

# FatWire | Content Server 7

Version 7.6

## Rollup Installation Guide

**Document Revision Date:** Jun. 15, 2011



FATWIRE CORPORATION PROVIDES THIS SOFTWARE AND DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall FatWire be liable for any direct, indirect, incidental, special, exemplary, or consequential damages of any kind including loss of profits, loss of business, loss of use of data, interruption of business, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) arising in any way out of the use of this software or the documentation even if FatWire has been advised of the possibility of such damages arising from this publication. FatWire may revise this publication from time to time without notice. Some states or jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Copyright © 2011 FatWire Corporation. All rights reserved.

The release described in this document may be protected by one or more U.S. patents, foreign patents or pending applications.

FatWire, FatWire Content Server, FatWire Engage, FatWire Satellite Server, CS-Desktop, CS-DocLink, Content Server Explorer, Content Server Direct, Content Server Direct Advantage, FatWire InSite, FatWire Analytics, FatWire TeamUp, FatWire Content Integration Platform, FatWire Community Server and FatWire Gadget Server are trademarks or registered trademarks of FatWire, Inc. in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. AIX, AIX 5L, WebSphere, IBM, DB2, Tivoli and other IBM products referenced herein are trademarks or registered trademarks of IBM Corporation. Microsoft, Windows, Windows Server, Active Directory, Internet Explorer, SQL Server and other Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. Red Hat, Red Hat Enterprise Linux, and JBoss are registered trademarks of Red Hat, Inc. in the U.S. and other countries. Linux is a registered trademark of Linus Torvalds. SUSE and openSUSE are registered trademarks of Novell, Inc., in the United States and other countries. XenServer and Xen are trademarks or registered trademarks of Citrix in the United States and/or other countries. VMware is a registered trademark of VMware, Inc. in the United States and/or various jurisdictions. Firefox is a registered trademark of the Mozilla Foundation. UNIX is a registered trademark of The Open Group in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

This product includes software developed by the Indiana University Extreme! Lab. For further information please visit <http://www.extreme.indiana.edu/>.

Copyright (c) 2002 Extreme! Lab, Indiana University. All rights reserved.

This product includes software developed by the OpenSymphony Group (<http://www.opensymphony.com/>).

The OpenSymphony Group license is derived and fully compatible with the Apache Software License; see <http://www.apache.org/LICENSE.txt>.

Copyright (c) 2001-2004 The OpenSymphony Group. All rights reserved.

You may not download or otherwise export or reexport this Program, its Documentation, or any underlying information or technology except in full compliance with all United States and other applicable laws and regulations, including without limitations the United States Export Administration Act, the Trading with the Enemy Act, the International Emergency Economic Powers Act and any regulations thereunder. Any transfer of technical data outside the United States by any means, including the Internet, is an export control requirement under U.S. law. In particular, but without limitation, none of the Program, its Documentation, or underlying information of technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident, wherever located, of) any other country to which the U.S. prohibits exports of goods or technical data; or (ii) to anyone on the U.S. Treasury Department's Specially Designated Nationals List or the Table of Denial Orders issued by the Department of Commerce. By downloading or using the Program or its Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list or table. In addition, if the Program or Documentation is identified as Domestic Only or Not-for-Export (for example, on the box, media, in the installation process, during the download process, or in the Documentation), then except for export to Canada for use in Canada by Canadian citizens, the Program, Documentation, and any underlying information or technology may not be exported outside the United States or to any foreign entity or "foreign person" as defined by U.S. Government regulations, including without limitation, anyone who is not a citizen, national, or lawful permanent resident of the United States. By using this Program and Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not a "foreign person" or under the control of a "foreign person."

*FatWire Content Server Rollup Installation Guide*

Document Revision Date: Jun. 15, 2011

Product Version: 7.6

## **FatWire Technical Support**

[www.fatwire.com/Support](http://www.fatwire.com/Support)

## **FatWire Headquarters**

FatWire Corporation  
330 Old Country Road  
Suite 303  
Mineola, NY 11501  
[www.fatwire.com](http://www.fatwire.com)

## Table of Contents

<b>1</b>	<b>Installing FatWire Content Server 7.6</b>	<b>5</b>
	Overview	6
	Pre-Installation Steps	7
	Pre-Installation Decisions	9
	Post-Installation Summary	11
	Rollup Installation Procedures	12
	Running the GUI Installer	12
	Upgrading Silently	20
	Changes to Content Server	27
	All Installations	27
	Installations with log4j	27
	Installations with WEM Framework	28
	New Login Page	28
	New Site: AdminSite	29
	New Application: WEM Admin	29
	New Security Model	29
	Addition of Groups	29
	Updated General Administrator	29
	New Web Application: CAS	29
	CAS-Protected URLs	30
	CAS Clustering	30
	Changes to Property and Configuration Files	30
	Schema Changes	31
<b>2</b>	<b>Post-Installation Steps</b>	<b>33</b>
	Reapplying Customizations	34
	Configuring Browsers	34
	Enabling System Tools on a Delivery System	34
	Verifying Content Server Installations Without WEM Framework	35
	Verifying Content Server Installations Running WEM Framework	39
	Redeploying CAS on a New Server (CS-WEM Installations)	42

---

Deploying Secondary CAS Cluster Members (CS-WEM Installations) . . . . .	44
Enabling the Clarkii Online Image Editor . . . . .	45
Setting Up inCache . . . . .	46
Setting Up Apache log4j . . . . .	46
Setting Up Content Server Developer Tools . . . . .	46
Installing the Database Performance Utility . . . . .	46
Installing Language Packs . . . . .	47
Installing Remote Satellite Server . . . . .	47

## Chapter 1

# Installing FatWire Content Server 7.6

This chapter provides instructions for installing FatWire Content Server 7.6.

This chapter contains the following sections:

- [Overview](#)
- [Pre-Installation Steps](#)
- [Pre-Installation Decisions](#)
- [Post-Installation Summary](#)
- [Rollup Installation Procedures](#)
- [Changes to Content Server](#)

## Overview

FatWire Content Server 7.6 provides the following new features:

- System tools, which provide general administrators with a range of diagnostic utilities for troubleshooting directly from the Content Server Advanced interface. Features include configuring log4j loggers, accessing various types of system information, managing caches, searching the contents of the Content Server log, and testing the performance of the shared file system. For information about system tools, see the *Content Server Administrator's Guide*.
- The option to migrate from Content Server's existing logging system to Apache log4j.
- Central Authentication Service (CAS) clustering, which makes it possible to balance the load of user authentications for the FatWire Web Experience Management (WEM) Framework (see below).
- FatWire Content Server Developer Tools (CSDT), which enable developers to work in a distributed environment on their own Content Server instances using tools such as the Eclipse Integrated Development Environment and version control system integration. Using CSDT, a development team can manage Content Server resources and share those resources with other members of the team. CSDT is accessible only if the WEM Framework is installed (see below). For information about CSDT, see the *Guide to Content Server Developer Tools*.
- Asset caching capabilities, which the inCache framework (see below) now provides.

The following options, available since FatWire Content Server 7.5 Patch 3, are provided as well. If any option was enabled in 7.5 Patch 3, 4, or 5, it remains enabled in Content Server 7.6.

- The WEM Framework, which runs on Content Server. If you choose to install this option, the WEM login screen will replace the Content Server login screen, which affects the way Content Server Dash, Advanced, and InSite interfaces are accessed. WEM Framework consists of the following components:
  - REST API** – Enables developers to communicate with Content Server for the purpose of building and implementing applications on the WEM framework.
  - Universal UI container** – Provides a single interface for accessing FatWire products and custom-built applications running on WEM Framework and enables rendering of the applications' interfaces.
  - WEM Admin interface** – Enables the coupling of users to WEM-integrated applications and provides for centralized user management. The WEM Admin interface is **not** installed on delivery systems.
  - REST Security Model** – Enables administrators to control access to the resources of applications implemented on WEM.
  - Single Sign-On** – Enables WEM users to access all applications allowed to them during the session without having to sign in to each application.

WEM requires Central Authentication Service (CAS), which can be clustered or non-clustered. The CAS web application will be deployed during the installation process. Secondary members of a CAS cluster will be deployed manually in the post-installation process.

- The inCache framework, which is FatWire's implementation of Terracotta's Ehcache open source product available under the Apache license. The inCache framework

provides significant performance improvements over our traditional page caching method. It provides asset caching capabilities as well. The inCache framework is installed by default but its page caching and asset caching capabilities must be configured manually. If inCache is supported but not set up in your current installation, your current page caching method will run by default when Content Server 7.6 is installed. For information about setting up inCache page caching and asset caching, see the *Content Server Administrator's Guide*.

- The database performance enhancement utility, which can be used on systems running in delivery or content management/development mode to create additional indexes for database tables. If you wish to use this utility in Content Server 7.6, you must install it manually.
- The Clarkii Online Image Editor (OIE), from InDis Baltic, which can be enabled in the Content Server Dash, Advanced, and InSite interfaces in place of your current Online Image Editor. For information about Clarkii OIE, see the *Content Server Developer's Guide* as well as the Dash and Advanced user guides.

## Pre-Installation Steps

This guide is written for experienced Content Server installation engineers. Before upgrading to Content Server 7.6, complete the following steps:

- Read the release notes and the *Supported Platform Document*.

### Note

All FatWire product documentation is available on our e-docs site, at <http://support.fatwire.com>. The site is password protected. Accounts can be opened from the home page.

- Read the rest of this guide to familiarize yourself with the installation procedures available, the changes that will be made by the installer, and the post-installation steps.
- Start with a Content Server 7.5 or 7.5 Patch *x* installation. You will run the rollup installer on all systems in your environment. There are two system types: content management/development and delivery. Content management systems and development systems are of the same type, but are used for different purposes.

The Content Server 7.6 rollup installer detects and reuses the system type (content management/development or delivery) and the deployment mode (automatic or manual) that were selected during the Content Server 7.5 installation. For example, if Content Server 7.5 was installed as a delivery system and deployed automatically, the

Content Server 7.6 rollup installer continues to treat the system as a delivery system and deploys automatically.

#### Note

- The system type and deployment mode cannot be changed.
- **The installation process does not install user interfaces on delivery systems**, except for a limited version of the Content Server Advanced interface to enable the management of select features.

- If your current Content Server application has been in use since it was first deployed, do the following:
  - Back up your current Content Server application by creating `cs.war` and `ContentServer.ear` files. Also, back up the installation directory, `Shared` directory, and database. For detailed instructions, see the *Content Server Backup and Recovery Guide*.

In the post-installation process, you will use the backed up installation directory, `Shared` directory, and database to reapply the customizations they may contain, as described in [“Reapplying Customizations,” on page 34](#).
  - If customizations were made to your current Content Server application since it was first deployed, and those customizations are not reflected in the `cs.war` and `ContentServer.ear` files located in `<cs_install_dir>/ominstallinfo/app`, remove the files and copy the `.war` and `.ear` files for your currently deployed Content Server application to the same directory.

During the installation, the `cs.war` file is archived as `cs-date-time.war`. In the post-installation process, you will use the archived version to reapply customizations where necessary, as described in [“Reapplying Customizations,” on page 34](#).
- For JDK 1.6, copy the `jaxb-impl-2.1.12.jar` file in the `Rollup/wem/lib` directory to the following location: `<PATH_TO_JDK_FOLDER>/jre/lib/endorsed`

#### Note

Do not use the `jaxb-impl` that ships with JDK 1.6. Content Server relies on the latest version of `jaxb-impl`, which we provide in the location named above. The latest `jar` file must be used in order to resolve a runtime conflict with WebLogic Server (which ships with JDK 1.6).

- On all application servers, do the following:
  - Update the startup script:
    - Set the `max PermGen` parameter in the range of 128MB–196MB.
    - Set `-Dcs.useJavaURLDecoder` to `false`. This ensures that the Apache URLCodec will be used to decode URL characters.
  - Update the `CLASSPATH` environment variable:
    - Add `<cs_install_dir>/bin`.
    - Remove older versions of the Java Runtime Environment.



- Add the path to Content Server's modified version of the Microsoft XML Parser (`MSXML.jar` in the `WEB-INF/lib` directory). If the class path refers to another version of the Microsoft XML Parser, Content Server will fail when parsing XML.
- On all operating systems, update the library path environment variable (Linux and Solaris: `LD_LIBRARY_PATH`; AIX: `LDPATH`; HP-UX: `SHLIB_PATH`; Windows: `PATH`) as follows:
  - Add `<cs_install_dir>/bin`.
  - Remove older versions of the Java Runtime Environment.

### Note

If the class path and library path are not set properly, **System Tools** on the **Admin** tab of the Content Server Advanced interface will have reduced functionality and CAS will not start.

- On JBoss and Tomcat application servers, place the following jar files in the `<app_server_home>/lib` directory. This ensures that the datasource will be correctly initialized when Content Server 7.6 is first started.
  - `commons-dbc-1.3.jar`  
You can download this file at <http://commons.apache.org/dbcp/>.
  - `commons-pool-1.5.5.jar`  
You can download this file at <http://commons.apache.org/pool/>.
- On the WebSphere application server, enable URL rewriting in the WebSphere administrative console. This ensures that the **Site Plan** tree in the Dash interface will load successfully.
- If you are starting with Content Server 7.5 Patch 3, 4, or 5 and the WEM Framework is installed, undeploy and delete the previous CAS installation before beginning the rollup.

## Pre-Installation Decisions

- Do you want to run the GUI installer or the silent installer?

The GUI installer provides access to extensive online help to guide you through the rollup installation. The silent installer does not provide access to online help; however, rolling up silently can save time, since you configure your installation settings before running the installer. For more information about these installation procedures, see [“Running the GUI Installer,” on page 12](#) and [“Upgrading Silently,” on page 20](#).
- Do you want developers to have access to Content Server Developer Tools (CSDT)?

CSDT is accessible only if the WEM Framework is installed. Therefore, if WEM was not installed previously, you must select WEM during the rollup installation. In the post-installation process, developers can then install the required Eclipse plug-in. For more information about CSDT, see the *Guide to Content Server Developer Tools*.

- Do you want to build REST-based applications and/or use Single Sign-On?

REST and Single Sign-On are provided only if the WEM Framework is installed. Therefore, if WEM was not installed previously, you must select WEM during the rollup installation. Be sure to install WEM on all systems in your Content Server environment (development, content management, and delivery). On a delivery system, only selected WEM components are installed to provide REST and Single Sign-On; the WEM Admin interface is **not** installed.

For Single Sign-On, you must also provide Central Authentication Service (CAS) deployment information during the installation process. The deployment information required depends on the deployment mode (automatic or manual), which is inherited from the Content Server 7.5 installation. Answer the following question to help you determine your CAS deployment information:

Which deployment mode was enabled for Content Server 7.5?

- If automatic deployment was enabled, the Content Server 7.6 installer will automatically deploy Content Server. It will also automatically deploy CAS on the server hosting the primary Content Server cluster member. The CAS deployment information that you provide during the installation process must therefore point to the server hosting the primary Content Server cluster member. If you want to move CAS to a different server, you must do so manually in the post-installation process.
- If manual deployment was enabled, you will manually deploy Content Server. You will also manually deploy CAS on the server of your choice (the server hosting the primary Content Server cluster member or another server). The CAS deployment information that you provide during the installation must point to this server.

If you are clustering CAS, only the primary member of the CAS cluster is deployed during the installation process. You must configure and deploy the secondary CAS cluster members manually during the post-installation process. For more information, see [“Deploying Secondary CAS Cluster Members \(CS-WEM Installations\),”](#) on page 44.

### Caution!

When WEM is installed on Content Server, the `fwadmin` general administrator is automatically assigned to the `RestAdmin` group (for unrestricted access to REST services), and enabled on `AdminSite` (where the WEM Admin application runs by default).

When you finish installing Content Server, **do not delete the `fwadmin` general administrator**. Doing so disables **all** access to Content Server when WEM is installed. Instead, to ensure security, change the password

For information about other changes that are made to Content Server when WEM is installed, see [“Installations with WEM Framework,”](#) on page 28. See also the *WEM Framework Administrator’s Guide* and the *WEM Framework Developer’s Guide*.

- Do you want to migrate from Content Server's existing logging system to Apache log4j during the installation process?

If so, you must select the log4j migration option during the installation process. For information about the changes that are made when you migrate to log4j, see [“Installations with log4j,” on page 27](#).

If you do not migrate to log4j during the installation process, you can switch to log4j at a later time. For instructions, see the *Content Server Administrator's Guide*.

## Post-Installation Summary

Once Content Server 7.6 is installed, you will follow up by reapplying customizations, configuring browsers, verifying the installation, and completing configuration steps that depend on whether you chose to install WEM, wish to enable inCache, or both. Installing Remote Satellite Server is covered in the *Installing Satellite Server Guide*.

## Rollup Installation Procedures

Complete one of the following procedures to install Content Server 7.6:

- [Running the GUI Installer](#)
- [Upgrading Silently](#)

### Running the GUI Installer

#### Note

Before starting this procedure, ensure that all pre-installation steps ([page 7](#)) have been completed.

Start the upgrade process on the primary Content Server cluster member. When the process is complete, upgrade each of the secondary cluster members.

#### To run the GUI installer

1. Execute the installer script from the directory into which you extracted the Content Server 7.6 rollup installer (Rollup.zip):
  - On Windows: `cscrollupinstall.bat`
  - On Unix: `cscrollupinstall.sh`
2. When prompted, enter the credentials of the `ContentServer` user.
3. In this step, you have the option to migrate from Content Server's existing logging system to Apache log4j. You must **not** select this option if log4j was already configured manually or if you want to keep your existing logging system.



**Note**

If you do not migrate to log4j during the installation process, you can switch to log4j at a later time. For instructions, see the *Content Server Administrator's Guide*.

4. This step concerns the WEM Framework and Content Server Developer Tools (CSDT). Select the **WEM** check box if either of the following conditions apply:

- You want to install WEM.

If you install WEM on one system in your Content Server environment, be sure to install WEM on the other systems as well. For example, if you install WEM on a content management system, be sure to install WEM on the development and delivery systems as well. On a delivery system, only selected WEM components are installed to provide REST and Single Sign-On; the WEM Admin interface is **not** installed.

- You want developers to have access to CSDT.

CSDT is accessible only if the WEM Framework is installed.

If WEM was installed previously, a confirmation screen is displayed.

**Note**

Before selecting the WEM option, read the note on the installer screen and consider the changes that are made to Content Server when WEM is installed, as described in "[Installations with WEM Framework](#)," on [page 28](#). See also the *WEM Framework Administrator's Guide* and the *WEM Framework Developer's Guide*.



5. If you selected to install WEM, enter CAS deployment information. The information you provide depends on whether you are upgrading a primary or secondary Content Server cluster member and whether you are clustering CAS.

#### Note

The rollup installer uses the deployment mode of your current installation.

- If automatic deployment is enabled and you are rolling up the primary Content Server cluster member, the installer will deploy CAS on the server hosting the primary Content Server cluster member. If you want to redeploy CAS on a different server, you must do so manually in the post-installation process (see [“Redeploying CAS on a New Server \(CS-WEM Installations\),”](#) on page 42).
- If manual deployment is enabled, you will deploy CAS on the server hosting the primary Content Server cluster member or on a separate server.

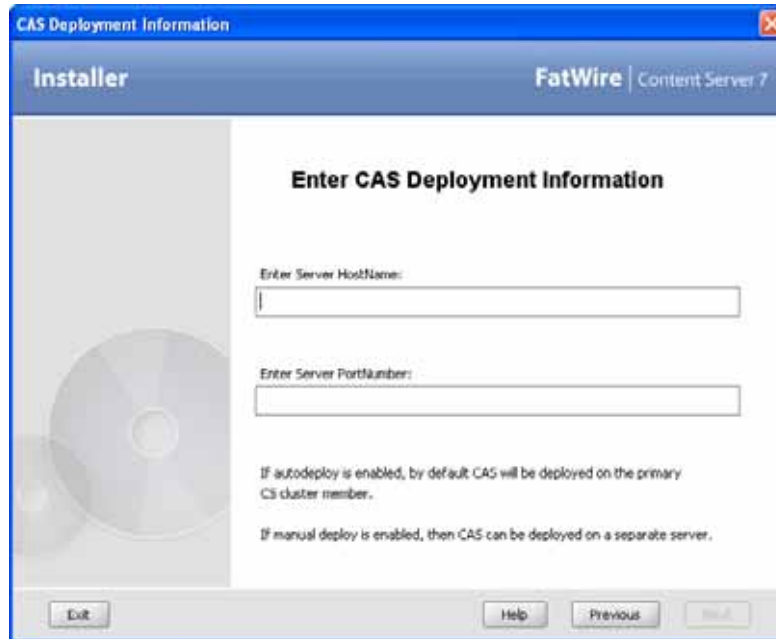
- **Upgrading the primary Content Server cluster member**

If WEM was installed previously, this screen shows only the host name of the server where CAS was deployed. You must verify that it is still correct.

If CAS was redeployed on a new server after the previous installation, since this screen does not show the first two fields, you must update this deployment information in the `omi.ini` file.

Field	CAS	Value
Server HostName	Clustered	Host name of the server running the load balancer
	Non-clustered	Host name of the server where CAS will be deployed
Server PortNumber	Clustered	Port number of the server running the load balancer
	Non-clustered	Port number of the server where CAS will be deployed
Server HostName (non-load balancer)	Clustered	Host name of the server where the primary CAS cluster member will be deployed
	Non-clustered	Host name of the server where CAS will be deployed This must match the value entered for Server HostName.

- **Upgrading a secondary Content Server cluster member**



Field	CAS	Value
Server HostName	Clustered	Host name of the server running the load balancer
	Non-clustered	Host name of the server where CAS has been deployed
Server PortNumber	Clustered	Port number of the server running the load balancer
	Non-clustered	Port number of the server where CAS has been deployed

**Note**

The installer will enter the CAS deployment information into the `SSOConfig.xml` file in `WEB-INF/classes` and into the `cas.properties`, `host.properties`, and `jbossTicketCacheReplicationConfig.xml` files in `<cs_install_dir>/bin`, enabling Content Server to connect to CAS.

If you redeploy CAS after the installation process is complete, you must also reconfigure these files. For more information, see [“Redeploying CAS on a New Server \(CS-WEM Installations\),”](#) on page 42.



6. At the installation midpoint, if manual deployment is enabled, you must deploy the Content Server web application. If WEM is selected to be installed and you are running the installer on the primary Content Server cluster member, you must also deploy the CAS web application on the server named in [step 5 on page 14](#).

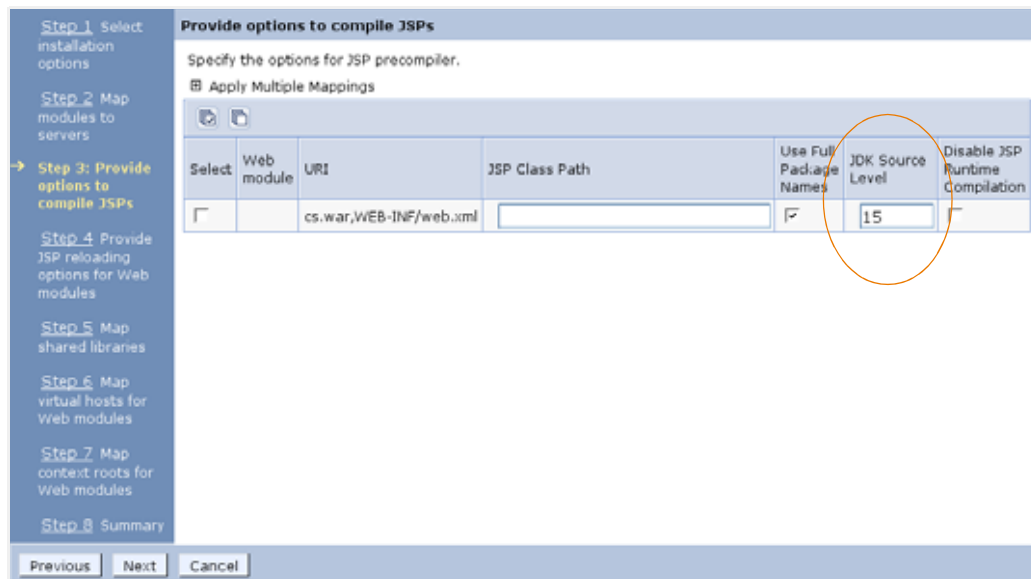
#### Note

If you are clustering CAS, the rollup installation deploys only the primary member of the CAS cluster. You must configure and deploy secondary CAS cluster members manually during the post-installation process. For more information, see “[Deploying Secondary CAS Cluster Members \(CS-WEM Installations\)](#),” on page 44.

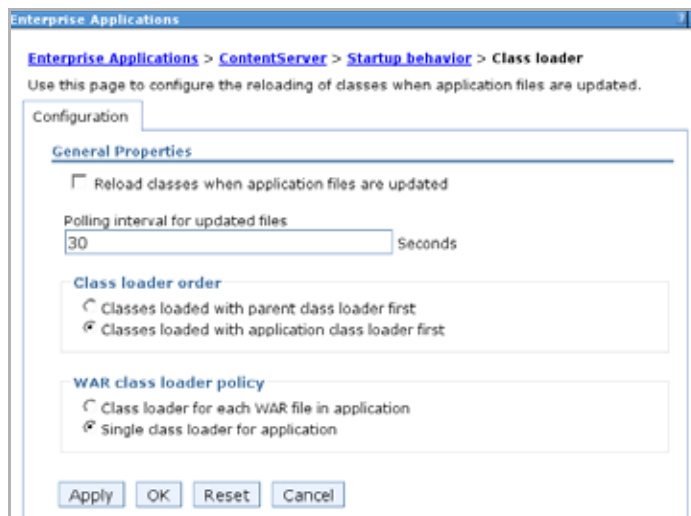
- If you are using the WebLogic application server, do the following:
  - Ensure that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
  - If you are clustering CAS, before deploying the primary CAS cluster member, add the following inside the `<weblogic-web-app>` tag in the `weblogic.xml` file (located in the `cas/WEB-INF` directory):

```
<session-descriptor>
  <persistent-store-type>replicated
</persistent-store-type>
  <url-rewriting-enabled>true
</url-rewriting-enabled>
</session-descriptor>
```

- If you are using the WebSphere application server, do the following:
  - Ensure that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
  - On the “Provide options to compile JSPs” screen, change the value of the “JDK Source Level” field to **15** for Content Server and for CAS, if it was deployed.



- On the “Enterprise Applications” screen, click **Content Server > Class loading and update detection**. On the screen that appears, do the following:
  - a. In the “Polling interval for updated files” field, enter **30**.
  - b. In the “Class load order” section, select **Classes loaded with application class loader first**.
  - c. In the “WAR class loader policy” section, select **Single class loader for application**.



7. Complete the rollup installation.
8. When the primary Content Server cluster member has been upgraded, repeat this procedure on all of the secondary Content Server cluster members, starting with [step 1 on page 12](#).
9. When all Content Server cluster members have been upgraded, complete the steps in [Chapter 2, “Post-Installation Steps”](#) as necessary for your configuration. Note the following:
  - Changes were made to Content Server as described in [“All Installations,” on page 27](#).
  - If you chose to migrate to log4j, changes were made to Content Server as described in [“Installations with log4j,” on page 27](#).
  - If you chose to install WEM, changes were made to Content Server as described in [“Installations with WEM Framework,” on page 28](#).

## Upgrading Silently

### Note

Before starting this procedure, ensure that all pre-installation steps ([page 7](#)) have been completed.

Start the upgrade process on the primary Content Server cluster member. When the process is complete, upgrade each of the secondary cluster members.

### To upgrade silently

1. Copy the `omii.ini` file from `<cs_install_dir>/ominstallinfo` to a folder outside `<cs_install_dir>` and rename the copy. The silent installer will use the copy to upgrade.
2. If the default user name and/or password for the `ContentServer` user was changed after Content Server 7.5 was installed, update the following properties in the renamed `omii.ini` file. The silent installer authenticates by referring to these credentials; if they are outdated, the installer will fail.

Property	Description
<code>CSInstallAccountName</code>	Provide the current user name for the <code>ContentServer</code> user. The default value is <code>ContentServer</code> .
<code>CSInstallAccountPassword</code>	Provide the encrypted password for the <code>ContentServer</code> user.

### Note

Use Content Server's Property Editor to get the encrypted password:

- 1) Using the Property Editor, open `futuretense.ini`.
- 2) Search for the `cs.mirrorpassword` property. If it is populated, store its value temporarily in a text file.
- 3) Replace the `cs.mirrorpassword` property value with the password you wish to encrypt.
- 4) Save the property file to have your password encrypted.
- 5) Copy the encrypted password to the `omii.ini` file.
- 6) Restore the value of `cs.mirrorpassword`, if it was populated.

3. If you want to migrate from Content Server's existing logging system to Apache log4j, add the following property to the renamed `omii.ini` file. You must **not** add this property if log4j was already configured manually or if you want to keep your existing logging system.

Property	Description
<code>ConvertToLog4J</code>	Set this property to <code>true</code> to migrate to log4j.

#### Note

If you do not migrate to log4j during the installation process, you can switch to log4j at a later time. For instructions, see the *Content Server Administrator's Guide*.

4. This step concerns the WEM Framework and Content Server Developer Tools (CSDT). Complete this step if any of the following conditions apply:
- WEM is already installed in your current installation and you want to keep WEM.
  - You want to install WEM.

If you install WEM on one system in your Content Server environment, be sure to install WEM on the other systems as well. For example, if you install WEM on a content management system, be sure to install WEM on the development and delivery systems as well. On a delivery system, only selected WEM components are installed to provide REST and Single Sign-On; the WEM Admin interface is **not** installed.

- You want developers to have access to CSDT.

CSDT is accessible only if the WEM Framework is installed.

If any of these conditions apply, add the properties in the table on [page 22](#) to the renamed `omii.ini` file. The information you provide depends on whether you are upgrading a primary or secondary Content Server cluster member and whether you are clustering CAS.

#### Note

The rollup installer uses the deployment mode of your current installation.

- If automatic deployment is enabled and you are rolling up the primary Content Server cluster member, the installer will deploy CAS on the server hosting the primary Content Server cluster member. If you want to redeploy CAS on a different server, you must do so manually in the post-installation process (see "[Redeploying CAS on a New Server \(CS-WEM Installations\)](#)," on [page 42](#)).
- If manual deployment is enabled, you will deploy CAS on the server hosting the primary Content Server cluster member or on a separate server.

Property	Description
WEM	Set this property to <code>true</code> to install WEM.
IsPrimaryClusterMember	If you are upgrading the primary Content Server cluster member, set this property to <code>true</code> . Otherwise, set it to <code>false</code> .
CASHostName	<b>Clustered CAS:</b> Point to the host name of the server running the load balancer. <b>Non-clustered CAS:</b> Point to the host name of the server where CAS will be or has been deployed.
CASPortNumber	<b>Clustered CAS:</b> Point to the port number of the server running the load balancer. <b>Non-clustered CAS:</b> Point to the port number of the server where CAS will be or has been deployed.
CASHostNameLocal	You must provide this value only when upgrading the primary Content Server cluster member. <b>Clustered CAS:</b> Point to the host name of the server where the primary CAS cluster member will be deployed. <b>Non-clustered CAS:</b> Point to the host name of the server where CAS will be deployed. This must match the <code>CASHostName</code> value.

#### Sample Configurations with Clustered CAS:

- If you are upgrading the primary Content Server cluster member and autodeploy is enabled:
 

```
WEM=true
IsPrimaryClusterMember=true
CASHostName=<host name of server with load balancer>
CASPortNumber=<port number of server with load balancer>
CASHostNameLocal=<host name of server where primary CAS
cluster member will be deployed> This must match the name of
the server hosting the primary Content Server cluster member.
```
- If you are upgrading a secondary Content Server cluster member:
 

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<host name of server with load balancer>
CASPortNumber=<port number of server with load balancer>
```

#### Sample Configurations with Non-Clustered CAS:

- If you are upgrading a primary Content Server cluster member and autodeploy is enabled:
 

```
WEM=true
IsPrimaryClusterMember=true
```

CASHostName=<host name of server where CAS will be deployed> This must match the name of the server hosting the primary Content Server cluster member.

CASPortNumber=<port number of server where CAS will be deployed> This must match the port number of the server hosting the primary Content Server cluster member.

CASHostNameLocal=<same as CASHostName>

- If you are upgrading a secondary Content Server cluster member:

WEM=true

IsPrimaryClusterMember=false

CASHostName=<host name of server where CAS has been deployed>

CASPortNumber=<port number of server where CAS has been deployed>

5. Decompress the Rollup.zip file.

6. Edit the install.ini file in the root of the extracted Rollup folder:

- a. Set the nodisplay property to true
- b. Set the loadfile property to <path and name of renamed omii.ini from [step 1](#)>.

#### Note

Verify that you have correctly specified the file system path. For example, for Windows:

```
CSInstallDirectory=C\:/csinstall
```

- or -

```
c:\\install
```

7. Execute the silent installer script from the directory into which you extracted the Content Server 7.6 rollup installer (Rollup.zip):

- On Windows: csrollupinstall.bat -silent
- On Unix: csrollupinstall.sh -silent

8. At the installation midpoint, if manual deployment is enabled, you must deploy the Content Server web application. If WEM is selected to be installed and you are running the installer on the primary Content Server cluster member, you must also deploy the CAS web application on the server that is specified in the renamed `omii.ini` file (see [step 4 on page 21](#)).

#### Note

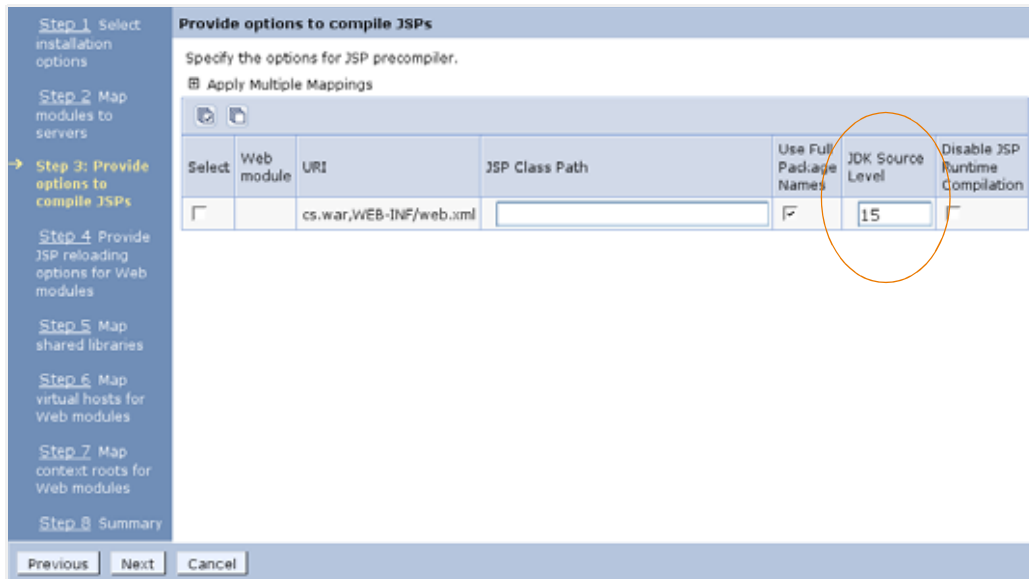
If you are clustering CAS, the rollup installation deploys only the primary member of the CAS cluster. You must configure and deploy secondary CAS cluster members manually during the post-installation process. For more information, see [“Deploying Secondary CAS Cluster Members \(CS-WEM Installations\)” on page 44](#).

- If you are using the WebLogic application server, do the following:
  - Ensure that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
  - If you are clustering CAS, before deploying the primary CAS cluster member, add the following inside the `<weblogic-web-app>` tag in the `weblogic.xml` file (located in the `cas/WEB-INF` directory):

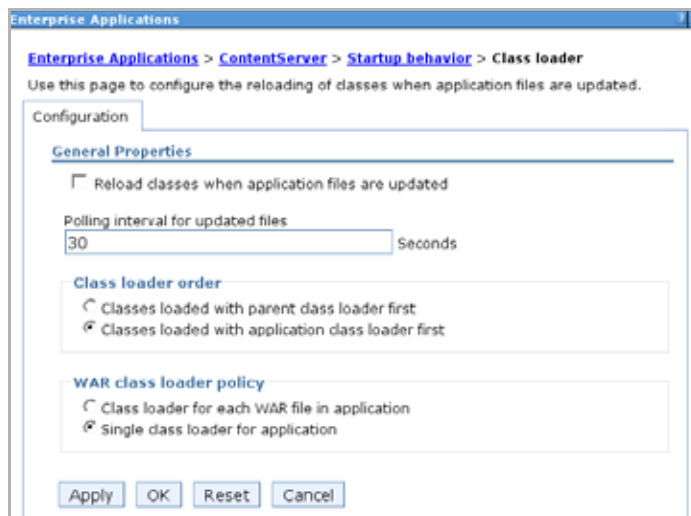
```
<session-descriptor>
  <persistent-store-type>replicated
</persistent-store-type>
  <url-rewriting-enabled>true
</url-rewriting-enabled>
</session-descriptor>
```



- If you are using the WebSphere application server, do the following:
  - Ensure that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
  - On the “Provide options to compile JSPs” screen, change the value of the “JDK Source Level” field to **15** for Content Server and for CAS, if it was deployed.



- On the “Enterprise Applications” screen, click **Content Server > Class loading and update detection**. On the screen that appears, do the following:
  - a. In the “Polling interval for updated files” field, enter **30**.
  - b. In the “Class loader order” section, select **Classes loaded with application class loader first**.
  - c. In the “WAR class loader policy” section, select **Single class loader for application**.



9. When the primary Content Server cluster member has been upgraded, repeat this procedure on all of the secondary Content Server cluster members, starting with [step 1 on page 20](#).
10. When all Content Server cluster members have been upgraded, complete the steps in [Chapter 2, “Post-Installation Steps”](#) as necessary for your configuration. Note the following:
  - Changes were made to Content Server as described in [“All Installations,” on page 27](#).
  - If you chose to migrate to log4j, changes were made to Content Server as described in [“Installations with log4j,” on page 27](#).
  - If you chose to install WEM, changes were made to Content Server as described in [“Installations with WEM Framework,” on page 28](#).

## Changes to Content Server

- [All Installations](#)
- [Installations with log4j](#)
- [Installations with WEM Framework](#)

### All Installations

The installation process installs the following components:

- System tools, on all Content Server systems. The system tools are located on the **Admin** tab of the Content Server Advanced interface. For more information about system tools, see the *Content Server Administrator's Guide*.

#### Note

To use system tools on a delivery system, you must create a dedicated site for system administration. For instructions, see “[Enabling System Tools on a Delivery System](#),” on page 34

- FatWire Content Server Developer Tools (CSDT), on all Content Server systems. CSDT is accessible only if the WEM Framework is installed. Developers who want to use CSDT must download and install the required Eclipse plug-in. For detailed instructions, see the *Guide to Content Server Developer Tools*.
- The inCache framework, on all Content Server systems. Previously, the inCache framework provided only page caching capabilities; it now provides asset caching capabilities as well. Both types of caching must be configured manually. For more information, see the *Content Server Administrator's Guide*.
- Clarkii OIE, on systems running in content management/development mode. A new property is installed in each system's `futuretense_xcel.ini` file and automatically points to the Clarkii OIE installation path, as follows:

```
xcelerate.imageeditor.clarkii4.basepath=
/<context root>/ImageEditor/clarkii4/
```

### Installations with log4j

If you chose to migrate from Content Server's existing logging system to Apache log4j, the installer made the following changes to property files in the `WEB-INF/classes` directory:

- Set log4j as Content Server's logging system in the `commons-logging.properties` file:
 

```
org.apache.commons.logging.Log=
org.apache.commons.logging.impl.Log4JLogger
```
- Added the `FWDefaultAppender` to the `log4j.properties` file:
 

```
log4j.rootLogger=INFO, FWDefaultAppender
log4j.appender.FWDefaultAppender.File=
<cs_install_dir>/futuretense.txt
log4j.appender.FWDefaultAppender.Append=true
```

```
log4j.appender.FWDefaultAppender.BufferSize=256
log4j.appender.FWDefaultAppender.MaxFileSize=10MB
log4j.appender.FWDefaultAppender.encoding=UTF-8
log4j.appender.FWDefaultAppender.layout.ConversionPattern=
    [%d] [%c{4}] %m%n
log4j.appender.FWDefaultAppender=
    org.apache.log4j.RollingFileAppender
log4j.appender.FWDefaultAppender.MaxBackupIndex=15
log4j.appender.FWDefaultAppender.layout=
    org.apache.log4j.PatternLayout
log4j.appender.FWDefaultAppender.bufferedIO=false
```

- Copied the loggers in the `commons-logging.properties` file to the `log4j.properties` file and prepend each logger name with `log4j.logger`. For example: `com.fatwire.logging.<logger name>` becomes `log4j.logger.com.fatwire.logging.<logger name>`.

These changes created two new nodes under **System Tools** on the **Admin** tab of the Content Server Advanced interface:

- The **Configure log4j** node enables general administrators to view current loggers, change logger levels, and add new loggers directly from the Advanced interface. In addition, since changed logger levels and added loggers remain in effect only until Content Server is restarted, it is possible to retain changes by copying a text version of the logger properties to the `log4j.properties` file.
- The **Log Viewer** node enables you to view, search, tail, and download the contents of the Content Server log.

## Installations with WEM Framework

If you chose to install WEM, the installer made several changes to Content Server's login page, property files, database schema, and other components. The changes are:

- [New Login Page](#)
- [New Site: AdminSite](#)
- [New Application: WEM Admin](#)
- [New Security Model](#)
- [Updated General Administrator](#)
- [New Web Application: CAS](#)
- [CAS-Protected URLs](#)
- [CAS Clustering](#)
- [Changes to Property and Configuration Files](#)
- [Schema Changes](#)

### New Login Page

Installing WEM replaces the Content Server login page with the WEM login page (see [page 39](#)), which affects the way Content Server interfaces are accessed (URL is unaffected).

## New Site: AdminSite

Installing WEM creates a new site called “AdminSite” in the Content Server Advanced interface on all Content Server systems **except** those installed in delivery mode. The new asset types `FW_View` and `FW_Application` are automatically created in Content Server’s database and enabled on the AdminSite. The asset types are used to register applications (such as the Content Server Advanced interface) and the applications’ views so they can be rendered in the WEM framework.

For more information about registration asset types, see “[Schema Changes](#),” on page 31. For more information about using the asset types to register applications, see the *WEM Framework Developer’s Guide*.

## New Application: WEM Admin

Installing the WEM Framework installs the default application called WEM Admin ([page 40](#)) for managing users’ access to Content Server and other WEM-integrated applications. WEM Admin runs on the AdminSite (**which is installed only on systems running in content management/development mode**).

## New Security Model

Installing WEM creates a new node on the **Admin** tab of the Content Server Advanced interface. The node, named **Security**, is used to create groups with privileges to operate on objects in Content Server’s database, which map to REST resources in WEM. The resources are used by applications implemented on WEM. Assigning users to a group grants them group privileges.

## Addition of Groups

Installing WEM creates two default groups: `RestAdmin` and `SiteAdmin_AdminSite` (accessible from the **Security** node on the **Admin** tab). The `RestAdmin` group allows members to connect to REST with full administrative permissions to REST resources. The `SiteAdmin_AdminSite` group allows members to connect to REST, but with fewer administrative privileges than the `RestAdmin` group allows.

## Updated General Administrator

Installing WEM adds the `fwadmin` general administrator to the `RestAdmin` group and enables the general administrator on the AdminSite, which provides access to the WEM Admin interface. Instructions for creating additional general administrators are available on [page 42](#).

### Reminder

Do not delete the `fwadmin` user. Doing so disables **all** access to Content Server when WEM is installed. Instead, to ensure security, change the password.

## New Web Application: CAS

If CAS was autodeployed during the Content Server installation process, it was deployed by default on the server hosting the primary Content Server cluster member and configured to authenticate against the Content Server database. If you need to redeploy

CAS on a different server, you must do so manually. For instructions, see [“Redeploying CAS on a New Server \(CS-WEM Installations\),”](#) on page 42.

## CAS-Protected URLs

The following URLs are protected by CAS when WEM is installed:

- wem/fatwire/\*\*
- /REST/\*\*
- /faces/jsp/\*\*
- /ContentServer? [pagename=OpenMarket/Xcelerate/UIFramework/LoginPage|OpenMarket/Xcelerate/UIFramework/ShowMainFrames, #]
- Satellite? [pagename=fatwire/insitemplating/request|OpenMarket/Xcelerate/ControlPanel/Request|OpenMarket/Xcelerate/ControlPanel/EditPanel|fatwire/wem/ui/Ping|OpenMarket/Xcelerate/UIFramework/ShowPreviewFrames, #]

## CAS Clustering

If you are clustering CAS to balance the load of user authentications for WEM, the installation process configures and deploys only the primary cluster member. Additional cluster members must be configured and deployed manually. For instructions, see [“Deploying Secondary CAS Cluster Members \(CS-WEM Installations\),”](#) on page 44.

## Changes to Property and Configuration Files

Installing WEM deploys `SSOConfig.xml`. The file is located in Content Server’s `/WEB-INF/classes` directory. The following properties are also created (or modified):

Property File	Property	Description
futuretense_xcel.ini	wem.enabled	This property is created and set to <code>true</code> if WEM is installed.
	xcelerate.userimageattr	This property is created if WEM is installed. It points to the WEM user’s image attribute, which holds image data for the user’s account and profile.
futuretense.ini	cs.ssovalidator	This property is created if WEM is installed. It points to the SSO validator plug-in. Its default value is: <code>com.fatwire.wem.sso.cas.cs.plugin.SSOValidatorPlugin</code>
	singlesignon	This existing property determines whether single sign-on is enabled. This property is set to <code>true</code> if WEM (or LDAP) is installed. <b>Caution!</b> Do not change this value to <code>false</code> if WEM is installed. Doing so causes login to fail.

## Schema Changes

The rollup installer makes several changes to schema when it installs the WEM option.

### Updates to SystemUserAttr

The `urlvalue` column is added to the `SystemUserAttr` table. In the `SystemInfoTable`, the value of `defdir` for the `SystemUserAttr` table is updated to:  
<shared\_dir>/usrurl/

### New Tables

- When the WEM Framework is installed, the following tables are created in the database of all Content Server systems **except those in delivery mode**:
  - `FW_Application`
  - `FW_Application_Dim`
  - `FW_Application_DimP`
  - `FW_View`
  - `FW_View_Dim`
  - `FW_View_DimP`

The `FW_Application` and `FW_View` asset types are used to register applications and their views as described in “[New Site: AdminSite,](#)” on page 29.

- When the WEM Framework is installed, the following tables are created in the database of **all Content Server systems**:
  - `FW_CSGroups`
  - `FW_CSSecurityConfig`
  - `FW_CSUserGroups`

The tables above support the creation of REST security groups and configurations.





## Chapter 2

# Post-Installation Steps

Perform the steps in this chapter as required for your configuration:

- [Reapplying Customizations](#)
- [Configuring Browsers](#)
- [Enabling System Tools on a Delivery System](#)
- [Verifying Content Server Installations Running WEM Framework](#)
- [Redeploying CAS on a New Server \(CS-WEM Installations\)](#)
- [Deploying Secondary CAS Cluster Members \(CS-WEM Installations\)](#)
- [Enabling the Clarkii Online Image Editor](#)
- [Setting Up inCache](#)
- [Setting Up Apache log4j](#)
- [Setting Up Content Server Developer Tools](#)
- [Installing the Database Performance Utility](#)
- [Installing Language Packs](#)
- [Installing Remote Satellite Server](#)

## Reapplying Customizations

During the Content Server 7.6 installation, customizations that were made to your previous Content Server application may have been overwritten. You can retain these customizations as follows:

- Find customizations in the installation directory, `Shared` directory, and database that you backed up during pre-installation (page 8) and reapply them. For example, since default Content Server elements are overwritten during installation, find default elements that were customized for your previous Content Server application in the backed up `Shared` directory and reapply the customizations to the Content Server 7.6 default elements.
- Find customizations in the archived version of the `cs.war` file in the `<cs_install_dir>/ominstallinfo/app` directory and reapply them. For example, since configuration files such as `cs-cache.xml`, `ss-cache.xml`, and, for portal installations, `portlet.xml` are overwritten during installation, decompress the archived version of `cs.war`, find configuration files that were customized, and reapply the customizations to the Content Server 7.6 configuration files.

For detailed instructions on reapplying customizations, see the *Content Server Backup and Recovery Guide*.

## Configuring Browsers

Ensure that the browsers you use to access the Content Server 7.6 Advanced, Dash, and InSite interfaces are configured to check for new versions of stored pages upon each visit. This is particularly important on Content Server development systems.

## Enabling System Tools on a Delivery System

On a delivery system, to access the **System Tools** node on the **Admin** tab of the Content Server Advanced interface, you must create a dedicated site for system administration and grant the general administrator access to the site.

### To enable system tools on a delivery system

1. Log in to the Advanced interface as the `fwadmin` general administrator.
2. Create the system administration site:
  - a. On the **Admin** tab, expand **Sites**, and double-click **Add New**.
  - b. Enter the name and description for the site and click **Add Site**.
3. Grant the general administrator access to the site:
  - a. On the **Admin** tab, expand **Sites**, expand the new site, and double-click **Users**.
  - b. Enter the general administrator's user name and click **Select**.
  - c. Click the **Edit** icon next to the user name.
  - d. Select the **AdvancedUser** and **GeneralAdmin** roles and click **Save**.

The **System Tools** node on the **Admin** tab is now available to the general administrator. For detailed information about system tools, see the *Content Server Administrator's Guide*.

## Verifying Content Server Installations Without WEM Framework

Verify the installation by logging in to Content Server as an administrator.

### Logging in to the Advanced Interface

1. Point your browser to the following URL:

`http://<hostname>:<port>/<context>/Xcelerate/LoginPage.html`

Content Server displays the Advanced interface login form:



**FatWire** | Content Server 7

User Name:

Password:

Login Reset

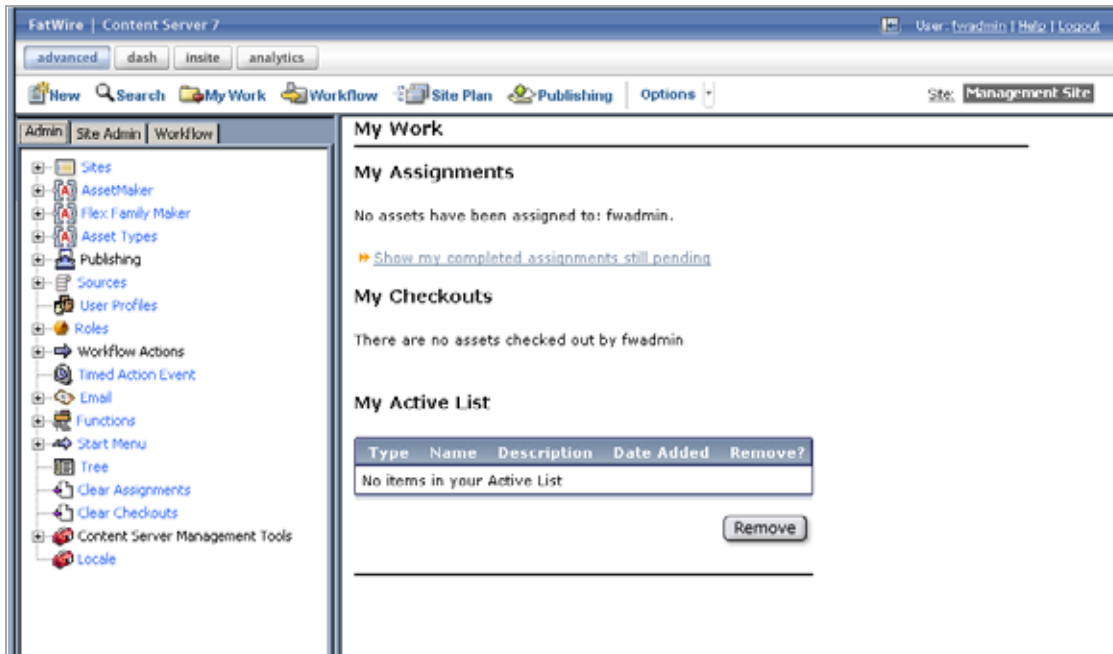
 **Login: advanced**  
Forgot your password?  
Don't have an account?

**Installed Products:**  
Content Server 7.6  
CS-Engage 7.6.0  
Commerce Connector 7.6.0

2. Log in with the credentials of the `fwadmin` general administrator.
3. Click **Login**.

Depending on how many sites are configured in Content Server, one of the following happens:

- If no sites are configured, you are logged in to the built-in Content Server management site. Only system administration functionality is available.



- If only one site is configured, you are logged in to that site.



- If more than one site is configured, Content Server displays the “Select Site” screen. Select the site you wish to log in to.

**You have logged in as fwadmin**

Select a site that you want to work on:

Site	Description	Assigned Role
<a href="#">BurlingtonFinancial</a>	Burlington Financial	GeneralAdmin, ArtworkEditor, Approver, ContentEditor, WorkflowAdmin, Analyst, Pricer, Marketer, SiteAdmin, Checker, MarketingAuthor, MarketingEditor, Author, Editor, ContentAuthor, Expert, ProductAuthor, ProductEditor, DocumentAuthor, DocumentEditor, Designer, ArtworkAuthor
<a href="#">FirstSite1</a>	FirstSite Mark II	ArtworkEditor, GeneralAdmin, Approver, ContentEditor, WorkflowAdmin, Analyst, Pricer, Marketer, SiteAdmin, Checker, MarketingAuthor, MarketingEditor, Author, Editor, ContentAuthor, Expert, ProductAuthor, ProductEditor, DocumentAuthor, ArtworkAuthor, Designer, DocumentEditor
<a href="#">GE Lighting</a>	GE Lighting	Designer, SiteAdmin, WorkflowAdmin, GeneralAdmin

[\[Log in again\]](#)

## Logging in to the Dash Interface

1. Point your browser to the following URL:

`http://<hostname>:<port>/<context>`

Content Server displays the Dash interface login page.

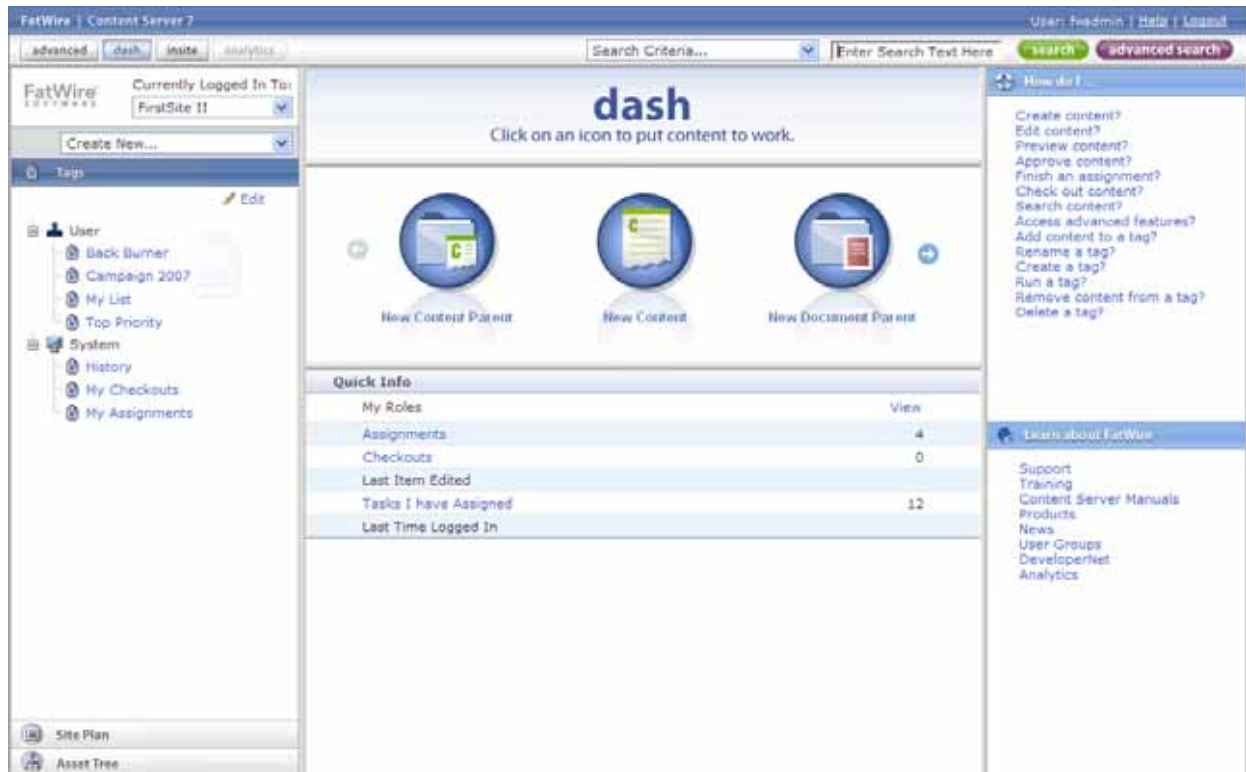


2. Log in with the credentials of the fwadmin general administrator.
3. Click **Login**.

Depending on how many sites are configured in Content Server, one of the following happens:

- If no sites are configured, Content Server notifies you by displaying a message. You will not be able to log in to the Dash interface until at least one site exists on your system.

- If only one site is configured, you are logged in to that site.



- If more than one site is configured, Content Server displays the “Select Site” screen. Select the site you wish to log in to.

You are currently logged in as 'fwadmin'

Select a site that you want to work on:

Select	Name	Description	Roles
<input type="radio"/>	BurlingtonFinancial	Burlington Financial	WorkflowAdmin, SiteAdmin, GeneralAdmin
<input type="radio"/>	GE Lighting	GE Lighting	Designer, WorkflowAdmin, SiteAdmin, GeneralAdmin
<input type="radio"/>	HelloAssetWorld	Hello Asset World	WorkflowAdmin, GeneralAdmin
<input type="radio"/>	FirstSiteII	FirstSite Mark II	GeneralAdmin

[ [Log in again](#) ]

## Verifying Content Server Installations Running WEM Framework

1. Point your browser to the following URL:  
`http://<hostname>:<port>/<context>/login`
2. Log in with the credentials of the `fwadmin` general administrator.



FatWire Web Experience Management Version 1.0

SECURE USER LOGIN

FatWire SOFTWARE

Username

Password

[Forgot password?](#)

Remember me

3. Click **Login**.
4. Select **AdminSite** and click the **Admin** icon (the first icon).



FatWire Web Experience Management Version 1.0

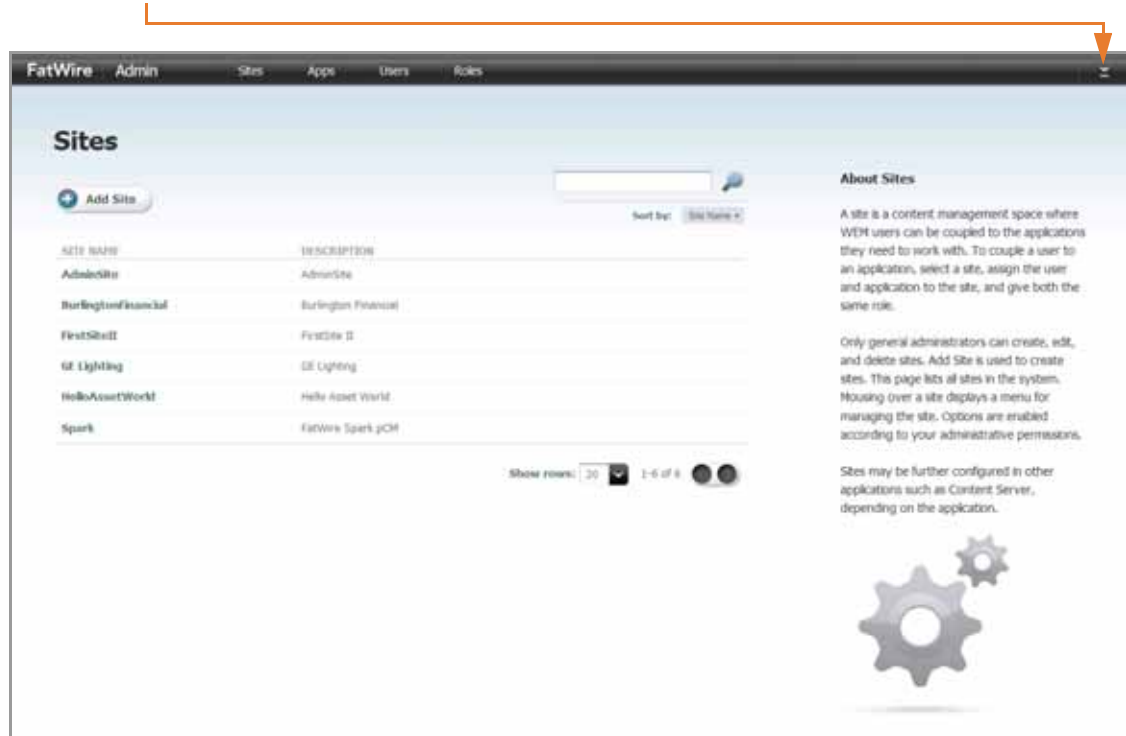
FatWire SOFTWARE

Site  
AdminSite

App

[Login again](#)

- Click the arrow at the right of the WEM interface, then click the pin icon.



WEM displays the icons of registered applications assigned to the Admin Site. The **Sites**, **Users**, and **Roles** pages list all sites, users, and roles in the system. The **Apps** page lists default applications running on WEM: Content Server Advanced, Dash, and InSite interfaces.

WEM Admin



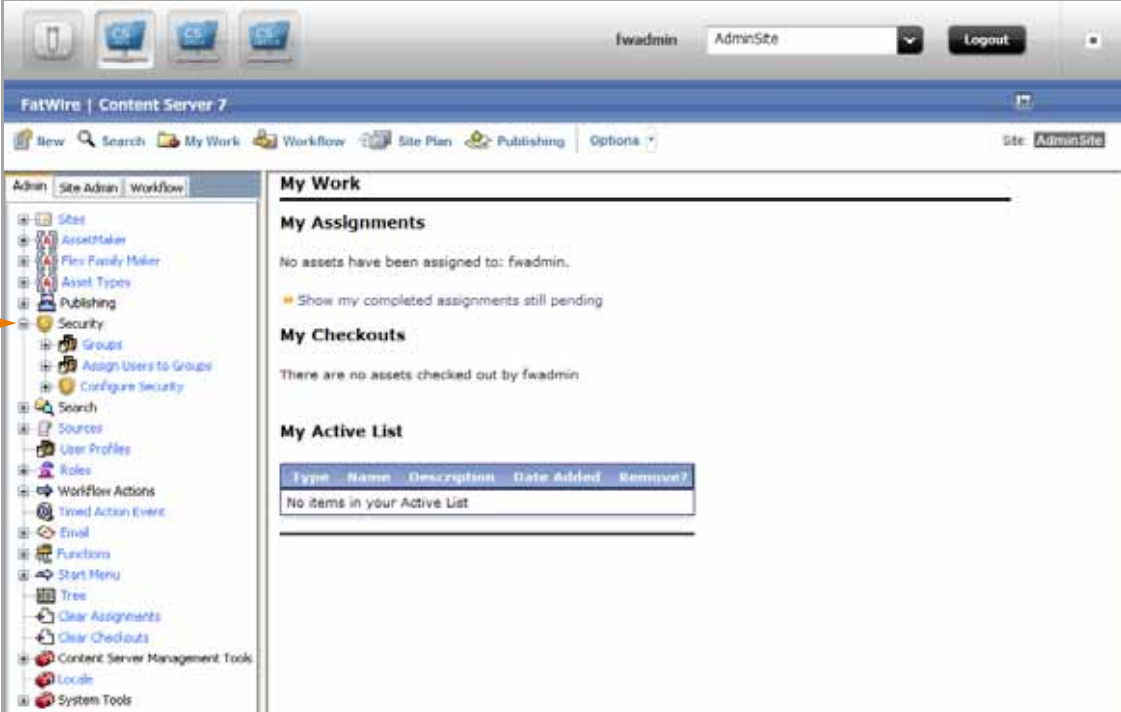


- Verify that the Content Server Advanced and Dash interfaces are displayed as shown on pages 36–38.

### Note

With WEM installed, the Content Server Advanced interface displays the **Security** node on the **Admin** tab (shown below), which supports the configuration of groups with privileges to REST resources that are used by applications running on WEM.

### Security Node (Content Server Advanced Interface)



The screenshot displays the FatWire Content Server 7 Admin interface. The top navigation bar includes the user 'fwadmin' and the site 'AdminSite'. The left navigation pane is expanded to the 'Admin' tab, and the 'Security' node is highlighted with an orange arrow. The main content area shows the 'My Work' section with 'My Assignments', 'My Checkouts', and 'My Active List' sections.

Type	Name	Description	Date Added	Remove?
No items in your Active List				

### Note

The `fwadmin` general administrator was added to the `RestAdmin` group in order to connect to REST services and therefore to the WEM Admin interface. **Do not delete this general administrator.**

If you need to create additional general administrators, follow the steps below:

1. Log in to the Advanced interface as the `fwadmin` general administrator.
2. Create a new general administrator.
  - Create the user:  
**Admin tab > Content Server Management Tools > User.** For “Access Privileges” (ACLs), select at least: **Browser, ElementReader, PageReader, UserReader, xceditor, xceladmin**
  - Enable the user on AdminSite:  
**Admin tab > Sites > AdminSite > Users > enter username > Select > Edit (pencil icon) > select roles, at least: AdvancedUser, DashUser, GeneralAdmin, SiteAdmin, WorkflowAdmin**
  - Assign the user to the `RestAdmin` group:  
**Admin tab > Security > Assign Users to Groups > Add New > assign to RestAdmin group.**

User Name	Groups
Arthur	'RestAdmin'
ContentServer	'RestAdmin'
fwadmin	'RestAdmin'

Add New

Site administrators on Content Server systems running the WEM Framework must be manually assigned to the `SiteAdmin_AdminSite` group, a default REST security group similar to `RestAdmin`, but with fewer administrative privileges.

## Redeploying CAS on a New Server (CS-WEM Installations)

### Note

This section applies to non-clustered CAS or a primary CAS cluster member.

If you installed WEM and need to redeploy CAS on a new server, you must do so manually:

1. Remove CAS from the server where it was deployed previously.
2. Deploy `cas.war` (or `cas.ear`) on the new server. If you are clustering CAS, the server is defined as the primary CAS cluster member.

3. Reconfigure Content Server to detect CAS by updating the `casURL` property in the `SSOConfig.xml` file in the `WEB-INF/classes` directory of the `cs.war` file:
  - **For non-clustered CAS**

```
property name="casUrl" value="http://<CAS host name>:<CAS
port number>/cas"
```
  - **For the primary CAS cluster member**

```
property name="casUrl" value="http://<load balancer host
name>:<load balancer port number>/cas"
```
4. Copy the following CAS configuration files from the `<cs_install_dir>/bin` directory to a directory on the new server:
  - `cas.properties`
  - `host.properties`
  - `jbossTicketCacheReplicationConfig.xml`
5. Update the CAS configuration files:
  - **For non-clustered CAS**
    - In the `cas.properties` file, update the following properties:
 

```
cas.securityContext.serviceProperties.service=http://
<CAS host name>:<CAS port number>/cas/services/
j_acegi_cas_security_check
cas.securityContext.casProcessingFilterEntryPoint.
loginUrl=http://<CAS host name>:<CAS port number>/
cas/login
cas.securityContext.ticketValidator.casServerUrlPrefix
=http://<CAS host name>:<CAS port number>/cas
```
    - In the `host.properties` file, update the following property:
 

```
host.name=cas.<CAS host name>-1
```
    - In the `jbossTicketCacheReplicationConfig.xml` file, do the following:
      - In the "ClusterName" attribute, replace `TreeCache-Cluster` with a unique name:
 

```
<attribute name="ClusterName">TreeCache-Cluster
</attribute>
```
      - In the "ClusterConfig" attribute, update the following parameter:
 

```
bind_addr="host name of server where cluster
member will be deployed"
```
  - **For the primary CAS cluster member**

Update the `host.properties` and `jbossTicketCacheReplicationConfig.xml` files as described in [step 2](#) and [step 3 on page 44](#).
6. On the new server, add the directory containing the CAS configuration files to the `CLASSPATH` environment variable. If the class path is not set properly, CAS will not start.

## Deploying Secondary CAS Cluster Members (CS-WEM Installations)

If you installed WEM and are clustering CAS to balance the load of user authentications, the installation process configured and deployed only the primary member of the CAS cluster. You must configure and deploy secondary CAS cluster members manually.

### To configure and deploy a secondary CAS cluster member

1. Copy the following configuration files from the `<cs_install_dir>/bin` directory of the primary member to the `<cs_install_dir>/bin` of the secondary member:

- `cas.properties`
- `host.properties`
- `jbossTicketCacheReplicationConfig.xml`

2. Update the following property in the `host.properties` file:

```
host.name=cas-<host name of server where cluster member will  
be deployed>-<cluster member number>
```

#### Note

The host name and member number should be unique for each cluster member. For example, for a primary and secondary member, the property might differ as follows:

```
host.name=cas-10.120.12.123-1  
host.name=cas-10.120.12.127-2
```

3. Update the `jbossTicketCacheReplicationConfig.xml` file as follows:

- In the "ClusterName" attribute, replace `TreeCache-Cluster` with a unique name:

```
<attribute name="ClusterName">TreeCache-Cluster  
</attribute>
```

#### Note

This name must be the same for all cluster members. If you are using more than one CAS cluster, make sure to use a different name for each cluster.

- In the "ClusterConfig" attribute, update the following parameters:
 

```
<UDP mcast_addr="multicast address"
      mcast_port="multicast port"
      bind_addr="host name of server where cluster member
      will be deployed"
      ip_ttl="number of network hops between cluster
      members"
      ... />
```

#### Note

The `mcast_addr` and `mcast_port` parameters are set to 239.555.0.0 and 48866 by default. Since these values must be the same for all cluster members, if you change them for one member, be sure to change them for all other members as well.

The `ip_ttl` parameter is set to 0 by default. If cluster members are on the same host, retain this default value. However, if cluster members are on the same subnet, set `ip_ttl` to 1, or if cluster members are on the same site, set `ip_ttl` to 32.

4. On the application server of the secondary cluster member, add `<cs_install_dir>/bin` to the `CLASSPATH` environment variable. If the class path is not set properly, CAS will not start.
5. The `cas.war` file generated for the primary member is the clustered and generic version of CAS. Deploy this `cas.war` file on the application server of the secondary cluster member.

#### Note

If you are using the WebLogic application server, before deploying the secondary CAS cluster member, add the following to the `<weblogic-web-app>` tag in the `weblogic.xml` file (located in `cas/WEB-INF`):

```
<session-descriptor>
  <persistent-store-type>replicated
</persistent-store-type>
  <url-rewriting-enabled>true
</url-rewriting-enabled>
</session-descriptor>
```

6. Repeat this process for each additional cluster member.

## Enabling the Clarkii Online Image Editor

Because Clarkii OIE is not enabled by the installation process, your existing Online Image Editor is displayed in attributes that are configured to use an online image editor. To enable Clarkii OIE in Content Server's user interfaces, configure the attribute editor to specify Clarkii OIE (and its properties) for selected fields in selected asset types. For detailed instructions, see the *Content Server Developer's Guide*.

## Setting Up inCache

If you rolled up from Content Server 7.5 Patch 3, 4, or 5 and the inCache framework was not enabled, its page caching capabilities are not automatically enabled in version 7.6 (the traditional page caching method runs by default). inCache's new asset caching capabilities are not automatically enabled in version 7.6 either. Both types of caching must be configured manually. Configuring inCache page caching creates the `FW_RegenCriteria` table in Content Server's database during runtime. The `FW_InvalidationMemory` table is created in Content Server's database when any caching first runs (even if inCache is not set up).

If you wish to set up inCache page caching and asset caching, see the *Content Server Administrator's Guide*.

## Setting Up Apache log4j

If you did not migrate to Apache log4j during installation, you can manually switch to log4j by updating the `commons-logging.properties` and `log4j.properties` files in the `WEB-INF/classes` directory. For detailed instructions, see the *Content Server Administrator's Guide*.

## Setting Up Content Server Developer Tools

FatWire Content Server Developer Tools (CSDT) are accessible only if the WEM Framework is installed. Developers who want to use CSDT must download and install the required Eclipse plug-in. For detailed instructions, see the *Guide to Content Server Developer Tools*.

## Installing the Database Performance Utility

To improve Content Server performance, a database performance utility is provided with this release. This utility creates additional indexes for database tables. It can be used on CM- and delivery-mode systems.

### To import the indexing utility

1. Unzip `DatabasePerformanceUtility.zip` (located in `Misc/DatabasePerformanceUtility/`).
2. Import the `sitecatalog` and `elementcatalog` into Content Server using `catalogmover` (located in the Content Server installation directory).
3. Execute the following:

```
http://<hostname>:<port>/<context-root>/
  Install?COMMANDNAME=READURL&USERNAME=ContentServer&PASSWORD=
  <password>&pagename=OpenMarket/Xcelerate/Installation/Asset/
  AddIndex
```

## Installing Language Packs

By default, Content Server interfaces display in the English language. If you want your Content Server interfaces to display in additional languages such as German, French, Spanish, Italian, or Japanese, you must install a language pack for each additional language. For instructions, see the *Internationalization Settings Guide*.

## Installing Remote Satellite Server

Remote Satellite Server is used for load balancing. Installation instructions are available in the *Installing Satellite Server Guide*.

### Note

- To upgrade Remote Satellite Server, it is not sufficient to copy `jar` files from the Content Server 7.6 installation. Instead, you must run the Satellite Server 7.6 installer, which you can obtain from FatWire Technical Support at <http://www.fatwire.com/support>.
- If you plan to enable the inCache system for page caching, you will also have to configure Satellite Server (both co-resident and remote) to support inCache. Instructions are available in the *Content Server Administrator's Guide*.

