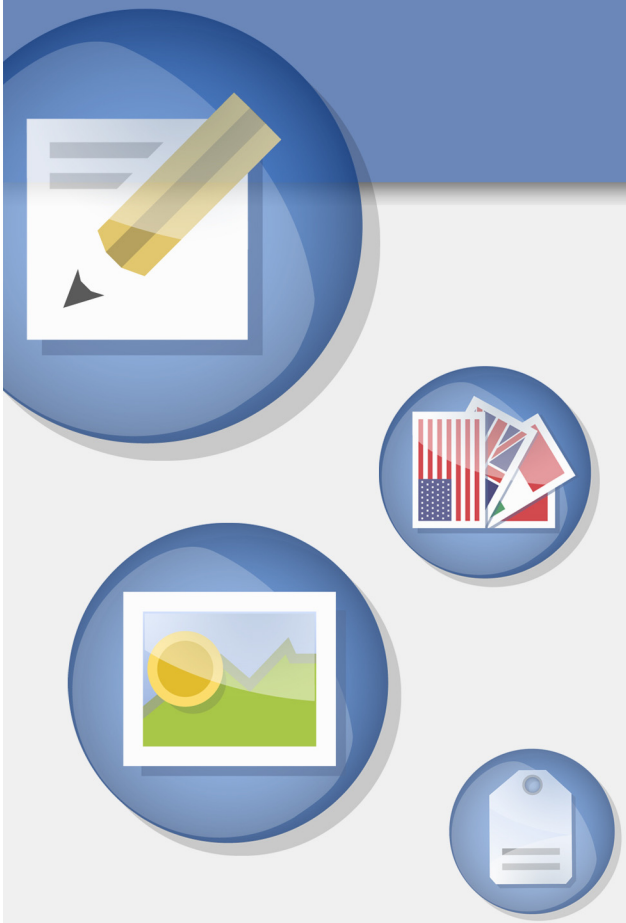
FatWire | Content Server 7

Version 7.5 Patch 5



Rollup Installation Guide

Document Revision Date: Sep. 14, 2010

FatWire® SOFTWARE

FatWire Content Server Rollup Installation Guide
Document Revision Date: Sep. 14, 2010
Product Version: 7.5 Patch 5

FatWire Technical Support
www.fatwire.com/Support

FatWire Headquarters
FatWire Corporation
330 Old Country Road
Suite 303
Mineola, NY 11501
www.fatwire.com

Table of

Contents

Chapter 1

Installing FatWire Content Server 7.5 Patch 5

This chapter provides instructions for installing FatWire Content Server 7.5 Patch 5.

This chapter contains the following sections:

Overview

FatWire Content Server Patch 3 and subsequent patches provide the following options: FatWire Web Experience Management (WEM) Framework, the inCache page caching framework, and the database performance enhancement utility. The Clarkii Online Image Editor (OIE) is introduced in Patch 5.

If the following options were enabled in patch 3 or 4, they remain enabled in patch 5:

- The WEM Framework option 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.

  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.
- inCache is our implementation of Terracotta's Ehcache open source product available under the Apache license. The inCache framework provides significant performance improvements over our standard page cache method. If you have not enabled this option in previous patches, the traditional page caching method will run by default when patch 5 is installed.
- The database performance enhancement utility can be used on systems running in delivery or content management mode to create additional indexes for database tables. If you wish to use this utility in patch 5, you must install it manually.

Clarkii OIE, from InDis Baltic, can be enabled in Content Server's Dash, Advanced, and InSite interfaces in place of your current Online Image Editor.

Pre-Installation Steps

This guide is written for experienced Content Server installation engineers. Before upgrading to Patch 5, 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.

- 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 (development, staging, testing, and delivery).
- If the default user name and/or password were changed for the `ContentServer` user or general admin (`fwadmin`) after CS 7.5 was installed, update the `omii.ini` file. During the patch installation, the installer authenticates by referring to `omii.ini` for user names and passwords. If they are outdated, the installer will fail.

  Update the `omii.ini` file, as indicated below, on every cluster member regardless of its installation mode (delivery or content management). The `omii.ini` file is located in the following directory: `<cs_install_dir>/ominstallinfo/`

  - If the default user names were changed, update the following properties:
    - `CSInstallAccountName=<current_userName>`
      (the default value is `ContentServer`)
    - `CSInstallAppName=<current_userName>`
      (the default value is `fwadmin`, the general admin)
  - If the above users' default passwords were changed, update the following properties:
    - `CSInstallAccountPassword=<encrypted password for the CSInstallAccountName user>`
    - `CSInstallAppPassword=<encrypted password for the CSInstallAppName user>`

    Use Content Server's Property Editor to get encrypted passwords:

    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. The system is ready to be upgraded to a new patch.
- Set the `max PermGen` parameter on all application servers in the range of 128MB–196MB.
- Before performing a portal server installation, back up the `portlet.xml`, `web.xml` and any other server-specific configuration files. After the installation midpoint, you will merge these configuration files manually and package them back into Content Server's `.ear` and `.war` files. You will do this whether or not you are installing WEM.

- For JDK 1.6, copy `jaxb-impl-2.1.12.jar` file (located in `Rollup/wem/lib`) 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).

- Read the rest of this chapter to determine your preferred installation method: Silent or GUI-based. The rollup installer, in either mode, detects and uses the deployment method that was used to install Content Server 7.5. For example, if Content Server 7.5 was installed in delivery mode, the rollup installer detects the delivery mode and continues to treat the system as a delivery system. **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 you wish to install the WEM framework, consider the changes that will be made by the installer. See "WEM Framework Installations," on page 15. See also the *WEM Framework Administrator's Guide* and the *WEM Framework Developer's Guide.*

  WEM requires Central Authentication Services (CAS). The installer will either deploy CAS automatically or prompt you to deploy CAS. The following deployment options are supported: CAS on a primary Content Server cluster member, an application server cluster member marked as primary, or a separate application server.

  Caution!

  When WEM is installed on Content Server, the general administrator (`fwadmin`) 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 general administrator (`fwadmin`), which was used during the installation process.** Doing so disables **all** access to Content Server when WEM is installed. Instead, change the user name and/or password.

- The inCache framework will be installed by default, but disabled. For more information about inCache and its configuration, see the *Content Server Developer's Guide*.
- For information about Clarkii OIE, see the *Content Server Developer's Guide,* as well as the Dash and Advanced user guides.

Post-Installation Summary

Once Content Server 7.5 Patch 5 is installed, you will follow up by verifying the installation and completing configuration steps that depend on whether you chose to install WEM, or wish to enable inCache, or both. Installing Remote Satellite Server is covered in the Satellite Server installation guide.

Rollup Installation Procedures

Complete one of the following procedures to install Patch 5 on your Content Server 7.5 system:

- Upgrading Silently
- Running the GUI Installer

Upgrading Silently

Note

Before starting this procedure, ensure that pre-installation steps (page 6) 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.

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.

   Note

   It is assumed that your `omii.ini` file correctly specifies the credentials listed on page 7 of the "Pre-Installation Steps." The silent installer will add the specified general administrator to the RestAdmin group and enable the administrator on the AdminSite.

2. If you are not installing WEM, skip to step 4.
3. If you are installing WEM, add the following properties to the renamed file.

Property	Description
`WEM`	Set this property to `true` to install WEM.
`IsPrimaryClusterMember`	Set this property to `true` if the silent installer is used to apply the patch on a primary Content Server cluster.
`CASHostName`	Point to the host name of the server where CAS will be deployed.
`CASPortNumber`	Point to the port number of the server where CAS will be deployed.

Sample Configurations:

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

```
WEM=true
IsPrimaryClusterMember=true
CASHostName=<PRIMARY_CS_HOST_NAME>
CASPortNumber=<PRIMARY_CS_PORT_NUMBER>
```

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

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<PRIMARY_CS_HOST_NAME>
CASPortNumber=<PRIMARY_CS_PORT_NUMBER>
```

- If you are manually deploying CAS on a server other than the primary Content Server cluster member:

```
WEM=true
IsPrimaryClusterMember=false
CASHostName=<SERVER_HOST_NAME>
CASPortNumber=<SERVER_PORT_NUMBER>
```

4. Decompress the `Rollup.zip` file.
5. Edit the `install.ini` file (located in the root of the extracted `Rollup` folder):
   a. Set `nodisplay=true`
   b. Uncomment the `loadfile` property and set it as follows:
   `loadfile=<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:

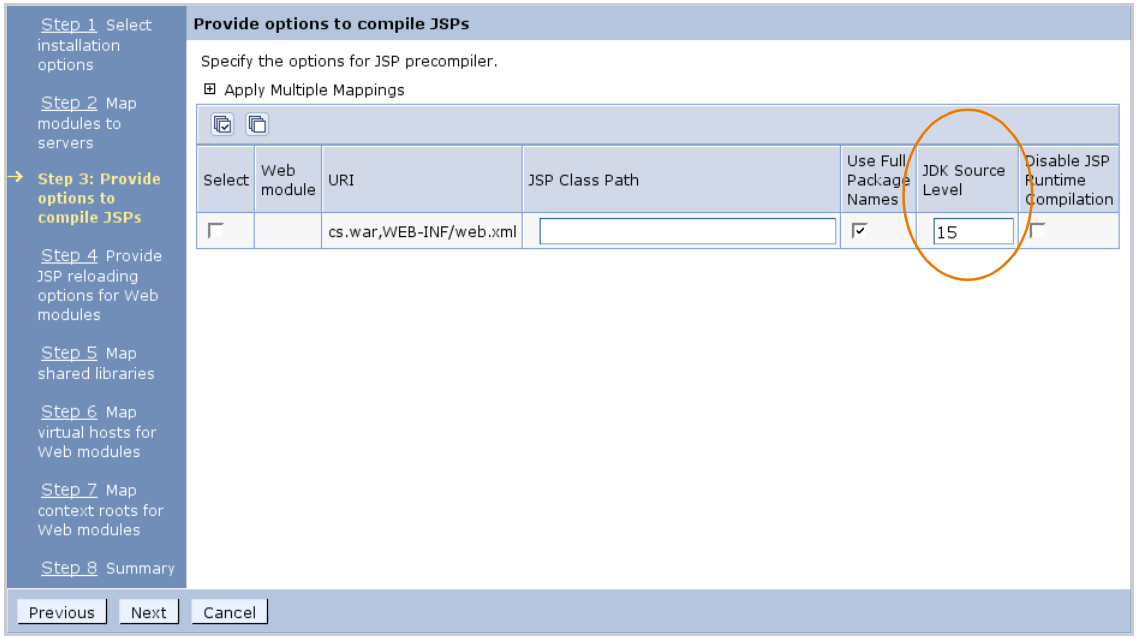
```
CSInstallDirectory=C\:/csinstall
```

- or -

```
c\:\\install
```

6. Run `csrollupinstall.bat` or `csrollupinstall.sh -silent`.

7. At the installation midpoint, if manual deployment is enabled, you must deploy the Content Server web application (*and* the CAS web application if WEM is selected to be installed). For Content Server (*and* the CAS web application if WEM is selected), change the value of the "JDK Source Level" field to `15` in the "Provide options to compile JSPs" screen:



8. When the primary cluster member has been upgraded, repeat this procedure on all of the secondary Content Server cluster members, starting with step 1.
9. When all 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 15.
   - If you chose to install WEM, then changes were made to Content Server as described in "WEM Framework Installations," on page 15.

Running the GUI Installer

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

Note

Before starting this procedure, ensure that pre-installation steps (page 6) have been completed.

To run the installer

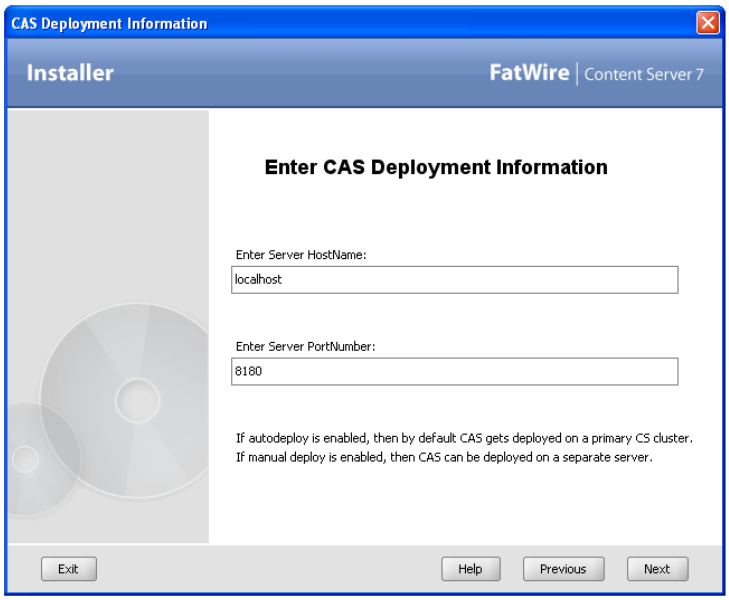
1. If you are installing WEM, do one of the following:

   Verify that the credentials of Content Server's current general administrator (`fwadmin` by default) are correctly specified in the `/ominstallinfo/omii.ini` file. The properties are `CSInstallAppName` and `CSInstallAppPassword`. The GUI installer will add this general administrator to the RestAdmin group and enable the administrator on the AdminSite.
2. Run the Content Server 7.5 Patch 5 installer by executing `csrollupinstall.bat` or `csrollupinstall.sh` from the directory into which you extracted the patch.
3. In this step you have the option to install WEM.

Note

Before selecting the WEM option, read the note on the installer screen and refer to the documentation listed on page 8 if you need further information about WEM. If you select the WEM option, you will also have to specify CAS deployment information.

4. If you selected **WEM**, specify CAS deployment information: The host name and port number of the server on which CAS will be or has been deployed, depending on whether you are running the installer on a primary or secondary cluster member. For more information about CAS deployment, refer to the installer's online help.

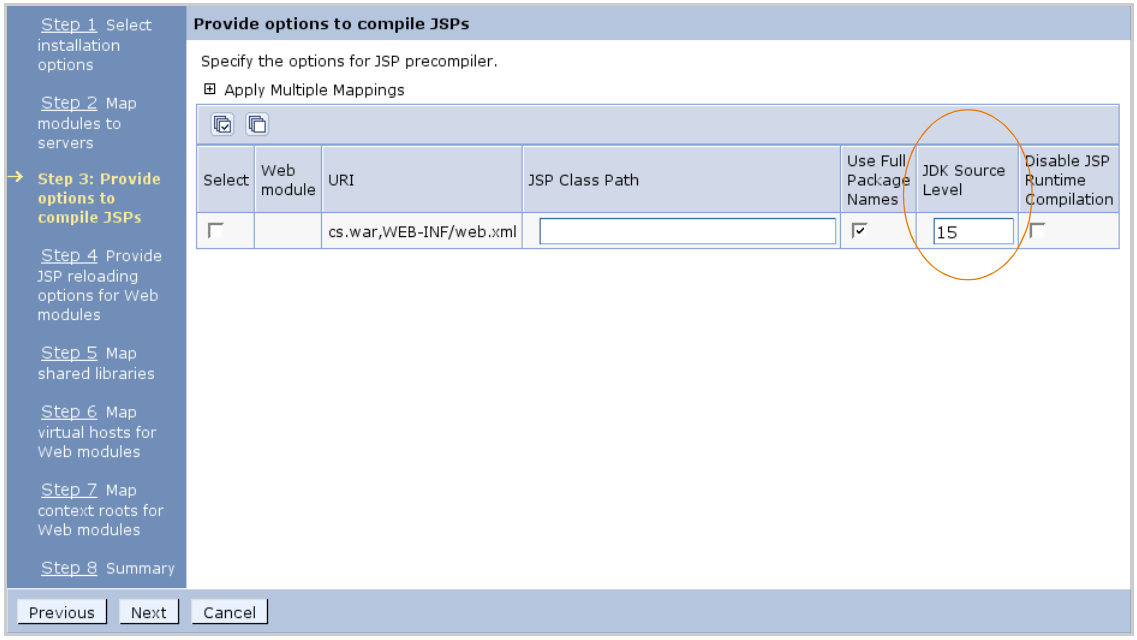


Note

For all deployment types, the installer will enter the server's information into the `SSOConfig.xml` file (in Content Server's `WEB-INF/classes` folder), enabling Content Server to connect to CAS.

If you redeploy CAS after the installation process is complete, you must also reconfigure CAS and the `SSOConfig.xml` file.

5. At the installation midpoint, if manual deployment is enabled, you must deploy the Content Server web application (*and* the CAS web application if WEM is selected to be installed). For the Content Server web application (*and* CAS web application if WEM is selected), if you are using WebSphere Application Server, change the value of the "JDK Source Level" field to `15` in the "Provide options to compile JSPs" screen:



6. Complete the patch installation.
7. When the primary cluster member has been upgraded, repeat this procedure on all of the secondary Content Server cluster members, starting with step 1.
8. When all 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 15.
   - If you chose to install WEM, then changes were made to Content Server as described in "WEM Framework Installations," on page 15.

Changes to Content Server

All Installations

The installation process installs the following components:

- inCache page caching framework, on all Content Server systems; inCache is disabled by default.
- Clarkii OIE, on systems running in 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/
```

WEM Framework Installations

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

New Login Page

Installing WEM replaces the Content Server login page with the WEM login page (see page 27), which affects the way Content Server interfaces are accessed (URL is unaffected).

New Site: AdminSite

Installing WEM creates a new site called "AdminSite" in Content Server's 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 17. For more information 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 28) 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 mode**).

New Security Model

Installing WEM creates a new node on the **Admin** tab in Content Server's 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

The general administrator that was used during the installation process (`fwadmin`) was added by the installation process to the RestAdmin group. The general administrator was also enabled on the AdminSite, which provides access to the WEM Admin interface. Instructions for creating additional general administrators are available on page 30.

Reminder

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

New Web Application: CAS

If CAS was autodeployed during the Content Server installation process, then it was deployed by default on a primary Content Server cluster member and configured to authenticate against the Content Server database. If you need to redeploy CAS, you must do so manually. For instructions, see "Redeploying CAS (CS-WEM Installations)," on page 31.

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,#]`

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 15.

- 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:

- Verifying Content Server Installations Without WEM Framework
- Verifying Content Server Installations Running WEM Framework
- Redeploying CAS (CS-WEM Installations)
- Enabling the Clarkii Online Image Editor
- Enabling inCache
- Installing the Database Performance Utility
- Installing Remote Satellite Server

Verifying Content Server Installations Without WEM Framework

Verify the installation by logging in to Content Server as an administrator. This section covers the following types of installations:

- Web Installations
- Portal Installations

Web Installations

Logging in to the Advanced Interface

1. Point your browser to the following URL:

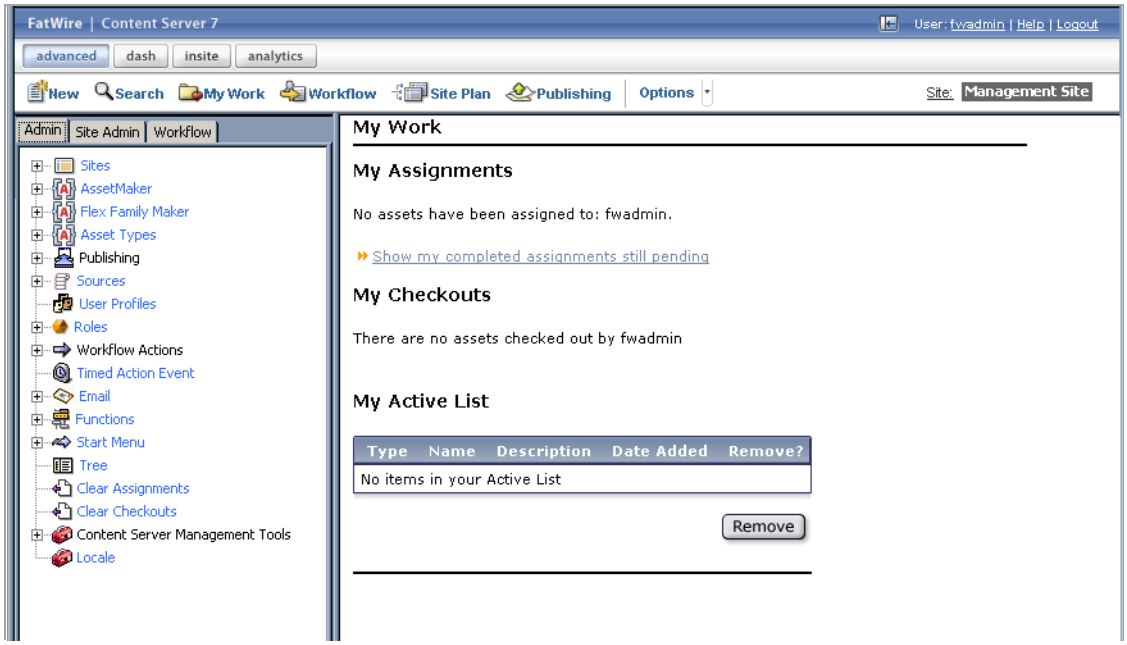
   `http://<hostname>:<port>/<context>/Xcelerate/LoginPage.html`

   Content Server displays the Advanced interface login form:

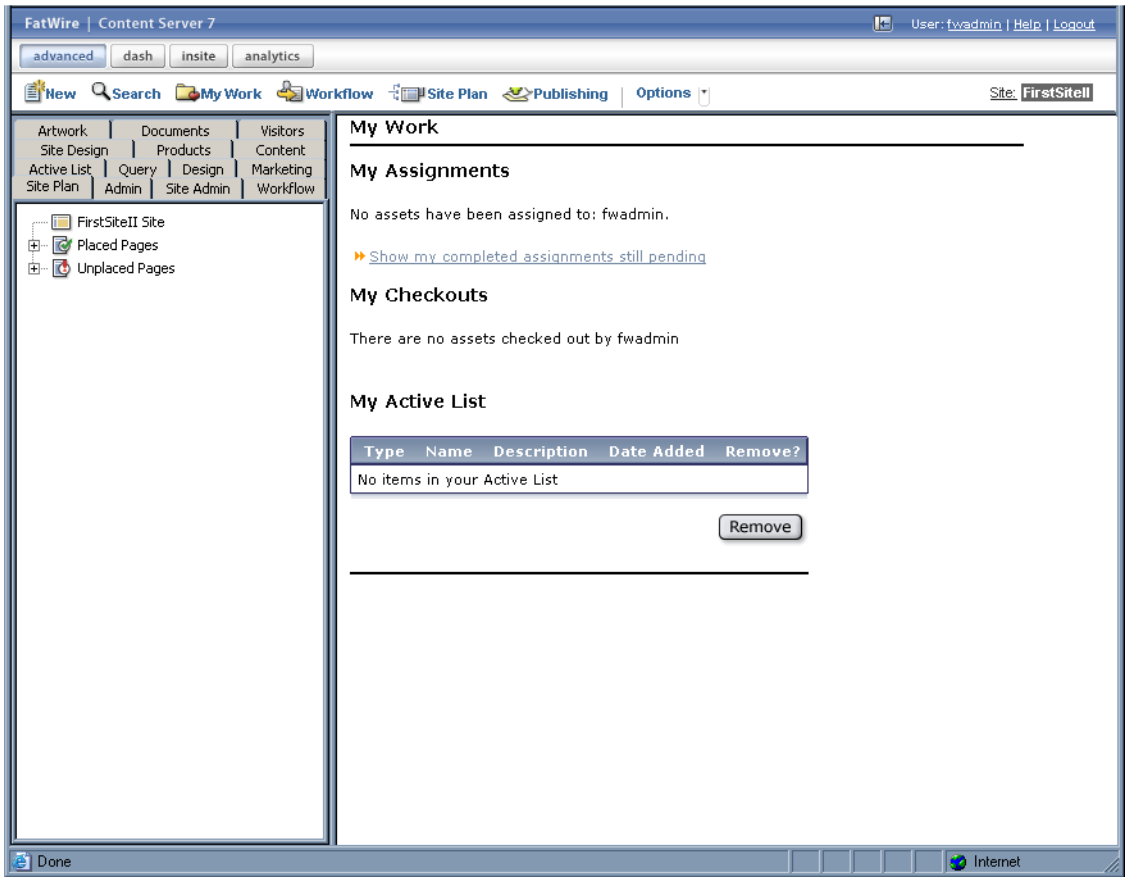
2. Log in with the credentials of the general administrator that was used during the installation process (the default credentials are `fwadmin`/`xceladmin`).
3. Click **Login**.

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

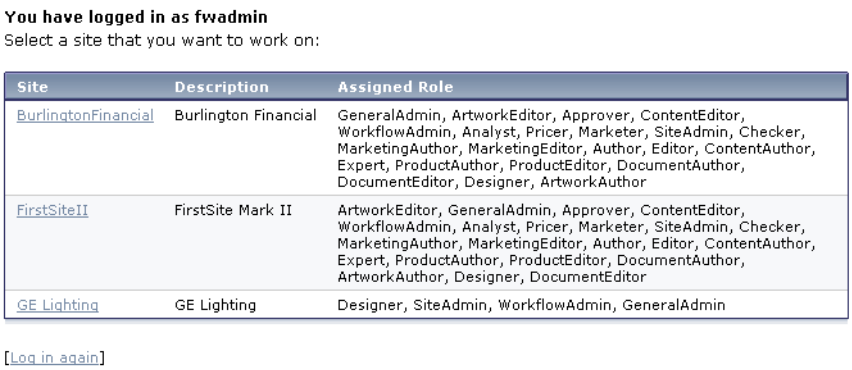
- If no sites are configured, you are logged in to the built-in Content Server management site. Only system administration functionality is available.



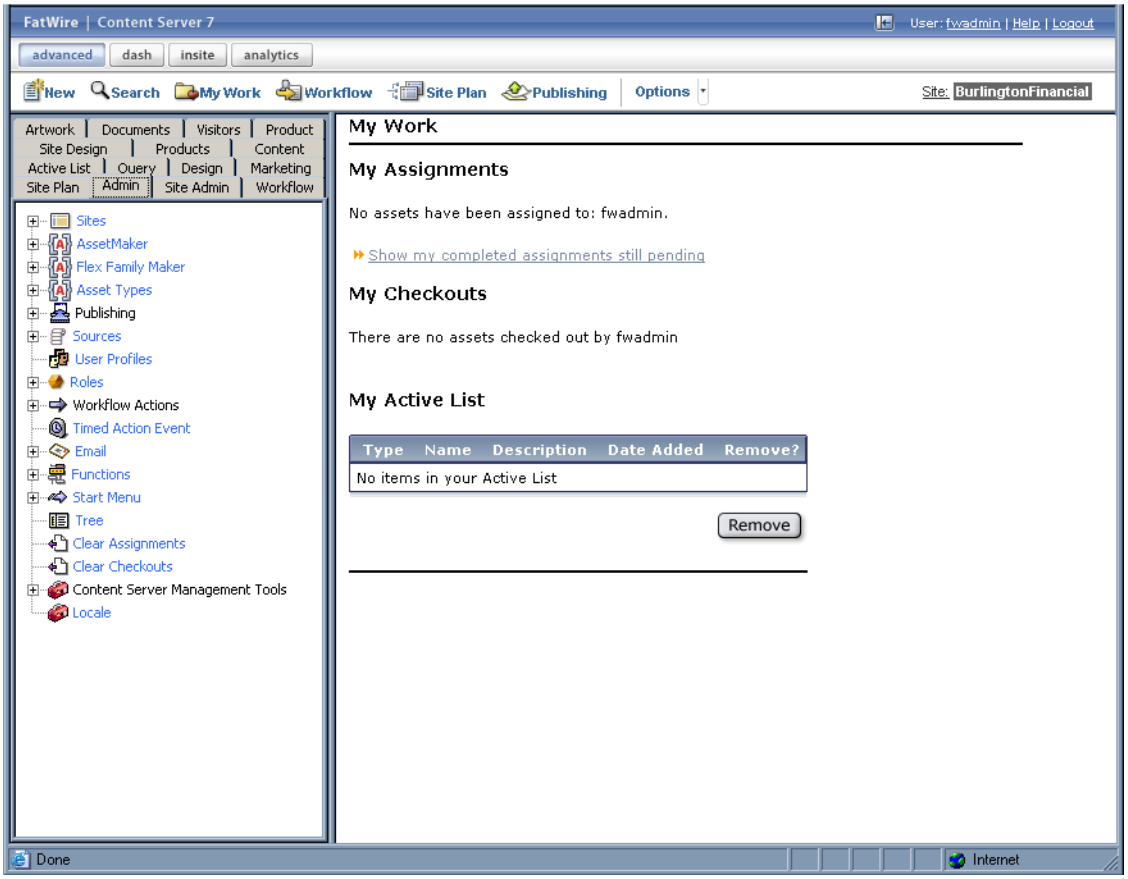
- If one site is configured, you are logged in to that site.



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



When you select a site, you are logged in to that site.



Logging in to the Dash Interface

1. Point your browser to the following URL:

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

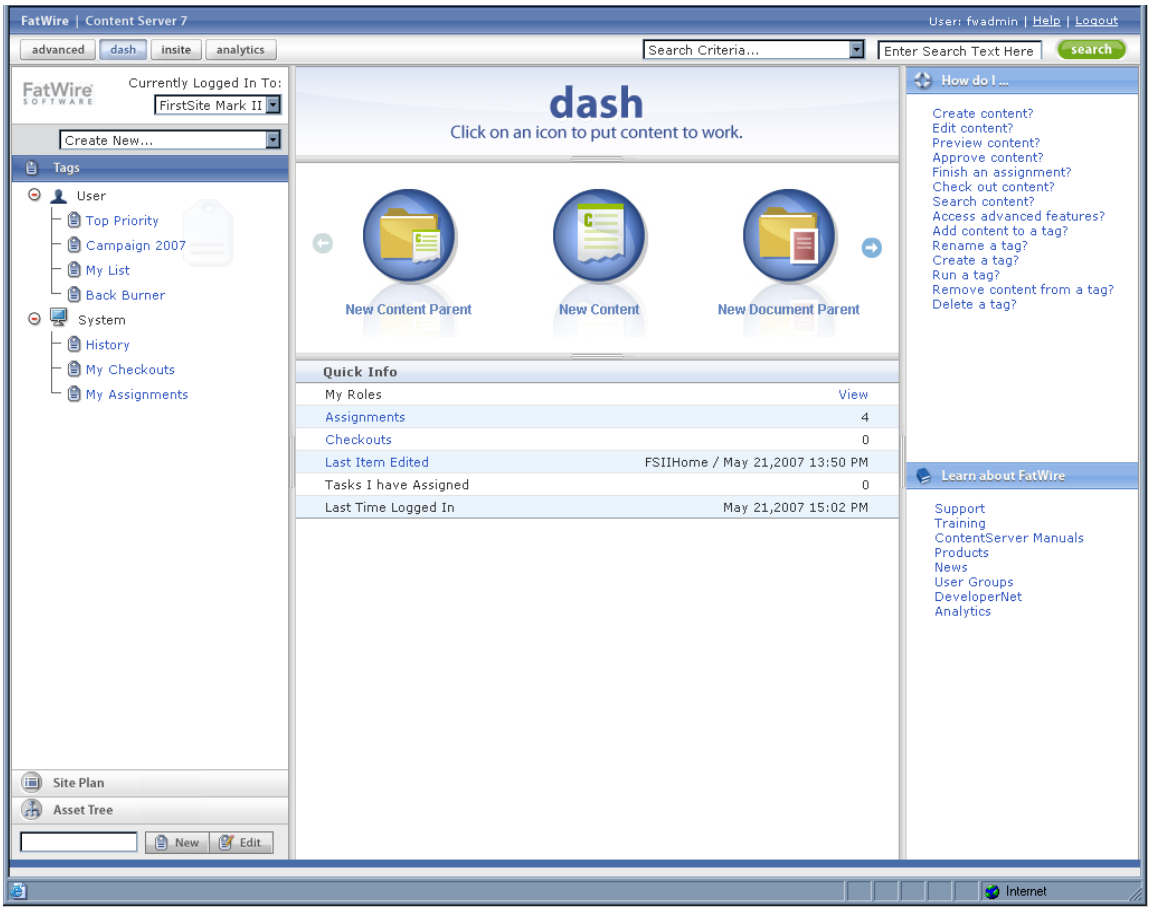
   Content Server displays the Dash interface login page.

2. Log in with the credentials of the general administrator that was used during the installation process (the default credentials are `fwadmin`/`xceladmin`).
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 displays a message notifying you of that fact. You will not be able to log in to the Dash interface until at least one site exists on your system.

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



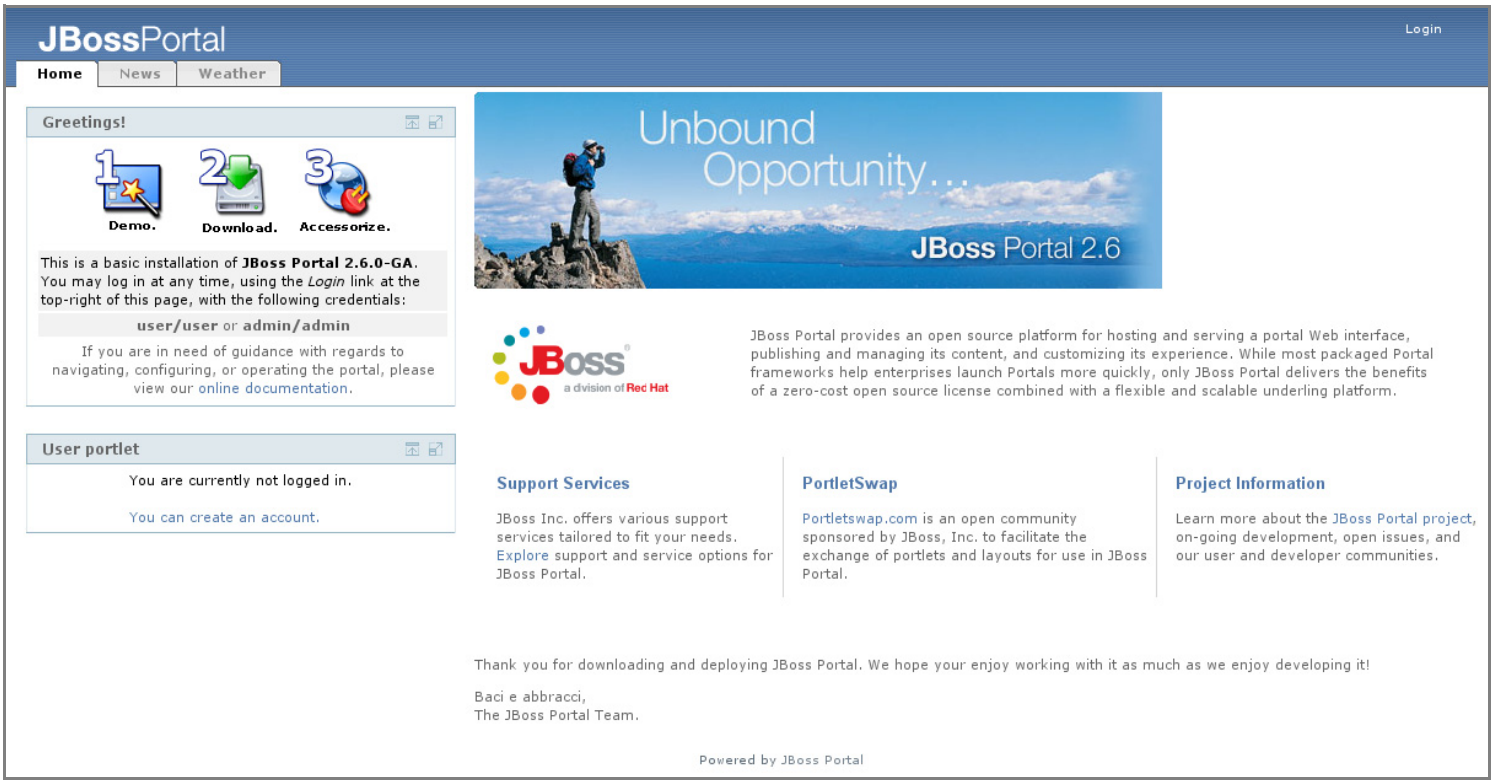
- If more than one site is configured, Content Server displays the “Select Site” screen. Select the site you wish to log in to.

When you select a site, you are logged in to that site.

Portal Installations

Verify the installation by accessing the portal interface in a browser:

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



Content Server is now ready for configuration. Follow the steps in the rest of this chapter.

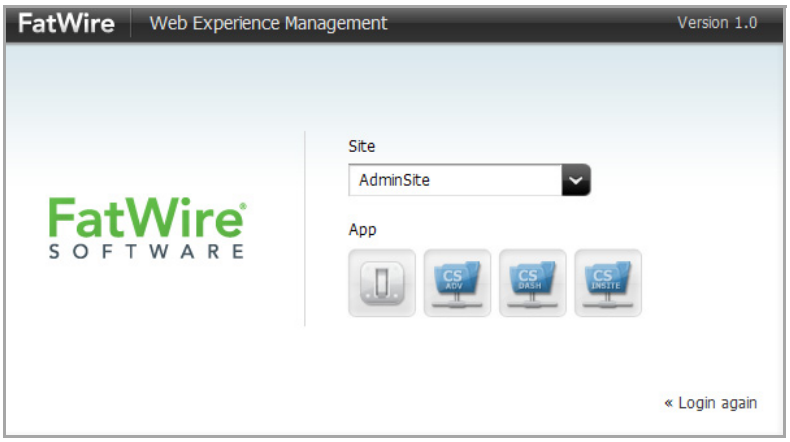
Verifying Content Server Installations Running WEM Framework

1. Point your browser to the following URL:

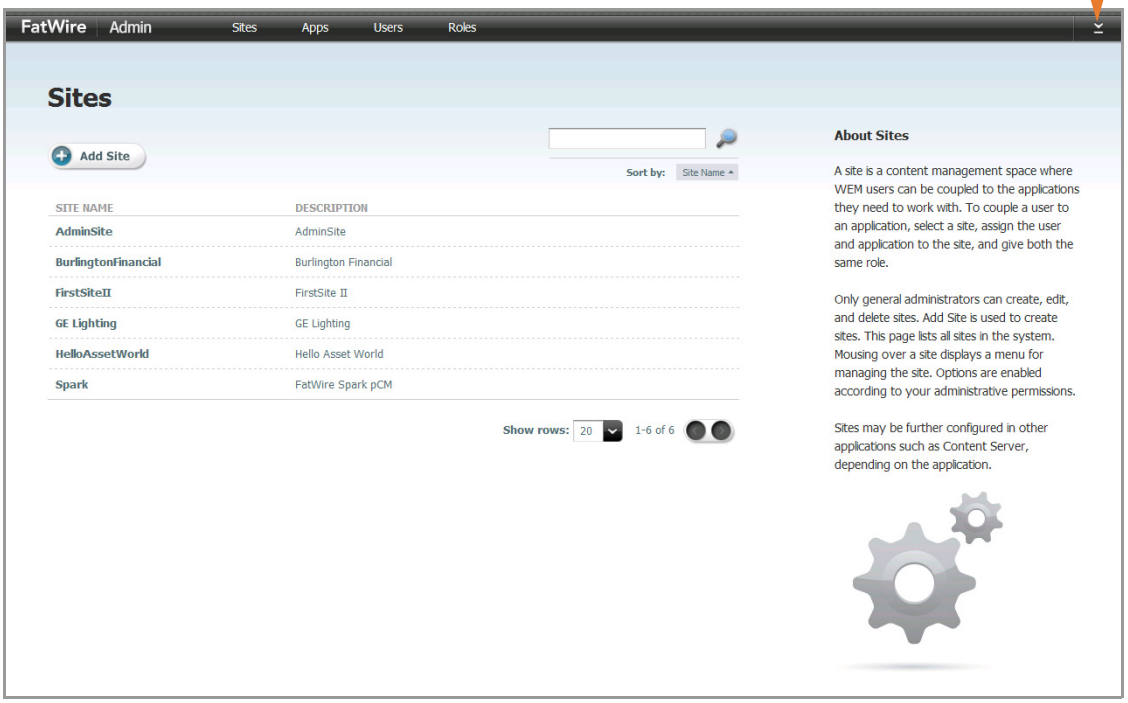
   `http://<hostname>:<port>/<context>/login`

2. Log in with the credentials of the general administrator that was used during the installation process (the default credentials are `fwadmin`/`xceladmin`).

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

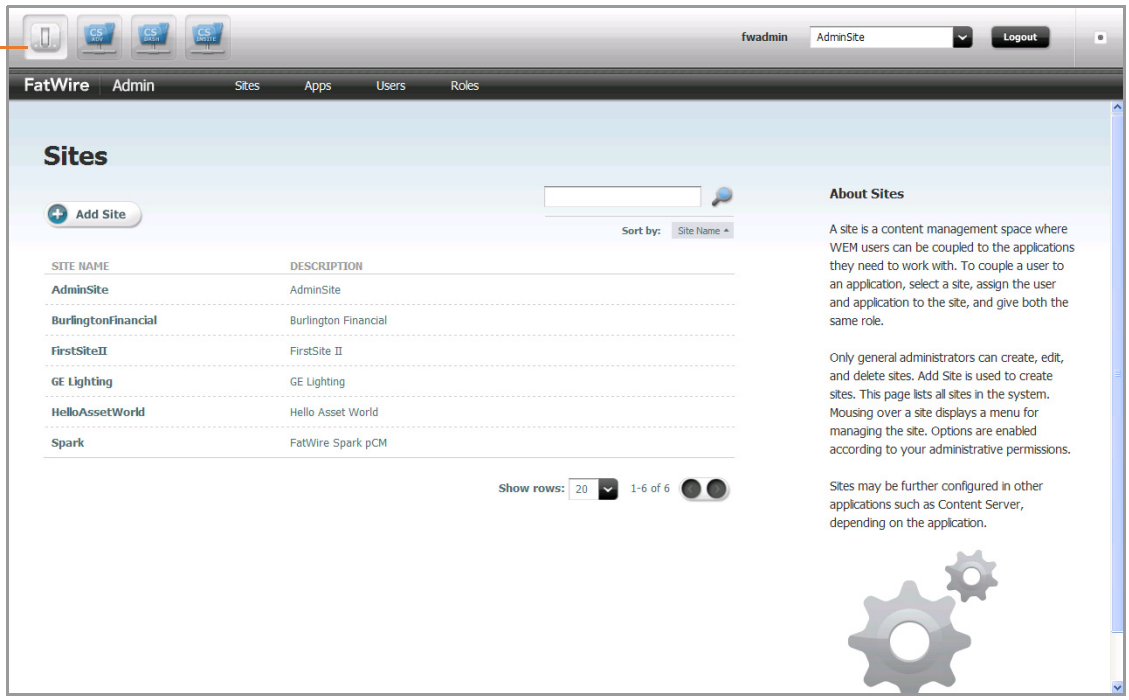


5. Click the arrow at the right of the WEM interface, then click the pin icon.



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: CS Advanced, CS Dash, and CS InSite interfaces.

WEM Admin

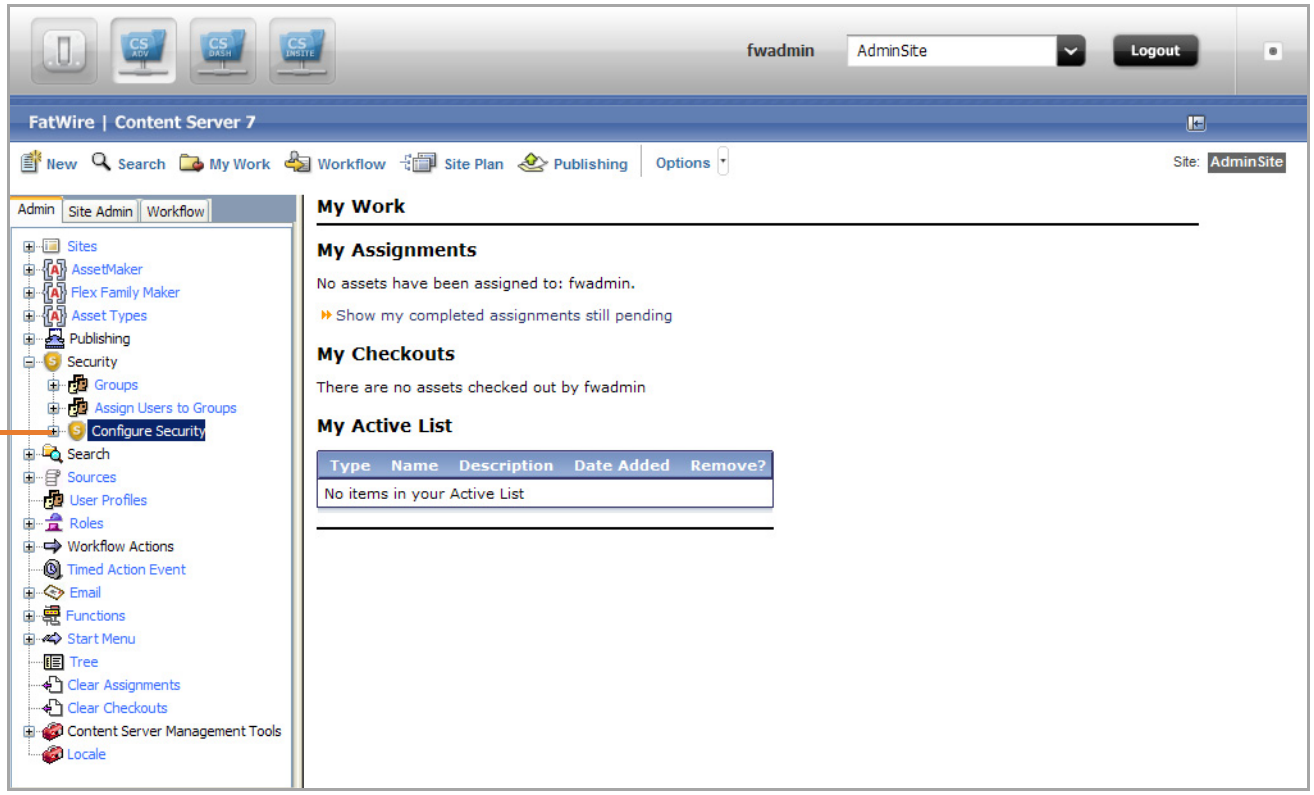


6. Verify that CS Advanced and CS Dash display their interfaces as shown on pages 21–25.

Note

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

Security Node (CS Advanced Interface)

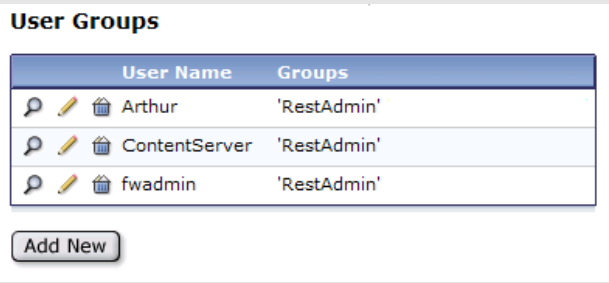


Note

The general administrator that was used during the installation process (`fwadmin`) 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 Content Server Advanced as the general administrator that was used during the installation process.
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*.



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 (CS-WEM Installations)

If you installed WEM and need to redeploy CAS, you must do so manually. Follow up by removing CAS from the primary cluster member, and reconfigure Content Server to detect the CAS application's new server. (i.e., locate the `SSOConfig.xml` file in the `WEB-INF/classes` directory of the `cs.war` file and update the `casURL` property to point to the server where CAS is redeployed).

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*.

Enabling inCache

If inCache was not enabled in either patch 3 or patch 4, it is not automatically enabled in patch 5 (the traditional caching method runs by default). It remains disabled until the `cs.useEhcache` property is set to `true` for each JVM and Remote Satellite Server, and until it is configured to work with Content Server. Enabling the inCache component creates the following tables in Content Server's database during runtime:

- `FW_InvalidationMemory`
- `FW_RegenCriteria`

If you wish to enable inCache, see the *Content Server Developer's Guide* for instructions.

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 Remote Satellite Server

Remote Satellite Server is used for load balancing. Installation instructions are available in the Satellite Server installation guide.