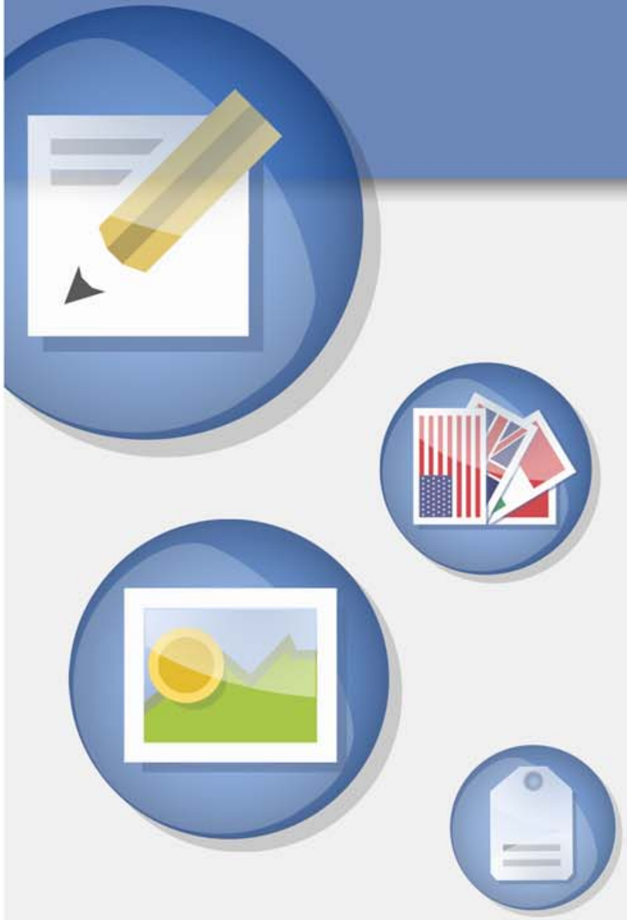
FatWire | Content Server 7

Version 7. 6 Patch 2

Rollup Installation Guide



Document Revision Date: Jan. 31, 2012

FatWire®
SOFTWARE

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.

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/.

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.

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: Jan. 31, 2012
Product Version: 7. 6 Patch 2

FatWire Headquarters
FatWire Corporation
330 Old Country Road
Suite 303
Mineola, NY 11501

Table of Contents

About This Guide

This guide describes the process of rolling up to FatWire Content Server 7.6 Patch 2.

Who Should Use This Guide

This guide is intended for installation engineers with experience installing and configuring enterprise-level software such as databases, application servers, and content management related products.

Related Documents

See the following documents in the FatWire documentation set:

- *FatWire Content Server Administrator's Guide*
- *FatWire Content Server Developer's Guide*
- *FatWire Content Server Guide to Content Server Developer Tools*
- *FatWire Web Experience Management Framework Administrator's Guide*
- *FatWire Web Experience Management Framework Developer's Guide*
- *FatWire Content Server Advanced User's Guide*
- *FatWire Content Server Dash User's Guide*

Conventions

The following text conventions are used in this guide:

- **Boldface** type indicates graphical user interface elements that you select.
- *Italic* type indicates book titles, emphasis, or variables for which you supply particular values.
- `Monospace` type indicates file names, URLs, sample code, or text that appears on the screen.
- **`Monospace bold`** type indicates a command.

Third-Party Libraries

FatWire Content Server 7.6 patch 2 and its applications include third-party libraries. For additional information, see *FatWire Content Server 7.6 Patch 2: Third-Party Licenses*.

Chapter 1

Installing FatWire Content Server 7.6 Patch 2

This chapter provides instructions for installing FatWire Content Server 7.6 Patch 2.

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 Patch 2 introduces resultset caching over the inCache framework as an alternative to storing resultsets in hash tables. Both frameworks use Java memory. Once resultset caching over in Cache is enabled, the Resultset Cache tool is displayed in the System Tools node, on the Admin tab in Content Server's Advanced interface. Enabling resultset caching over inCache does not require enabling either page or asset caching over inCache. More information about the resultset cache tool is available in the *Content Server Administrator's Guide*.

Content Server patches are cumulative. This patch includes features and options from previous releases beginning with Content Server 7.5 Patch 3, as described below. If any option is supported and enabled in your current installation, it remains enabled when you finish installing this patch. Features and options included in this patch are the following:

- System Tools, which provide general administrators with a range of diagnostic utilities for troubleshooting directly from the Content Server Advanced interface. The diagnostic utilities enable 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 (described 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 team members. CSDT is accessible only if the WEM Framework is installed (see below). For information about CSDT, see the *Guide to Content Server Developer Tools*.
- 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 and asset caching capabilities must be configured manually. If inCache is supported but not set up in your current installation, your current page and asset caching methods will run by default when Content Server 7.6 Patch 2 is installed. Information about setting up inCache page caching and asset caching is available in the *Content Server Administrator's Guide*.
- 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 database performance enhancement utility, which can be used on systems running in either delivery or CM/development mode to create additional indexes for database tables. If you wish to use this utility in Content Server 7.6.*x*, 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 Patch 2, 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, changes that will be made by the installer, and the post-installation steps.
- Start with a Content Server 7.5.*x* or 7.6.*x* installation. You will run the rollup installer on all systems in your environment. There are two system types: development/content management, and delivery. Development systems and content management systems are of the same type, but are used for different purposes.

  The Content Server 7.6 patch rollup installer detects and reuses the system type (development/content management, or delivery) and the deployment mode (automatic or manual) that were selected during the Content Server 7.5.*x* (or 7.6.*x*) installation process. For example, if Content Server 7.5 was installed as a delivery system and deployed automatically, the Content Server 7.6 Patch 2 rollup installer continues to treat the system as a delivery system and deploys automatically.

> **Note**
>
> - 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.
> - A primary Content Server cluster member cannot be reconfigured to be a secondary cluster member, and vice versa.

- 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 36.
  - 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 36.
- 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. For example: `-XX:MaxPermSize-128m`
    - 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 Patch 2 is first started.
  - `commons-dbcp-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 the WEM Framework is installed on your current Content Server system, do the following:
  - Undeploy and delete the previous CAS installation before beginning the rollup.
  - Modify the `omii.ini` file for all Content Server cluster members by setting the values of `CASHostName` and `CASPortNumber` fields as shown below:

> **Note**
>
> Avoid performing this step during the process of using the graphical installer (you will have to stop the installer, change the `omii.ini` file, and rerun the installer).

Field	CAS	Value
`CASHostName`	Clustered	Host name of the server running the load balancer.
	Non-clustered	Host name of the server where CAS will be deployed.

Field	CAS	Value
`CASPortNumber`	Clustered	Port number of the server running the load balancer.
	Non-clustered	Port number of the server where CAS will be deployed.

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 allows you to perform an automated installation based on the configuration information provided in the `omii.ini` file. For more information about these installation procedures, see "Running the GUI Installer," on page 14 and "Upgrading Silently," on page 23.

- 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, or install applications such as FatWire Community Server and FatWire Gadget Server, 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.

    Answers to the following questions will help you determine your CAS deployment information:

    Which deployment mode was enabled for Content Server 7.5 and how does mode determine the deployment process?

    If you are running the installer on the *primary Content Server cluster member* and WEM is to be installed or upgraded, the deployment scenarios are the following:

    - If automatic deployment is in effect, the installer will deploy Content Server and CAS on the same server.

    - If the installer detects the deployment mode to be manual, you will deploy Content Server. You will also deploy CAS. However, unlike the installer, you can deploy CAS either on the same server as the primary Content Server cluster member, or on a separate server.

Once the installation process is complete, and you want to move CAS to a different server, you must manually redeploy CAS in the post-installation process.

How are secondary CAS cluster members deployed?

During the installation process, you will provide CAS deployment information for the secondary CAS cluster members. You will configure and deploy those members manually, as shown in "Deploying Secondary CAS Cluster Members (CS-WEM Installations)," on page 45.

- What types of changes are made to Content Server when the WEM Framework is installed?

  Caution!

  When the WEM Framework 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 the WEM Framework is installed. Instead, to ensure security, change the password.

  For information about changes that are made to Content Server when WEM is installed, see "Installations with WEM Framework," on page 31. 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 30.

  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 Patch 2 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 *Installing Satellite Server.*

Rollup Installation Procedures

Complete one of the following procedures to install Content Server 7.6 Patch 2:

- Running the GUI Installer
- Upgrading Silently

Running the GUI Installer

Note

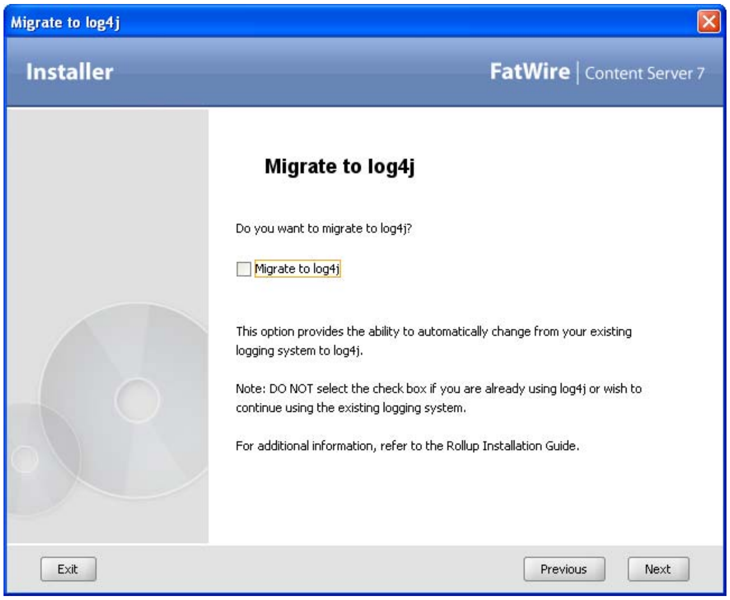
Before starting this procedure, ensure that all pre-installation steps (page 9) have been completed.

The rollup installer contains online help. When additional help is required, the procedure below displays the selected installer screen and provides detailed information about the data you are prompted to enter.

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 Patch 2 rollup installer (`Rollup.zip`):
   - On Windows: `csrollupinstall.bat`
   - On Unix: `csrollupinstall.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.



Migrate to log4j

Do you want to migrate to log4j?

□ Migrate to log4j

This option provides the ability to automatically change from your existing logging system to log4j.

Note: DO NOT select the check box if you are already using log4j or wish to continue using the existing logging system.

For additional information, refer to the Rollup Installation Guide.

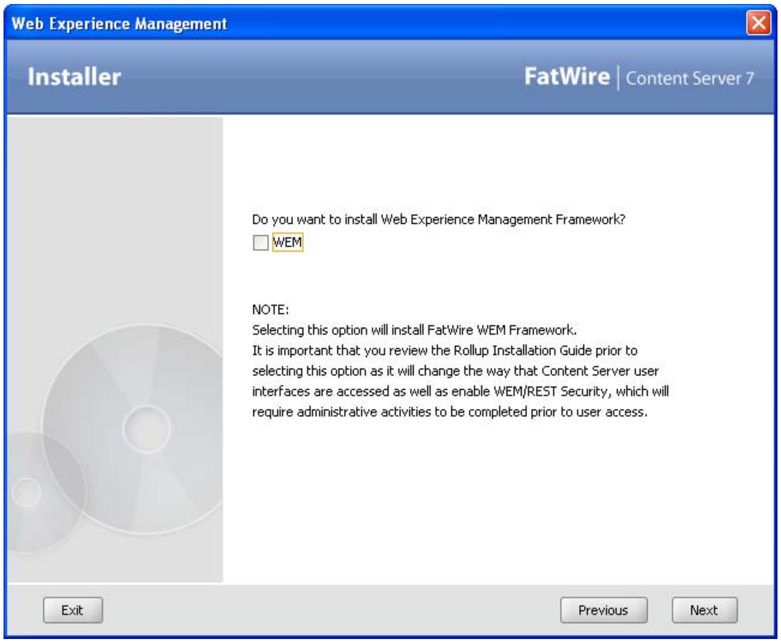
> **Note**
>
> If you do not migrate to log4j during the installation process, you can switch to log4j at a later time. For instructions, see the *Content Server Administrator's Guide*.

4. This step concerns the WEM Framework and Content Server Developer Tools (CSDT). Select the **WEM** check box if any 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 31. See also the *WEM Framework Administrator's Guide* and the *WEM Framework Developer's Guide.*



Do you want to install Web Experience Management Framework?
□ WEM

NOTE:
Selecting this option will install FatWire WEM Framework.
It is important that you review the Rollup Installation Guide prior to selecting this option as it will change the way that Content Server user interfaces are accessed as well as enable WEM/REST Security, which will require administrative activities to be completed prior to user access.

5. If you are not installing or upgrading the WEM Framework, skip to step 6 on page 21 and complete any steps that apply to your installation. Otherwise, continue with the current step.

   In this step, you will enter CAS deployment information, which depends on whether you are installing or upgrading the WEM Framework on a primary or secondary Content Server cluster member.

   > **Note**
   >
   > When rolling up the primary Content Server cluster member, note the following:
   >
   > - If automatic deployment is in effect, the installer will deploy Content Server and CAS on the same server. Once the installation process is complete, you can manually redeploy CAS on a different server, as described in "Redeploying CAS on a New Server (CS-WEM Installations)," on page 47.
   > - If manual deployment is in effect, you will deploy Content Server. You will also deploy CAS either on the same server, or on a separate server. Once the installation process is complete, and you decide to redeploy CAS on a different server, you can do so manually as described in "Redeploying CAS on a New Server (CS-WEM Installations)," on page 47.

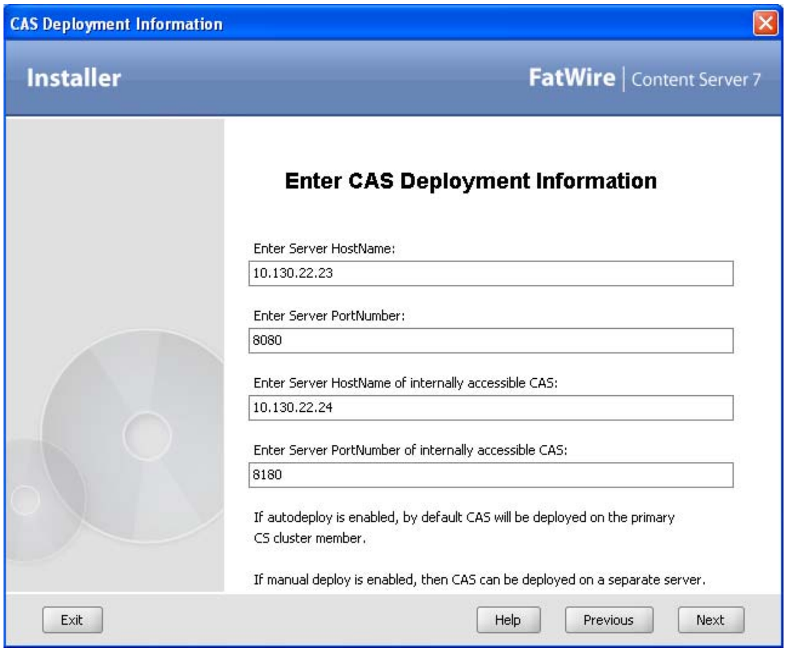
   To enter CAS deployment information, do one of the following:

   - To Install the WEM Framework
   - To Upgrade the WEM Framework

To Install the WEM Framework

a. Install the WEM Framework on the primary Content Server cluster member, do the following:

1) Fill in the fields, using Table 1 as a reference.



Enter CAS Deployment Information

Enter Server HostName: 10.130.22.23

Enter Server PortNumber: 8080

Enter Server HostName of internally accessible CAS: 10.130.22.24

Enter Server PortNumber of internally accessible CAS: 8180

If autodeploy is enabled, by default CAS will be deployed on the primary CS cluster member.

If manual deploy is enabled, then CAS can be deployed on a separate server.

Table 1: Fields for installing on a primary Content Server cluster member

Field	Value
Server HostName	External host name of the server running the single CAS instance or CAS load balancer. **Note:** "External host name" is the name of the host that will be accessed by end users.
Server PortNumber	External port number of the server running the single CAS instance or CAS load balancer. **Note:** "External port number" is the number of the port that will be accessed by end users.
Server HostName Internally Accessible CAS	Internal host name of the server running the single CAS instance or CAS load balancer. **Note:** If the host name is not accessible internally by Content Server's host machine, enter either the internally recognized host name of the CAS instance or the name of the internal CAS load balancer. Otherwise, enter the value of `Server HostName` (in the first field).

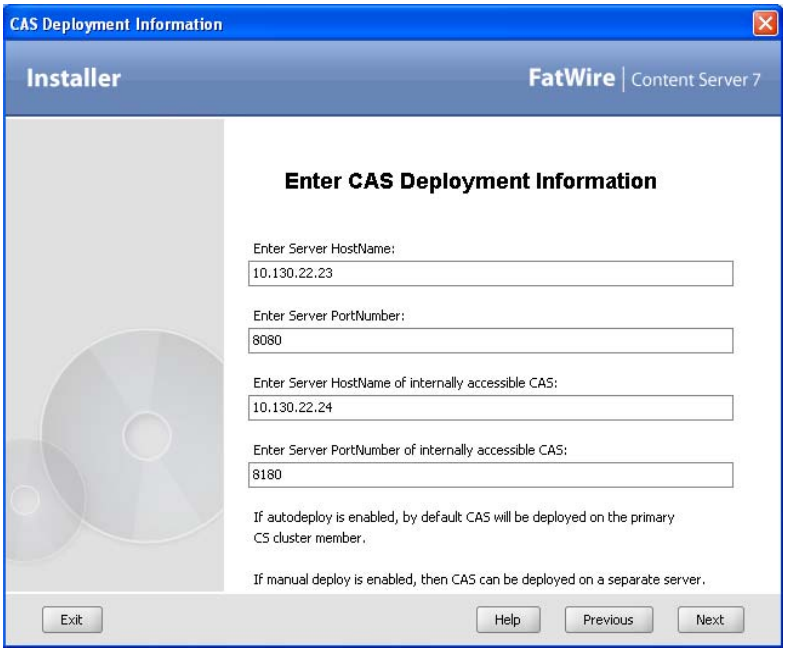
Table 1: Fields for installing on a primary Content Server cluster member *(continued)*

Field	Value
Server PortNumber Internally Accessible CAS	Internal port number of the server running the single CAS instance or CAS load balancer. **Note:** If the host name is not accessible internally by Content Server's host machine, enter either the internally recognized port number name of the CAS instance or the port number of the internal CAS load balancer. Otherwise, enter the value of `Server PortNumber` (in the second field).

2) Click **Next** and continue with step 6 on page 21.

b. If you are installing the WEM Framework on a secondary Content Server cluster member, do the following:

1) Fill in the fields with the same values that you used in step a on page 17 (Table 1, on page 17).



Enter CAS Deployment Information

Enter Server HostName: 10.130.22.23

Enter Server PortNumber: 8080

Enter Server HostName of internally accessible CAS: 10.130.22.24

Enter Server PortNumber of internally accessible CAS: 8180

If autodeploy is enabled, by default CAS will be deployed on the primary CS cluster member.

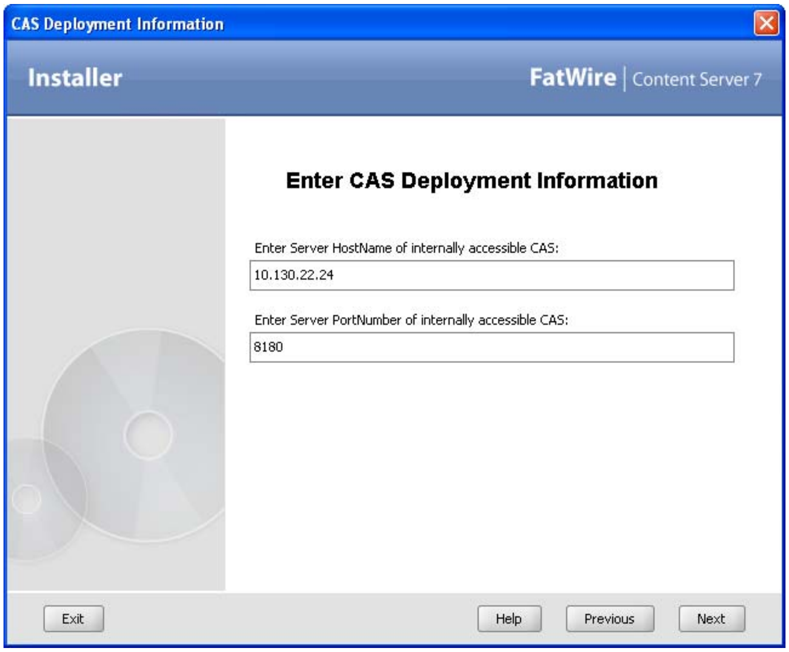
If manual deploy is enabled, then CAS can be deployed on a separate server.

2) Click **Next** and continue with step 6 on page 21.

To Upgrade the WEM Framework

a. If you are upgrading the primary Content Server cluster member, do the following:

1) Fill in the fields, using Table 2 as a reference.



Enter CAS Deployment Information

Enter Server HostName of internally accessible CAS:
10.130.22.24

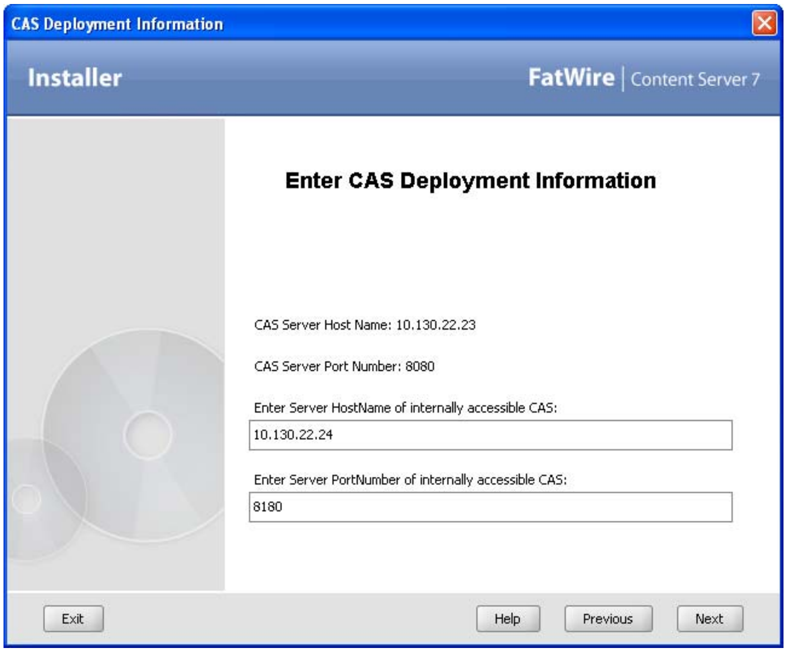
Enter Server PortNumber of internally accessible CAS:
8180

Table 2: Fields for upgrading on a primary Content Server cluster member

Field	Value
Server HostName Internally Accessible CAS	Internal host name of the server running the single CAS instance or CAS load balancer. **Note:** If the host name is not accessible internally by Content Server's host machine, enter the internally recognized host name of the CAS instance or the internal CAS load balancer. Otherwise, enter the value of the `Server HostName` (the first field in Table 1, on page 17).
Server PortNumber Internally Accessible CAS	Internal port number of the server running the single CAS instance or CAS load balancer. **Note:** If the host name is not accessible internally by Content Server's host machine, enter the internally recognized port number of the CAS instance or the internal CAS load balancer. Otherwise, enter the value of `Server PortNumber` (the second field in Table 1, on page 17).

2) Click **Next** and continue with step 6 on page 21.

b. If you are upgrading a secondary Content Server cluster member, do the following:



Enter CAS Deployment Information

CAS Server Host Name: 10.130.22.23

CAS Server Port Number: 8080

Enter Server HostName of internally accessible CAS: 10.130.22.24

Enter Server PortNumber of internally accessible CAS: 8180

Note

The first two fields in the screen above display the values that you set in the “Pre-Installation Steps,” as shown on page 11.

1) Fill in the “Server HostName (non load balancer)” and “Server PortNumber (non load balancer)” fields, using Table 3 as a reference.

Table 3: Fields for upgrading on a secondary Content Server cluster member

Field	Value
Server HostName Internally Accessible CAS	Internal host name of the server running the single CAS instance or CAS load balancer. **Note:** If the host name is not accessible internally by Content Server’s host machine, enter either the internally recognized host name of the CAS instance or the name of the internal CAS load balancer. Otherwise, enter the value of `Server HostName` (in the first field).

Table 3: Fields for upgrading on a secondary Content Server cluster member *(continued)*

Field	Value
Server PortNumber Internally Accessible CAS	Internal port number of the server running the single CAS instance or CAS load balancer. **Note:** If the host name is not accessible internally by Content Server's host machine, enter either the internally recognized port number of the CAS instance or the port number of the internal CAS load balancer. Otherwise, enter the value of `Server PortNumber` (in the second field).

2) Click **Next**.

6. Continue to populate the installer screens with the requested information. At the midpoint of the installation process, complete the following steps, as necessary for your system:

   a. If you are using a CAS cluster or you have used a name other than that of the current machine DNS name or IP address in the "Server HostName Internally Accessible CAS" field, ensure that CAS will be able to bind to the local server address instead of the load balancer address in the back end. Continue as follows:

   Edit the following CAS configuration files in `<cs_install_dir>/bin`, using the example below as a guide:

   - In the `host.properties` file, update the following property:

     `host.name=cas."`*`host name of server where cluster member will be deployed`*`"-1`

   - In the `jbossTicketCacheReplicationConfig.xml` file, go to the `ClusterConfig` attribute and update the following parameter:

     `bind_addr="`*`host name of server where cluster member will be deployed`*`"`

   Example:

   In this example, CAS is to be deployed in a two-node cluster with a load balancer, as follows:

   - `LBCAS.fatwire.com` is the load balancer
   - `CASA.fatwire.com` runs CAS instance 1
   - `CASB.fatwire.com` runs CAS instance 2

   In the installer, you would have entered `LBCAS.fatwire.com` in the "Server HostName Internally Accessible CAS" field. The same value would then be automatically used in the CAS configuration files, in place of the variable *`host name of server where cluster member will be deployed`* (in the `host.name` and `bind_addr` properties). To edit the files, replace the value `LBCAS.fatwire.com` with `CASA.fatwire.com` for a CAS instance to deployed to instance 1, and with `CASB.fatwire.com` for a CAS instance to be deployed to instance 2.

- **b.** If you are using the WebLogic application server, manually deploy your web applications as follows:
    - **1)** Prepare to deploy the Content Server web application by ensuring that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
    - **2)** 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>
      ```

    - **3)** Deploy the Content Server web application.
    - **4)** If you are running the installer on the primary Content Server cluster member and WEM is selected to be installed, deploy and start the CAS web application on the server that you specified during the installation process.
- **c.** If you are using the WebSphere application server, manually deploy your web applications as follows:
    - **1)** Prepare to deploy the Content Server web application by ensuring that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
    - **2)** Deploy the Content Server web application.
    - **3)** If you are running the installer on the primary Content Server cluster member and WEM is selected to be installed, deploy and start the CAS web application on the server that you specified during the installation process.

7. Complete the rollup installation.

8. When the primary Content Server cluster member has been upgraded, repeat this installation procedure on all of the secondary Content Server cluster members, starting with step 1 on page 14.

9. When all Content Server cluster members have been upgraded, do the following:

- Complete the steps in Chapter 2, “Post-Installation Steps” as necessary for your configuration.

  For example, during the installation process, either you or the installer deployed the Content Server web application. If you also deployed the primary CAS cluster member and you are clustering CAS, you will manually configure and deploy the secondary CAS cluster members in the post-installation process. For instructions, see “Deploying Secondary CAS Cluster Members (CS-WEM Installations),” on page 45.
- When performing the post-installation steps, note the following:
    - Changes were made to Content Server as described in “All Installations,” on page 30.
    - If you chose to migrate to log4j, changes were made to Content Server as described in “Installations with log4j,” on page 30.

- If you chose to install WEM, changes were made to Content Server as described in "Installations with WEM Framework," on page 31.

Upgrading Silently

Note

Before starting this procedure, ensure that all pre-installation steps (page 9) 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 or `SatelliteServer` 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
`CSInstallAccountName`	Provide the current user name for the `ContentServer` user. The default value is `ContentServer`.
`CSInstallAccountPassword`	Provide the encrypted password for the `ContentServer` user.
`SSUserPassword`	Provide the encrypted password for the `SatelliteServer` 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
`ConvertToLog4J`	Set this property to `true` 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:

   - You want to install or upgrade the WEM Framework.

     If you install the WEM Framework 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, you must also install WEM on the development and delivery systems. 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 Table 4, on page 25 to the renamed `omii.ini` file. The information you provide depends on whether you are installing or upgrading the WEM Framework on a primary or secondary Content Server cluster member and whether you are clustering CAS. Sample configurations begin on page 25.

> **Note**
>
> When rolling up the primary Content Server cluster member, note the following:
>
> - If automatic deployment is in effect, the installer will deploy Content Server and CAS on the same server. Once the installation process is complete, you can manually redeploy CAS on a different server, as described in "Redeploying CAS on a New Server (CS-WEM Installations)," on page 47.
> - If manual deployment is in effect, you will deploy Content Server. You will also deploy CAS either on the same server, or on a separate server. Once the installation process is complete, and you decide to redeploy CAS on a different server, you can do so manually as described in "Redeploying CAS on a New Server (CS-WEM Installations)," on page 47.

Table 4: Properties for installing or upgrading WEM on a primary or secondary Content Server cluster member

Property	Description
`WEM`	Set this property to `true` to install or upgrade the WEM Framework.
`IsPrimaryClusterMember`	If you are upgrading or installing the WEM Framework on the primary Content Server cluster member, set this property to `true`. Otherwise, set it to `false`.
`CASHostNameLocal`	**Clustered CAS**: Host name of the server running the internally accessible CAS load balancer. **Non-clustered CAS**: Internal host name of the server where CAS will be deployed.
`CASPortNumberLocal`	**Clustered CAS**: Port number of the server running the internally accessible CAS load balancer. **Non-clustered CAS**: Internal port number of the server where CAS will be deployed.
`CASHostName`	**Clustered CAS**: Host name of the server running the CAS load balancer. **Non-clustered CAS**: Host name of the server where CAS will be deployed.
`CASPortNumber`	**Clustered CAS**: Port number of the server running the CAS load balancer. **Non-clustered CAS**: Port number of the server where CAS will be deployed.

Sample Configurations for Installing the WEM Framework

a. If you are installing the WEM Framework on the primary Content Server cluster member, use the sample configurations below as a reference. To continue the installation process, skip to step 5 on page 27.

- If CAS is clustered:

```
WEM=true
IsPrimaryClusterMember=true
CASHostName=<host name of server with load balancer>
CASPortNumber=<port number of server with load
   balancer>
CASHostNameLocal=<host name of the internally
   accessible server with load balancer>
CASPortNumberLocal=<port number of the internally
   accessible server with load balancer>
```

- If CAS is not clustered:

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

```
CASHostName=<host name of server where CAS will be
   deployed>
CASPortNumber=<port number of server where CAS will be
   deployed>
CASHostNameLocal=<internal host name of the server
   where CAS will be deployed>
CASPortNumberLocal=<internal port number of the server
   where CAS will be deployed>
```

b. If you are installing the WEM Framework on a secondary Content Server cluster member, use the sample configurations below as a reference. To continue the installation process, skip to step 5 on page 27.

- If CAS is clustered:

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<host name of server with load balancer>
CASPortNumber=<port number of server with load
   balancer
CASHostNameLocal=<host name of the internally
   accessible server with load balancer>
CASPortNumberLocal=<port number of the internally
   accessible server with load balancer>
```

- If CAS is not clustered:

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<host name of server where CAS has been
   deployed>
CASPortNumber=<port number of server where CAS has
   been deployed>
CASHostNameLocal=<internal host name of the server
   where CAS will be deployed>
CASPortNumberLocal=<internal port number of the server
   where CAs will be deployed>
```

Sample Configurations for Upgrading the WEM Framework

a. If you are upgrading the WEM Framework on the primary Content Server cluster member, use the sample configurations below as a reference. To continue the installation process, skip to step 5 on page 27.

- If CAS is clustered:

```
WEM=true
IsPrimaryClusterMember=true
CASHostName=<host name of server with load balancer>
CASPortNumber=<port number of server with load
   balancer>
CASHostNameLocal=<host name of the internally
   accessible server with load balancer>
CASPortNumberLocal=<port number of the internally
   accessible server with load balancer>
```

- If CAS is not clustered:

```
WEM=true
```

```
IsPrimaryClusterMember=true
CASHostName=<host name of server where CAS will be
   deployed>
CASPortNumber-<port number of server where CAS with be
   deployed>
CASHostNameLocal=<internal host name of the server
   where CAS will be deployed>
CASPortNumberLocal=<internal port number of the server
   where CAs will be deployed>
```

b. If you are upgrading the WEM Framework on a secondary Content Server cluster member, use the sample configurations below as a reference.

- If CAS is clustered:

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<host name of server with load balancer>
CASPortNumber=<port number of server with load
   balancer>
CASHostNameLocal=<host name of the internally
   accessible server with load balancer>
CASPortNumberLocal=<port number of the internally
   accessible server with load balancer>
```

- If CAS is not clustered:

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<host name of server where CAS has been
   deployed>
CASPortNumber=<port number of server where CAS has
   been deployed>
CASHostNameLocal=<internal host name of the server
   where CAS will be deployed>
CASPortNumberLocal=<internal port number of the server
   where CAS will be 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 Patch 2 rollup installer (`Rollup.zip`):

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

8. At the midpoint of the installation process, complete the following steps, as necessary for your installation:

   - If you are using a CAS cluster or you have used a name other than that of the current machine DNS name or IP address in the “Server HostName Internally Accessible CAS” field, ensure that CAS will be able to bind to the local server address instead of the load balancer address in the back end. Continue as follows:

     Edit the following CAS configuration files in `<cs_install_dir>/bin`, using the example below as a guide:

     - In the `host.properties` file, update the following property:

       `host.name=cas."`*`host name of server where cluster member will be deployed`*`"-1`

     - In the `jbossTicketCacheReplicationConfig.xml` file, go to the `ClusterConfig` attribute and update the following parameter:

       `bind_addr="`*`host name of server where cluster member will be deployed`*`"`

     Example:

     In this example, CAS is to be deployed in a two-node cluster with a load balancer, as follows:

     - `LBCAS.fatwire.com` is the load balancer
     - `CASA.fatwire.com` runs CAS instance 1
     - `CASB.fatwire.com` runs CAS instance 2

     In the installer, you would have entered `LBCAS.fatwire.com` in the “Server HostName Internally Accessible CAS” field. The same value would then be automatically used in the CAS configuration files, in place of the variable *`host name of server where cluster member will be deployed`* (in the `host.name` and `bind_addr` properties). To edit the files, replace the value `LBCAS.fatwire.com` with `CASA.fatwire.com` for a CAS instance to deployed to instance 1, and with `CASB.fatwire.com` for a CAS instance to be deployed to instance 2.

   - If you are using the WebLogic application server, deploy your web applications as follows:

     1) Prepare to deploy the Content Server web application by ensuring that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.

     2) 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>
```

        3) Deploy the Content Server web application.
        4) If you are running the installer on the primary Content Server cluster member and WEM is selected to be installed, deploy and start the CAS web application on the server that you specified during the installation process.

    - If you are using the WebSphere application server, deploy your web applications as follows:
        1) Prepare to deploy the Content Server web application by ensuring that `priority=1` is the first property of the `commons-logging.properties` file in the `WEB-INF/classes` directory.
        2) Deploy the Content Server web application.
        3) If you are running the installer on the primary Content Server cluster member and WEM is selected to be installed, deploy and start the CAS web application on the server that you specified during the installation process.

9. When all Content Server cluster members have been upgraded, do the following:
    - Complete the steps in Chapter 2, "Post-Installation Steps" as necessary for your configuration.

      For example, during the installation process, either you or the installer deployed the Content Server web application. If you also deployed the primary CAS cluster member and you are clustering CAS, you will manually configure and deploy the secondary CAS cluster members in the post-installation process. For instructions, see "Deploying Secondary CAS Cluster Members (CS-WEM Installations)," on page 45.

    - When performing post-installation steps, note the following:
        - Changes were made to Content Server as described in "All Installations," on page 30.
        - If you chose to migrate to log4j, changes were made to Content Server as described in "Installations with log4j," on page 30.
        - If you chose to install WEM, changes were made to Content Server as described in "Installations with WEM Framework," on page 31.

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 feature is 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 49.

- The inCache framework, on all Content Server systems. Previously, the inCache framework provided only page caching capabilities and asset caching capabilities. With Content Server 7.6 Patch 2, it now provides resultset caching, as well. All types of caching must be configured manually. For more information, see Chapter 2, "Post-Installation Steps" and the *Content Server Administrator's Guide*.
- 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*.
- Clarkii OIE, on systems running in development/content management 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.imp.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 41), 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 34. 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 42) 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 development/content management 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 44.

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 47.

CAS-Protected URLs

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

- `wem/fatwire/**`
- `/REST/**`
- `/faces/jspx/**`
- `/ContentServer?[pagename=OpenMarket/Xcelerate/UIFramework/LoginPage|OpenMarket/Xcelerate/UIFramework/ShowMainFrames,#]`
- `Satellite?[pagename=fatwire/insitetemplating/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 45.

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 `true` 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: `com.fatwire.wem.sso.cas.cs.plugin.SSOValidatorPlugin`
	`singlesignon`	This existing property determines whether single sign-on is enabled. This property is set to `true` if WEM (or LDAP) is installed. **Caution!** Do not change this value to `false` 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 32.

- 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
- Verifying Content Server Installations Without WEM Framework
- Verifying Content Server Installations Running WEM Framework
- Deploying Secondary CAS Cluster Members (CS-WEM Installations)
- Redeploying CAS on a New Server (CS-WEM Installations)
- Enabling System Tools on a Delivery System
- Setting Up inCache for Page and Asset Caching
- Enabling Resultset Caching
- Setting Up Apache log4j
- Setting Up Content Server Developer Tools
- Enabling the Clarkii Online Image Editor
- Installing the Database Performance Utility
- Installing Language Packs
- Installing Remote Satellite Server

Reapplying Customizations

During the Content Server 7.6 Patch 2 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 10) 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.

Verifying Content Server Installations Without WEM Framework

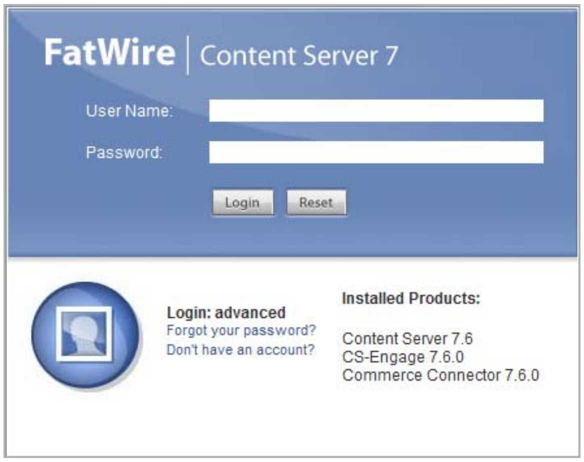
Verify the installation by logging in to Content Server as an administrator.

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:



Login: advanced

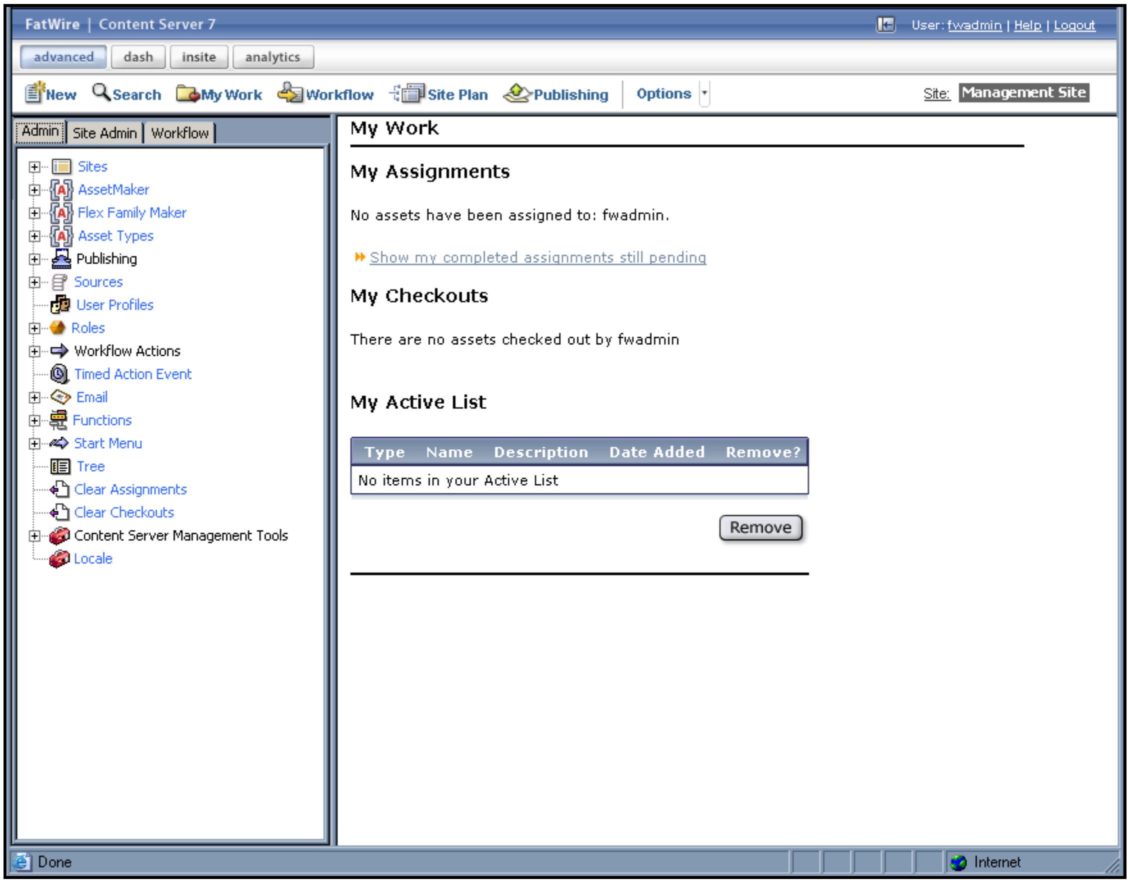
Installed Products:

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.



Site: Management Site

My Work

My Assignments

No assets have been assigned to: fwadmin.

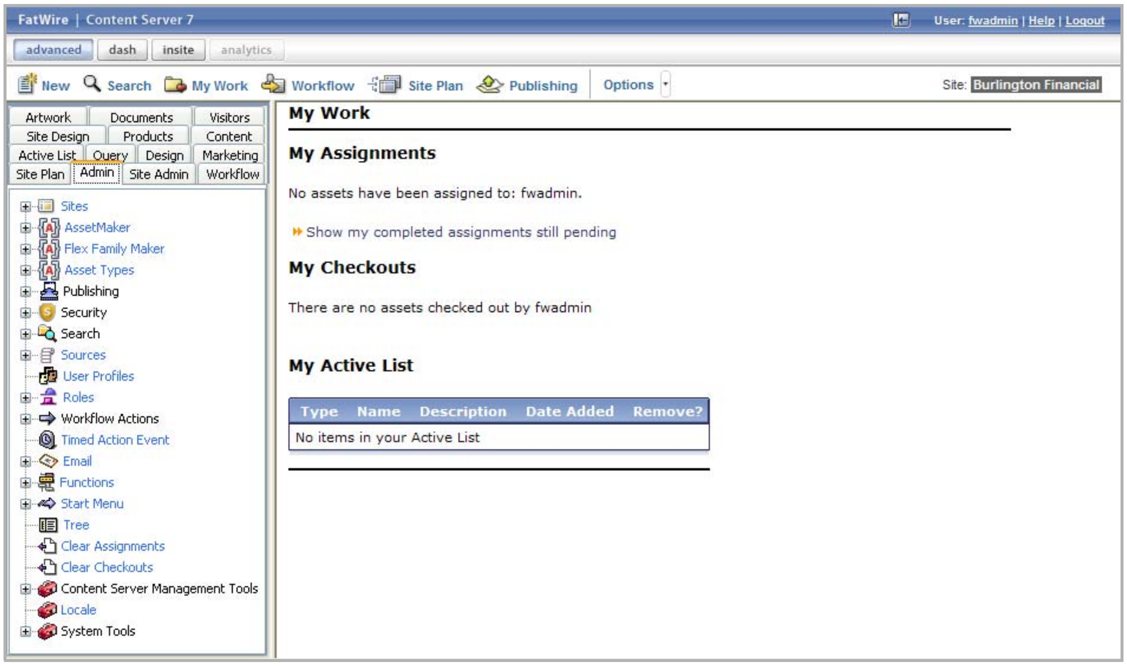
My Checkouts

There are no assets checked out by fwadmin

My Active List

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

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



My Work

My Assignments

No assets have been assigned to: fwadmin.

Show my completed assignments still pending

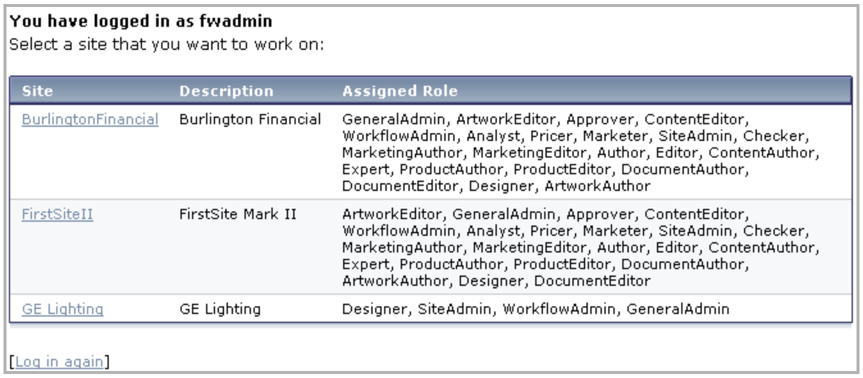
My Checkouts

There are no assets checked out by fwadmin

My Active List

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

- 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
BurlingtonFinancial	Burlington Financial	GeneralAdmin, ArtworkEditor, Approver, ContentEditor, WorkflowAdmin, Analyst, Pricer, Marketer, SiteAdmin, Checker, MarketingAuthor, MarketingEditor, Author, Editor, ContentAuthor, Expert, ProductAuthor, ProductEditor, DocumentAuthor, DocumentEditor, Designer, ArtworkAuthor
FirstSiteII	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
GE Lighting	GE Lighting	Designer, SiteAdmin, WorkflowAdmin, GeneralAdmin

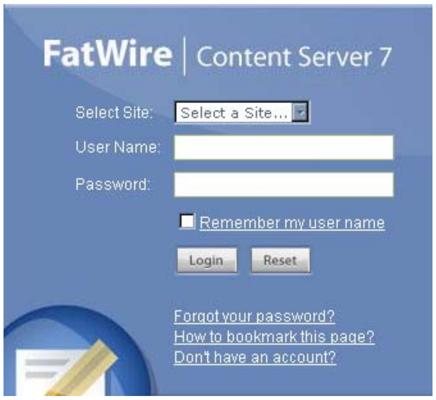
[Log in again]

Logging in to the Dash Interface

1. Point your browser to the following URL:

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

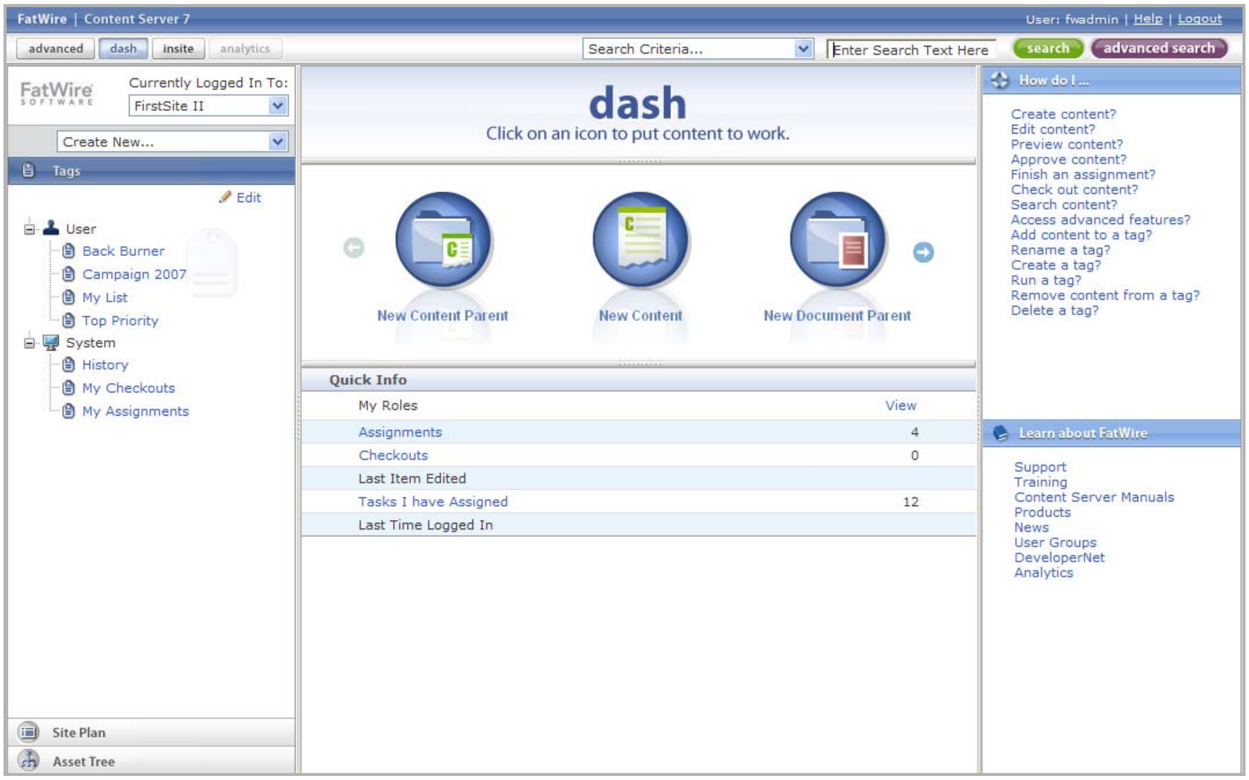
Content Server displays the Dash interface login page.



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:

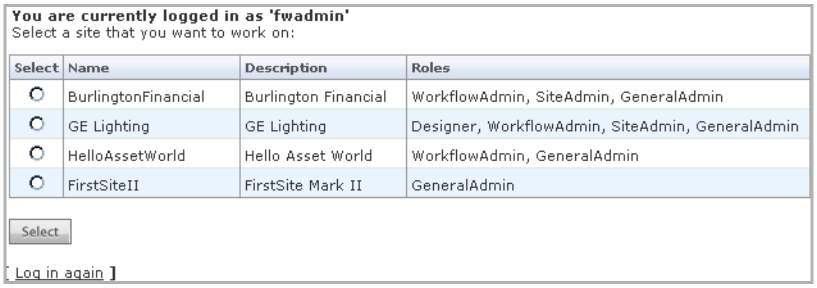
   - If no sites are configured, Content Server notifies you by displaying a message. You will not be able to log in to the Dash interface until at least one site exists on your system.
   - If only one site is configured, you are logged in to that site.



Quick Info

My Roles	View
Assignments	4
Checkouts	0
Last Item Edited	
Tasks I have Assigned	12
Last Time Logged In	

- 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:

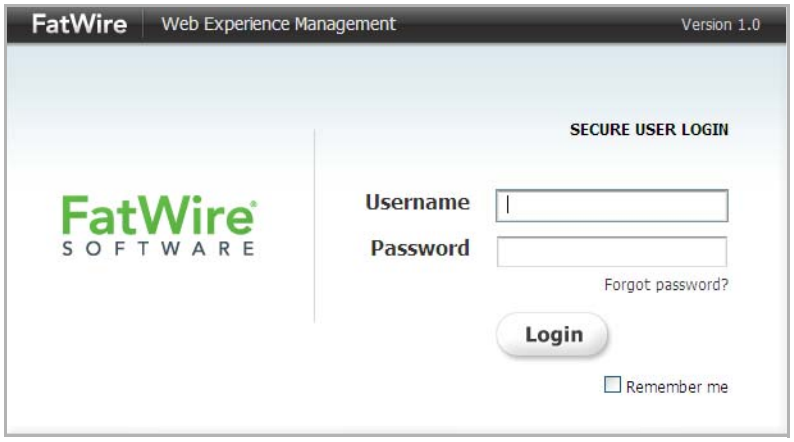
Select	Name	Description	Roles
○	BurlingtonFinancial	Burlington Financial	WorkflowAdmin, SiteAdmin, GeneralAdmin
○	GE Lighting	GE Lighting	Designer, WorkflowAdmin, SiteAdmin, GeneralAdmin
○	HelloAssetWorld	Hello Asset World	WorkflowAdmin, GeneralAdmin
○	FirstSiteII	FirstSite Mark II	GeneralAdmin

Verifying Content Server Installations Running WEM Framework

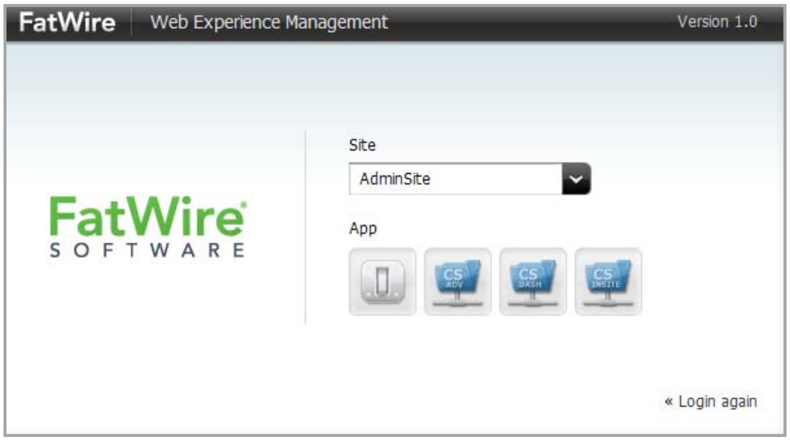
1. Point your browser to the following URL:

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

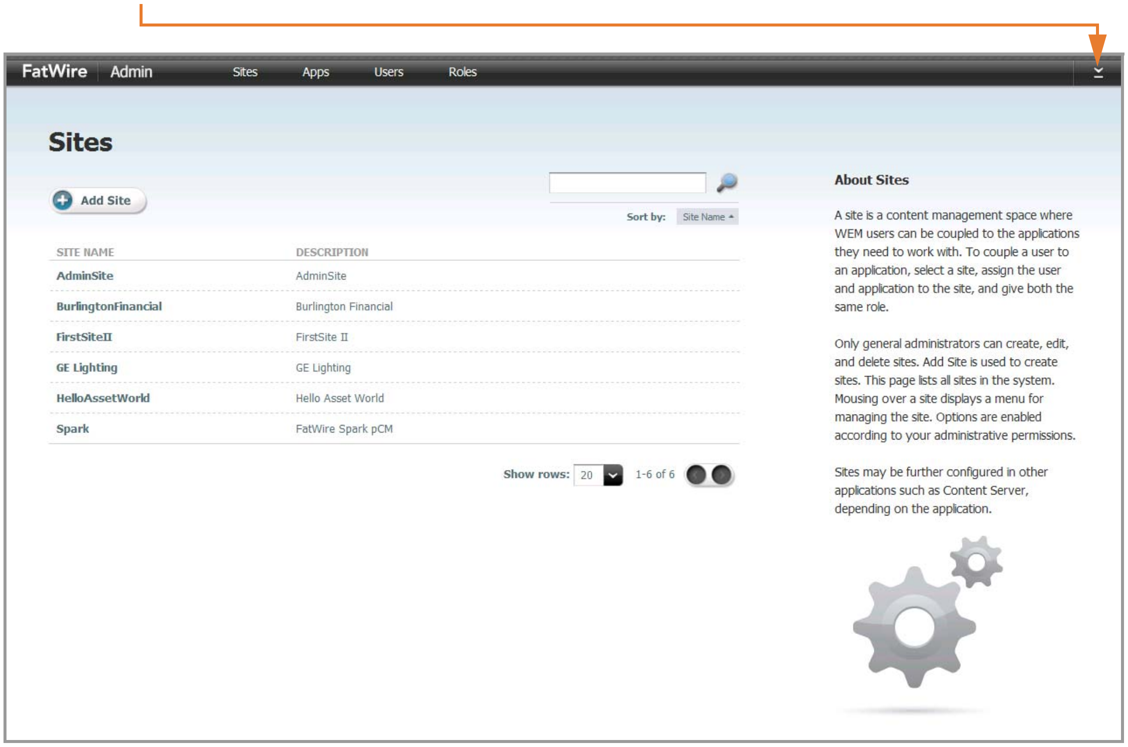
2. Log in with the credentials of the `fwadmin` general administrator.



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



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



Sites

SITE NAME	DESCRIPTION
AdminSite	AdminSite
BurlingtonFinancial	Burlington Financial
FirstSiteII	FirstSite II
GE Lighting	GE Lighting
HelloAssetWorld	Hello Asset World
Spark	FatWire Spark pCM

About Sites

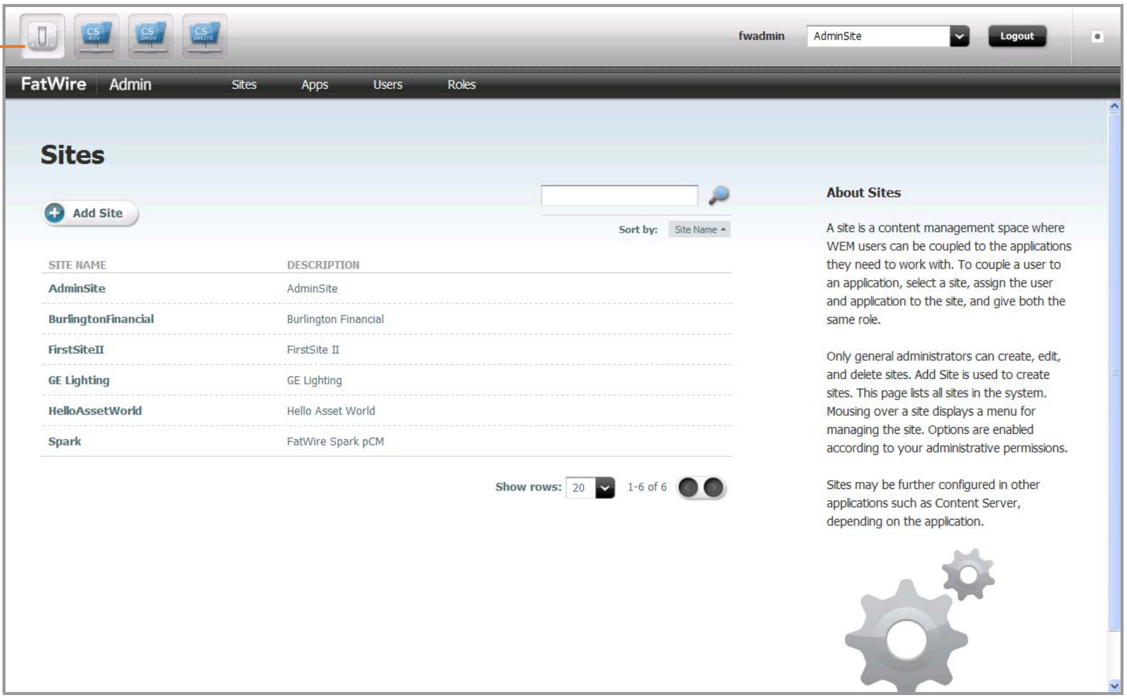
A site is a content management space where WEM users can be coupled to the applications they need to work with. To couple a user to an application, select a site, assign the user and application to the site, and give both the same role.

Only general administrators can create, edit, and delete sites. Add Site is used to create sites. This page lists all sites in the system. Mousing over a site displays a menu for managing the site. Options are enabled according to your administrative permissions.

Sites may be further configured in other applications such as Content Server, depending on the application.

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



Sites

SITE NAME	DESCRIPTION
AdminSite	AdminSite
BurlingtonFinancial	Burlington Financial
FirstSiteII	FirstSite II
GE Lighting	GE Lighting
HelloAssetWorld	Hello Asset World
Spark	FatWire Spark pCM

About Sites

A site is a content management space where WEM users can be coupled to the applications they need to work with. To couple a user to an application, select a site, assign the user and application to the site, and give both the same role.

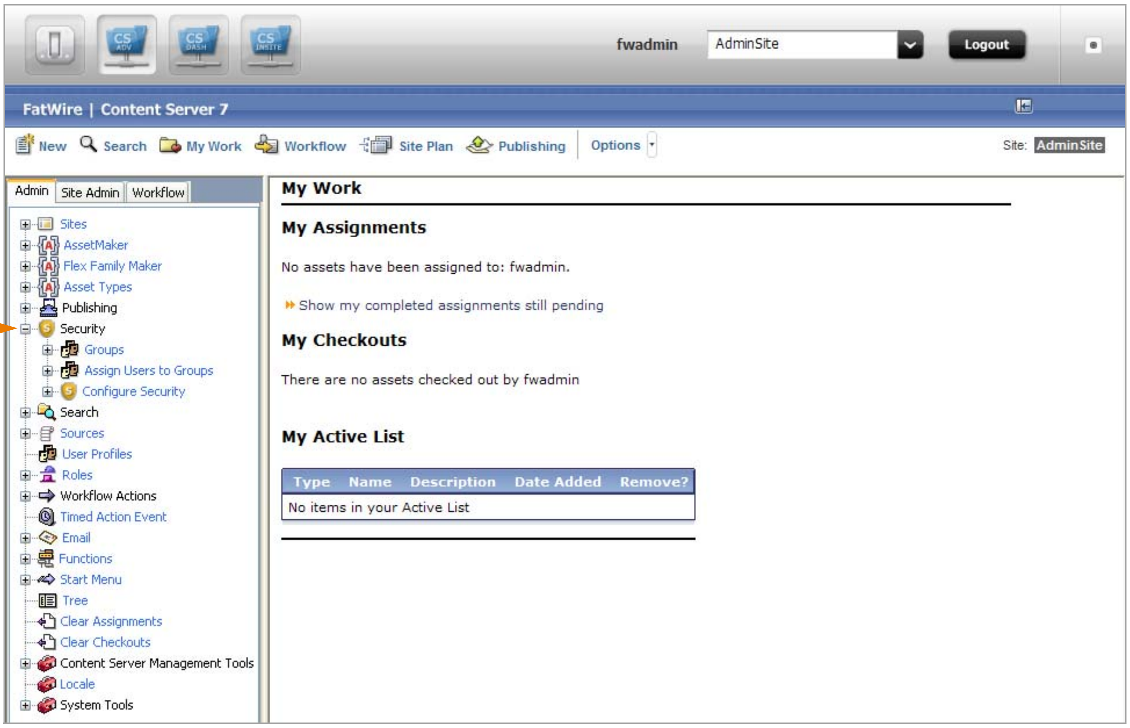
Only general administrators can create, edit, and delete sites. Add Site is used to create sites. This page lists all sites in the system. Mousing over a site displays a menu for managing the site. Options are enabled according to your administrative permissions.

Sites may be further configured in other applications such as Content Server, depending on the application.

6. Verify that the Content Server Advanced and Dash interfaces are displayed as shown on pages 37–39.

> **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)



My Work

My Assignments

No assets have been assigned to: fwadmin.

Show my completed assignments still pending

My Checkouts

There are no assets checked out by fwadmin

My Active List

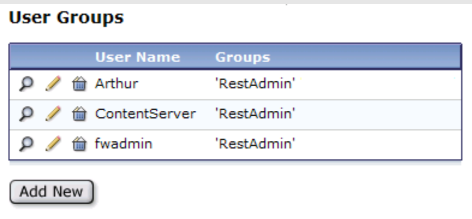
Type	Name	Description	Date Added	Remove?
No items in your Active List				

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**, **xceleditor, 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 Groups

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

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.

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.
7. Allow synchronization of CAS tickets between Content Server members. For each cluster member, edit the file WEB-INF/classes/cas-cache.xml as follows:
   a. Locate the line multicastGroupPort=4666, timeToLive=0
      - Ensure the port is unique for each Content Server cluster (all members must use the same port).
      - Change timeToLive to 1 if the cluster members reside on different physical servers.

b. Save the updated file.

8. To properly distribute CAS tickets among Content Server cluster members, a new cache based on inCache was introduced in version 7.6 patch 2. This cache is configured in the same way as cs-cache. However, it is located on a different port (the default is 4666).

   For CAS authorization to properly function in a cluster, locate the file `cas-cache.xml` in `WEB-INF/classes` and modify the following line:

   ```
   multicastGroupPort=4666, timeToLive=0
   ```

   as you would for cs-cache in a cluster. That is, adjust the `timeToLive`, and ensure that the same unique port is used by all cluster members to communicate.

   You can verify that all cluster members are sharing data by using System Tools, a node on the **Admin** tab of the Advanced interface. A separate instance of `cas-cache.xml` is used on Remote Satellite Server (default port 4667). Located in `WEB-INF/classes`, `cas-cache.xml` should be modified such that each Satellite Server uses a unique port, as no data is shared among Remote Satellite Servers.

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

Note

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

During the installation process, the installer entered your CAS deployment information into the following files, enabling Content Server to connect to CAS:

- `SSOConfig.xml` in `WEB-INF/classes`
- Files in `<cs_install_dir>/bin`:
  - `cas.properties`
  - `host.properties`
  - `jbossTicketCacheReplicationConfig.xml`

When the installation process is complete and you need to redeploy CAS on a new server, you must manually reconfigure the above files and CAS, as follows:

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 45.
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.

Enabling System Tools on a Delivery System

On a delivery system, to gain access to the **System Tools** node on the **Admin** tab of the Content Server Advanced interface, 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*.

Setting Up inCache for Page and Asset Caching

If you rolled up from Content Server 7.5.*x* and did not enable the inCache framework, its page caching capabilities are not automatically enabled in version 7.6.*x* (the traditional page caching method runs by default). If you rolled up from version 7.6.*x* and did not enable the inCache framework, its asset caching capabilities are not automatically enabled in version 7.6.*x*. 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).

For information about enabling page and/or asset caching for the inCache framework, see the *Content Server Administrator's Guide*.

Note

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.*

Enabling Resultset Caching

As of version 7.6 Patch 2, Content Server supports the alternative to store resultsets within the inCache framework instead of hash tables in Java memory. Enabling resultset caching over inCache amounts to setting the `rsCacheOverinCache` property (in `futuretense.ini`) to `true`. The **System Tools** node (on the **Admin** tab of the Advanced interface) then displays the resultset over inCache tool, which provides statistical information about the caches and their contents.

Enabling resultset caching over inCache does not require enabling either page or asset caching over inCache. Information about the inCache framework, its caching models, system tools, and the process of enabling them is available in 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*.

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*.

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 are displayed in the English language. If you want your Content Server interfaces to be displayed 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 *Installing Satellite Server.*

Note

- To upgrade Remote Satellite Server, run the Satellite Server 7.6 Patch 2 installer, available from FatWire Technical Support at `http://support.fatwire.com`.
- 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.*

Next Steps

FatWire Content Server can now be used for its business purpose. If you created a new installation, refer to the Content Server developer, administrator, and user guides for information about developing content management sites and web sites.