAAS User>” on page 8.

(If security is added to the Collaboration_Wait queue) The user must have access to the Collaboration_Wait queue, see “(Optional) Update security for Collaboration_Wait queue.” on page 56.

ii. Enter *CELogin* for Configuration Context.

n. Click **Finish**.

o. Click the **Disk icon** in the menu bar to commit the changes. Verify the changes and click **Continue**.

p. Once the status indicator shows Success, click **Close**.

12. Add Collaboration Workflow Configuration.

a. In the Process Configuration Console right-click the Router and select **Import from XML file...**.

b. Browse to and select:

<*TCM_install_path*>\FileNet\Collaboration\Workflow\CollaborationWorkflowConfiguration.xml

c. Click **Open**.

d. Select the **Merge** radio button.

e. Click **Import**.

f. Select **Yes** to continue (The operation cannot be undone).

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

h. Verify that the Collaboration_Operations queue installed properly by right-clicking the Collaboration_Operations queue and selecting Properties. Select the Operations tab and verify that the following operations exist:

- createTeamspace
- createTeamspaceFromTemplate
- createTask

i. Verify that Collaboration_Wait queue exists under the Work Queues.

13. (Optional) Update security for Collaboration_Wait queue.

    Use Process Config Console to perform this step.

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

    b. Select **Properties**.

    c. Select the **Security** tab.

    d. Add users and/or groups to set the security for the queue.

    e. Click **OK**.

    IMPORTANT If you update security on the Collaboration_Wait queue, make sure the JAAS user specified above ("Enter JAAS (Java Authentication and Authorization Service) Credentials." on page 55) has access to the queue. Queue security is open to everyone until users are added, then only the users and groups added have access.

14. Configure Component Manager.

    a. If not already running start Process Task Manager.

    b. Stop the Component Manager, if running.

    c. Select the General tab.

    Specify router and enter a valid user name and password.

    The user must have Query access to all of the component queues.

    For more information go to the *Documentation for FileNet P8 Platform* help and navigate to Process Engine > Process Task Manager > Component Manager > Configuring the Component Manager > General properties.

    d. 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\bsoutil.jar**
    - ***<TCM_install_path>*\FileNet\Collaboration\Workflow\lib\CollaborationOperations.jar**

    e. Click **Apply**.

    f. Start Component Manager.

15. Transfer the base CollaborationIntegration workflow definition to the Process Engine

Before you can run the base Collaboration Workflow shipped with TCM you must transfer the workflow definition to the Process Engine.

NOTE You do not have to store the workflow definition on the Content Engine, see "To change the default Process Designer behavior to not require saving the workflow definition:" on page 57.

a. On the Application Engine server, log in to Workplace as a member of a group with access rights for using the Process Designer.

b. Select the **Author** tab.

c. Select **Advanced Tools**.

d. Select **Process Designer**.

e. In Process Designer, select **File > Open**.

f. Browse to and select CollaborationIntegration.pep.

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

g. Select **File > Transfer**.

h. (If prompted to save the workflow) Browse to and select a folder in your Object Store. Give the Workflow definition a Document Title, and click **Finish** (or click **Next** to set security on the Workflow definition).

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

To change the default Process Designer behavior to not require saving the workflow definition:

i. In Process Designer select **Tools > Preferences...**

ii. Select the **Workflow** tab.

iii. Uncheck *Add/Check In Workflow Before Transfer/Launch*.

iv. Click **OK**.

16. Restart the Collaboration Engine.

a. On the Collaboration Engine server, locate the *Start Collaboration Engine* command line window.

b. Hit Enter to stop the Collaboration Engine and close the window.

c. Start the Collaboration Engine using the shortcut on the desktop.

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 please follow the instructions in "(Optional) Manually Configure TCM" on page 44.

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 Team Collaboration Manager.
3. Delete the Collaboration folder under the ***<TCM_install_path>*\FileNet folder**.

Collaboration Engine

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.

   The default location is:

   C:\Program Files

3. Run the uninstall program:

   ```
   Win32_filenet_TCM_uninstall.exe
   ```

   NOTE You can also use Add/Remove Programs from the Control Panel to remove 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 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 TCM Application installation location. The default location is:

   C:\Program Files

4. Run the uninstall program:

   ```
   Win32_filenet_TCM_uninstall.exe
   ```

   NOTE You can also use Add/Remove Programs from the Control Panel to remove 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 Collaboration Engine is the only FileNet component on your server, delete the FileNet folder.

Mail Server

To remove the Mail Server:

1. Log on to the server where you have Mail Server installed as a user with Administrative rights.
2. Navigate to the **_uninst** folder under the Mail Server installation location.

   The default location is:

   C:\Program Files

3. Run the uninstall program:

   ```
   filenet_collaboration_setup_uninstall.exe
   ```

   NOTE You can also use Add/Remove Programs from the Control Panel to remove 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.

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 TCM Application installation location. The default location is:

   C:\Program Files

3. Run the uninstall program:

   ```
   Win32_filenet_TCM_uninstall.exe
   ```

   NOTE You can also use Add/Remove Programs from the Control Panel to remove 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.

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 Platform Installation Guide*,

TCM Ports	
Clients / SSL	80 / 443
TCM Application (WebLogic)	7001 / 7002
Mail Server	25 110 (Pop3)

Index

A
add-on 20
Adobe Reader 4

B
before you begin 5

C
Collaboration Applications.xml 23
Collaboration Engine
  install 36
  remove 58
Collaboration Enterprise Security Definitions.xml 22
collocate 13
configuration/startup tasks 42
configure
  Collaboration Applications.xml 23
  Collaboration Enterprise Security Definitions.xml 22
  email notification 25
  JAAS credentials 55
  manual 44
  manually 6
  Object store security 20
  share config.properties among multiple TCM Applications 51
  symmetric encryption 26
  tasks 42
Content Engine
  add-ons 6
  CryptoKeyFile.properties location 28
  enable DTC and COM+ access 6
  prepare 18
  running the installer multiple times 7
  security 12
Content Engine Components
  remove 58
Content Engine GCD Administrator 12
  log in as 18
create cryptographic key 28
CryptoKeyFile.properties 26
custom installation 13

D
documentation
  help URL configuration 33
  install 15
  update the search index 15

E
email notification 25
encryption tool 49

F
FileNet P8 Platform 5
FileNet P8 Platform documentation 5, 15

H
high availability 6

I
install
  Collaboration Engine 36
  custom 13
  deploy TCM Application on WebLogic 35
  documentation 15
  Mail Server 39
  planning 5
  TCM Application 31

J
JAAS Credentials 55
JDK 1.4 13

M
Mail Server
  disable IIS port #25 7
  install 39
  remove 59
manual configuration 44
Manually configure TCM 6
maximum strength cryptographic keys 13

O
Object store
  database store 19
  filestore 19
  full text indexing 21
  security 20

P
P8 Add-ons 6
passwords 49
plan installation 5
port numbers
  required 13
  TCM default 60

prepare
Content Engine 18
installation 5
Process Engine 25
prerequisite tasks 14
Process Engine
prepare 25

R

remove
Collaboration Engine 58
Content Engine Components 58
Mail Server 59
software 58
TCM Application 58
required port numbers 13

S

security
Collaboration Administrators 8
Collaboration Engine user 8
Collaboration Users 8
Content Engine GCD Administrator 12
Initial object store Administrator account(s) 8
JAAS User 8
Mail Server user 8
Object store Users account(s) 8
security roles 7
to run the installer 12
Users with required-teamspace-security 8
Users with required-teamspace-template-security 8
security roles 7
share configuration files 51
SSL
setup SSL security 50
start TCM 53
symmetric encryption
Authentication Security Considerations 13
configure 26
create cryptographic key 28
CryptoKeyFile.properties 26
CryptoKeyFile.properties Content Engine location 28
maximum strength cryptographic keys 13
password encryption 49
TCMCryptoKeyFile.properties 26
unlimited strength .jars 43
UTCryptoKeyFile.properties 26

T

TCM addons 20
TCM Application
deploy on WebLogic 35
install 31
remove 58
WebLogic domain 7
TCM default ports 60
TCMCryptoKeyFile.properties 26

U

Unlimited strength encryption
symmetric encryption 43
user name display setting 6
User Token
Crypto key file path
WebLogic 32, 36, 37, 40
UTCryptoKeyFile.properties 26

W

WebLogic
deploy TCM Application 35