Content Server / Spark

Version: 6.3

Guidelines for Upgrading to Version 6.3

Document Revision Date: Jun. 15, 2011

FatWire SOFTWARE

Content Server / Spark: Guidelines for Upgrading to Version 6.3
Document Revision Date: Jun. 15, 2011
Product Version: 6.3

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

Introduction

This document provides instructions on upgrading your Content Server or Spark installation:

- From Content Server 5.x or 6.x to Content Server 6.3
- From Spark 6.x to Spark 6.3

Note

Anyone using this document is expected to have experience installing and configuring Content Server, Spark, and J2EE components such as databases, web servers, application servers, and portal servers.

This chapter applies to both Content Server and Spark. It contains the following sections:

Best Practices

- Before upgrading, create a complete backup of your Content Server (Spark) file system and database, in case an upgrade failure occurs.
- For Content Server installations, FatWire recommends that you do not upgrade clusters; delete the old cluster installations and replace them with new ones for best performance.
- FatWire recommends that you do not upgrade production environments. Upgrade only the development site, then publish to a new Content Server (Spark) 6.3 production installation.
- Upgrades on Jump Start kits are not supported.

Before Upgrading

Before upgrading, do the following:

1. Create a complete backup of your Content Server (Spark) file system and database.
2. Read the *Release Notes* (included on the Content Server (Spark) installation CD). The release notes (and the product documentation set for version 6.3) are also available at the following URL:

   `http://e-docs.fatwire.com`

   Note

   The e-docs website is password-protected; if you do not have a password, you will need to obtain one from FatWire Technical Support. For Technical Support contact information, see the following website:

   `http://www.fatwire.com/Support/contact_info.html`

3. Make sure you have all the information about your existing installation, such as web server configuration, application server configuration, database configuration, and LDAP configuration. All the information about your installation should have been recorded when Content Server (Spark) was originally installed.
4. Edit `futuretense.ini` in the Content Server installation directory (using the Property Editor) by making the following changes:
   a. In the “Basic” tab, make a note of the value set for `secure.CatalogManager`, then change the value to `false`. Change this property value back to its original value after the upgrade.
   b. In the “Cluster” tab, make a note of the value (if any) set for `ft.sync`, then set the value to `false`. After the upgrade, change the `ft.sync` value back to its original value.

Chapter 2

Upgrading from CS 5.*x* or CS 6.*x* to CS 6.3

This chapter provides instructions for upgrading Content Server installations that use either bundled or external LDAP servers.

This chapter contains the following sections:

Upgrade Steps

Note

Before starting the steps in this section, make sure you have read the "Best Practices" section and completed the steps in "Before Upgrading," both on page 6.

Complete the following steps to upgrade your CS 5.x or CS 6.x to CS 6.3:

1. Run `CombinedInstall.sh` (on Unix) or `CombinedInstall.bat` (on Windows) from the unzipped installation kit.
2. In the "Select Install Operation" screen, select **Install Fatwire Products** and click **Next**.
3. In the "Installation Directory" screen, choose the directory in which your existing CS 5.x or CS 6.x is installed, and click **Next**.
4. In the "Select Products" screen, select the products that you want to upgrade. In this document we assume that you select **ContentServer v6.3.0** as well as **Content Server Applications v6.3.0**. Click **Next**.
5. In the "Installation Type" screen, select **Single Server**, then click **Next**.
6. In the "IPS Install Options" screen, previously installed components are automatically detected. (You cannot deselect any products already installed; the installer will automatically upgrade them.) Select any additional options, then click **Next**.
7. In the "Content Server Configuration" screens:
   a. Enter the password for the Content Server administrator user (this user was used to install Content Server initially; the installer automatically detects the user name from your existing installation).

      Note

      The password that you enter must exactly match the password for the existing installation, or the upgrade will fail.

   b. Click **Next**.
   c. Enter the password for the "fwadmin" user.

      Note

      The password that you enter must exactly match the password for the existing installation, or the upgrade will fail.

   d. Click **Next**.

8. In the "Web Server Configuration" screen, the values in the fields are automatically filled in from your existing Content Server installation. Correct the values if your configuration has changed, then click **Next**.

> **Note**
>
> If you are performing LDAP integration with Sun ONE, replace the web server information with the application server host name and port number. You may use a web server in front of the application server after you finish the upgrade.

9. In the "Content Server Platform Type" screen, select the platform type that you are using, then click **Next**.
10. In the "Select Server for Installation" screen, select the server that you are using, then click **Next**.
11. Complete the configuration steps that apply to the server you selected in the previous step:

If you selected ...	Go to ...
WebLogic Application Server	"WebLogic Application Server" on page 24
WebSphere Application Server	"WebSphere Application Server" on page 25
Sun Application Server	"Sun Application Server" on page 25
WebLogic Portal Server	"WebLogic Portal Server" on page 26
Sun Portal Server on Web Server	"Sun Portal Server on WebServer" on page 27
JES Sun Portal Server on Sun Application Server	"JES Sun Portal Server on Sun Application Server" on page 27

12. The "Server Installation Options" screen displays a list of applications that will be upgraded. All the existing applications will be upgraded by default. Select any applications that you want to add to your existing installation, then click **Next**.
13. In the "Configuration Options" screen, check the box next to **Content Management** if you have sample sites in your existing installation that you want to upgrade, or if you want to install any new sample sites (such as FirstSite or Company Launchpad).

> **Note**
>
> If you already have sample sites installed, the checkbox is pre-selected and disabled. You cannot deselect it.

14. If you selected **Content Management**, proceed to the next step. If you did not select **Content Management**, proceed to step 21.

15. In the “Sample Portlets” screen, select **Spark Sample Portlets** if you wish to install the Spark sample site.

> **Note**
>
> If you are upgrading from CS 6.2 and have previously installed the Spark sample site, it is pre-selected. You cannot deselect it.

16. In the “Log Configuration” screen, select the type of logging you wish to have implemented.
17. In the “Sample Asset Type Options” screen, select the sample asset types that you want to upgrade/install. The ones that were originally installed will be selected automatically.

> **Warning**
>
> Any old sample asset types that were being used will be upgraded, and loss of data is possible. The loss of data will occur only if you used any of the **sample sites** or **sample asset types** in your existing implementation.

18. In the “Sample Site Options” screen, select the sample sites that you want to upgrade or install. The sample sites that were originally installed will be selected and upgraded automatically.
19. In the “FirstSiteII Components” screen, select the FirstSiteII components that you wish to install.
20. In the “CS-SiteLauncher Prototypes” screen, select the sample site that you want to install.
21. In the “Transact Connectivity Installation Options” screen, leave the default value selected.

    Note that this screen will appear only if you have Commerce Connector installed.
22. In the “Configuration Options” screen, select the products for which you want the Property Editor to open during the upgrade installation, then click **Next**.
23. In the “Content Server Applications Install” screen, click **Install** to start the upgrade process.
24. When the “Warning” dialog box is displayed, **DO NOT click OK**. Instead, continue with the next step.
25. Do one of the following:
    - If you are not using an external LDAP server, proceed to step 26.
    - If you are using an external LDAP server and you are upgrading from CS 5.x, proceed to “Upgrading from Content Server 5.x” on page 11.
    - If you are using an external LDAP server and you are upgrading from CS 6.x, proceed to “Upgrading from Content Server 6.x” on page 12.

26. Complete the steps that apply to the application server or portal server you are using. The steps show you how to test Content Server and complete the upgrade.

If using ...	Go to ...
WebLogic Application Server or Portal Server	"WebLogic Application Server or Portal Server" on page 30
WebSphere Application Server	"WebSphere Application Server" on page 30
Sun Application Server	"Sun Application Server" on page 31
Sun Portal Server	"Sun Portal Server" on page 32

Configuring an External LDAP Server

The following sections provide steps you must complete if you are using an external LDAP server.

Upgrading from Content Server 5.*x*

If you are using an external LDAP server in your Content Server 5.x installation, complete the following steps to configure the LDAP server for use with Content Server 6.3 and any sample sites you installed. During the configuration, you will verify:

- The mapping of Content Server ACLs to LDAP groups
- Users in LDAP and their assignments to the LDAP groups

Warning

If the user management components (users and mapped ACLs) as required by the installation do not exist in the external LDAP server when the upgrade is performed, the upgrade will fail.

When the "Warning" dialog is displayed, complete the following steps to configure the LDAP server before proceeding with the upgrade process:

1. Set the following property as shown below to notify Content Server that you are using LDAP for user authentication:

   `className.IUserDir=com.openmarket.directory.jndi.LDAPUserDir`

   (located in the `dir.ini` property file, "Interface Implementations" tab).
2. Verify that an LDAP group exists for each Content Server default ACL (listed in Table 1, "System Default ACLs" on page 14) and that the LDAP group names exactly match the ACL names.
3. Complete the following steps to configure users in LDAP:
   a. Verify that the LDAP system contains all of the Content Server system default users (see Table 2, "System Default Users and Sample Site Users" on page 14 for

a list of users). The LDAP server must contain all of the system default users for Content Server to function normally.

b. If you are installing any new sample sites:

1) Add each site's sample users to LDAP. See Table 3, "Mappings for Sample Sites, Users, and Roles" on page 15 for a list of sample sites and corresponding sample users.

2) Assign each user to the required LDAP groups. See Table 4, "Users and Required ACLs" on page 16 for a listing of the sample site users that must be assigned to each LDAP group.

c. Verify that all users have been assigned to their required LDAP groups.

4. Continue the upgrade process (return to step 26 on page 11).

Note

In version 5.x, LDAP was supported for storing users and ACLs only. When you upgrade to version 6.3, you have the option of storing sites and roles in LDAP as well. However, we recommend that you do not configure LDAP to store sites and roles until after the upgrade. For instructions on configuring the LDAP server to store sites and roles, refer to the *Content Server Administrator's Guide* or the *Spark Administrator's Guide* after you complete the upgrade process.

Upgrading from Content Server 6.*x*

If you are using an external LDAP server to store users and ACLs for your Content Server 6.x installation, and are installing any new sample sites (sites that were not installed as part of your existing CS installation), you need to make sure that the LDAP server contains the users and mapped ACLs as required by the sample site(s) you are installing.

If you are also using the external LDAP server to store sites and roles, you need to add any new sample sites to the LDAP server and then create the required mappings between users, sites, and roles in the LDAP server.

Warning

If the user management components (users, ACLs, sites, roles) and the mappings between these components as required by the installation do not exist in the external LDAP server when the upgrade is performed, the upgrade will fail.

When the "Warning" dialog is displayed (step 25 on page 10), complete the following steps to configure the LDAP server before proceeding with the upgrade process:

1. Verify that all of the Content Server system default ACLs (listed in Table 1, "System Default ACLs" on page 14) have corresponding LDAP user groups whose names exactly match the ACLs.

2. Complete the following steps to configure users in LDAP:
   a. Verify that the LDAP system contains all of the Content Server system default users (see Table 2, "System Default Users and Sample Site Users" on page 14 for a list of users). The LDAP server must contain all of the system default users for Content Server to function normally.
   b. If you are installing any new sample sites:
      1) Add each site's sample users to LDAP. See Table 3, "Mappings for Sample Sites, Users, and Roles" on page 15 for a list of sample sites and corresponding sample users.
      2) Assign each user to the required LDAP groups. See Table 4, "Users and Required ACLs" on page 16 for a listing of the sample site users that must be assigned to each LDAP group.
   c. Verify that all users have been assigned to their required LDAP groups.
3. If you are using LDAP to store sites and roles, complete the following steps in LDAP:
   a. For each new site that you installed, create a corresponding site in LDAP.
   b. For each site, create a group for each role that uses the site (see Table 3, "Mappings for Sample Sites, Users, and Roles" on page 15 for a list of the roles required for each site). Be sure to add the system default role named GeneralAdmin to each site.
   c. For each role group, add the appropriate users (see Table 3, "Mappings for Sample Sites, Users, and Roles" on page 15 for a list of the users that must be mapped to each role group).
4. Continue the upgrade process (return to step 26 on page 11).

Reference: System Defaults and Sample Site Parameters

Tables in this section contain parameters that will help you complete the steps for configuring an external LDAP server.

Table 1: System Default ACLs

ACLs	ACLs
Browser	UserReader
ContentEditor	Visitor
ElementEditor	VisitorAdmin
ElementReader	WSUser
PageEditor	WSAdmin
RemoteClient	WSEditor
SiteGod	xceladmin
TableEditor	xcelediter
UserEditor	xcelpublish

Table 2: System Default Users and Sample Site Users

User name	Password	User name	Password
ContentServer*	password	Moe	hello
DefaultReader*	SomeReader	fwadmin	xceladmin
fwadmin*	xceladmin	user_checker	user
mirroruser*	mirroruser	user_editor	user
user_author	user	editor	xcelediter
user_approver	user	user_marketer	user
user_designer	user	user_pricer	user
Coco	hello	user_analyst	user
Bobo	hello	user_expert	user
Flo	hello	firstsite	firstsite
Joe	hello		

* System default user. System default users are required to exist in LDAP for normal Content Server functionality.

Table 3: Mappings for Sample Sites, Users, and Roles

Site	User	Roles
Burlington Financial	fwadmin	Workflow Admin, SiteAdmin, General Admin
	editor	Checker, Author, Editor, Approver
	user_analyst	Analyst
	user_approver	Approver
	user_author	Author
	user_checker	Checker
	user_designer	Designer
	user_editor	Editor
	user_expert	Expert
	user_marketer	Designer, Marketer
GE Lightning	fwadmin	Designer, SiteAdmin, WorkflowAdmin, GeneralAdmin
	editor	Checker, Editor, Author, Pricer, Approver, Designer, Marketer
	user_approver	Approver
	user_author	Author
	user_checker	Checker
	user_designer	Designer
	user_editor	Editor
	user_marketer	Designer, Marketer
Hello Asset World	Bobo	WorkflowAdmin, GeneralAdmin
	Coco	HelloDesigner, GeneralAdmin
	Flo	HelloEditor
	Joe	HelloAuthor
	Moe	HelloAuthor
	fwadmin	WorkflowAdmin, GeneralAdmin

Table 3: Mappings for Sample Sites, Users, and Roles *(continued)*

Site	User	Roles
Company Launchpad (CO)	fwadmin	Designer, WorkflowAdmin, GeneralAdmin
	user_approver	Approver
	user_author	Author
	user_designer	Designer
FirstSite	fwadmin	Designer, WorkflowAdmin, GeneralAdmin
	firstsite	BrandManager, Approver, GeneralAdmin, Marketer, Artist, Author, StaffWriter, Editor, SiteAdmin, Designer, ProductSpecialist, WorkflowAdmin

Table 4: Users and Required ACLs

ACL (LDAP Group)	Users (Group Members)
Browser	all users
ContentEditor	firstsite
ElementEditor	user_designer, Coco, ContentServer, fwadmin, editor, mirroruser, firstsite
ElementReader	user_marketer, user_pricer, user_analyst, user_expert, firstsite, ContentServer, user_author, user_approver, Coco, Bobo, Flo, Joe, Moe, user_checker, user_editor
PageEditor	ContentServer, user_designer, Coco, fwadmin, editor, mirroruser, firstsite
RemoteClient	user_author, user_approver, user_designer, fwadmin, user_checker, user_editor, user_marketer, user_pricer, user_analyst, user_expert, firstsite
SiteGod	firstsite, ContentServer
TableEditor	ContentServer, user_designer, Coco, fwadmin, mirroruser, firstsite
UserEditor	ContentServer, Bobo, Admin, firstsite
UserReader	ContentServer, user_author, user_approver, user_designer, Coco, Bobo, Flo, Joe, Moe, fwadmin, user_checker, user_editor, mirroruser, user_marketer, user_pricer, user_analyst, user_expert, firstsite

Table 4: Users and Required ACLs *(continued)*

ACL (LDAP Group)	Users (Group Members)
Visitor	DefaultReader, user_author, user_approver, user_designer, fwadmin, user_checker, user_editor, mirroruser, user_marketer, user_pricer, user_analyst, user_expert, firstsite
VisitorAdmin	user_designer, fwadmin, mirroruser, firstsite
WSUser	user_author, user_approver, user_designer, fwadmin, user_checker, user_editor, user_marketer, user_pricer, user_analyst, user_expert, firstsite
WSAdmin	fwadmin, firstsite
WSEditor	user_author, user_approver, user_designer, fwadmin, user_checker, user_editor, user_marketer, user_pricer, user_analyst, user_expert, firstsite
xceladmin	Coco, Bobo, fwadmin, mirroruser, firstsite
xceleditor	user_author, user_approver, user_designer, Coco, Bobo, Flo, Joe, Moe, fwadmin, user_checker, user_editor, editor, mirroruser, user_marketer, user_pricer, user_analyst, user_expert, firstsite
xcelpublish	user_author, user_approver, user_designer, Coco, Bobo, Flo, Joe, Moe, fwadmin, user_checker, user_editor, editor, mirroruser, user_marketer, user_pricer, user_analyst, user_expert, firstsite

Chapter 3

Upgrading from Spark 6.*x* to Spark 6.3

This chapter provides instructions for upgrading Spark installations to version 6.3. All Spark installations use bundled LDAP servers, which are automatically configured during the upgrade process.

This chapter contains the following section:

- Upgrade Steps

Upgrade Steps

Note

Before starting the steps in this section, make sure you have read the "Best Practices" section and completed the steps in "Before Upgrading," both on page 6.

1. Run `sparkinstall.sh` (on Unix) or `sparkinstall.bat` (on Windows) from the unzipped installation kit.
2. In the "Installation Directory" screen, choose the directory in which your existing Spark 6.*x* is installed, and click **Next**.
3. In the "Content Server Configuration" screen, enter the password for the "fwadmin" user (the installer automatically detects the user name from your existing installation). Click **Next**.

Note

The password that you enter for the "fwadmin" user must exactly match the password for the existing installation, or the upgrade will fail.

4. In the "Web Server Configuration" screen, the values in the fields should be automatically filled in from your existing Content Server installation. Correct the values if your configuration has changed, then click **Next**.

Note

If you are performing LDAP integration with Sun ONE, replace the web server information with the application server host name and port number. You may use a web server in front of the application server after you finish the upgrade.

5. In the "Select Server for Installation" screen, select the portal server that you are using, then click **Next**.

6. Complete the configuration steps that apply to the server you selected in the previous step:

If you selected ...	Go to ...
WebLogic Portal Server	"WebLogic Portal Server" on page 26
Sun Portal Server on Web Server	"Sun Portal Server on WebServer" on page 27
JES Sun Portal Server on Sun Application Server	"JES Sun Portal Server on Sun Application Server" on page 27

7. In the "Configuration Options" screen, select the **Content Management** checkbox if you want to upgrade the samples in the Spark Site.
8. In the "Sample Portlets" screen, select **Refresh Spark sample portlets** if you want to refresh the reference Spark sample Portlets.
9. In the "Log Configuration" screen, select the kind of logging that you want to implement.

Note

In this step and the next, if the Content Management and Spark sample portlets were installed in your original installation, their checkboxes are pre-selected. You will not be able to deselect them.

10. In the "Sample Site Options" screen, select the sample sites that you want to upgrade or install. The sample sites that were originally installed will be selected and upgraded automatically.
11. In the "FatWire Corporation Install" screen, click **Install** to start the upgrade process.
12. When the "Warning" dialog box is displayed, **DO NOT click OK**. Instead, continue with the next step.
13. Complete the steps that apply to the application server or portal server you are using. The steps show you how to test Spark and complete the upgrade.

If using ...	Go to ...
WebLogic Portal Server	"WebLogic Application Server or Portal Server" on page 30
Sun Portal Server	"Sun Portal Server" on page 32

Appendix A

Configuring Application and Portal Servers

This appendix applies to Content Server and Spark upgrades. It provides instructions on configuring the application or portal server during the upgrade process.

This appendix contains the following sections:

WebLogic Application Server

1. In the “WebLogic Directory” screen, the directory in which WebLogic is installed are filled in by default from your existing installation. Make sure the directory is correct, then click **Next**.
2. In the “WebLogic Parameters” screen, the values for the WebLogic parameters are automatically filled in from your existing installation (do not change the values, unless they have changed since the original installation). Verify that all the WebLogic parameters are correct, then click **Next**.
3. In the “WebLogic Application Configuration” screen, do the following:
   a. Select **Yes** or **No** to indicate if you are running WebLogic as a managed server.
   b. For the **CS-LDAP Integration** option:
      - If you are using BEA's integrated LDAP, select **Yes**.
      - If you are not using LDAP, or if you have configured an external LDAP, such as Netscape Directory Server, Active Directory or any other external LDAP, select **No** for this option.
4. In the “Database Configuration” screen, do the following:
   a. Select the database you are using (make sure you select the version that you are currently using.)
   b. Verify the JNDI name.
   c. Click **Next**.
5. If you are running WebLogic as a managed server, proceed to the next step. If you are not running WebLogic as a managed server:
   - Proceed to step 12 on page 9 to continue the Content Server upgrade.
   - Proceed to step 9 on page 21 to continue the Spark upgrade.
6. In the “WebLogic Admin Server Integration” screen, the values are automatically filled in from your existing installation. Verify that the values are correct and click **Next**.
7. In the “WebLogic Admin Server Integration” screen, the value for the **WebLogic Server Administrator Account Name** is automatically filled in from your existing installation. Enter the correct password; you should have a record of the password in the installation worksheets for your existing installation. Click **Next**.
8. If you are upgrading a Content Server installation, proceed to step 12 on page 9.
   If you are upgrading a Spark installation, proceed to step 9 on page 21.

WebSphere Application Server

1. In the "WebSphere Deployment Root" screen, the values are automatically filled in from the existing installation. Refer to the installation worksheets for your existing installation and verify that all of the values are correct. Click **Next**.
2. In the "Database Configuration" screen:
   a. Select the database you are using (make sure you select the version that you are currently using.)
   b. Verify the JNDI name.
   c. Click **Next**.
3. If you are upgrading a Content Server installation, proceed to step 12 on page 9.
   If you are upgrading a Spark installation, proceed to step 9 on page 21.

Sun Application Server

1. In the "Sun Installation Directory" screen, do the following:
   a. Verify that the path to your Sun Application Server is correct and that it corresponds to your existing installation.
   b. Verify that the WebApplication URI is correct; it must be the WebApplication URI from the existing installation.
   c. Click **Next**.
2. In the "Database Configuration" screen, do the following:
   a. Select the database you are using (make sure it is the correct version that you are currently using).
   b. Verify the JNDI name.
   c. For the **CS-LDAP Integration** option:
      - If you are using the Sun ONE Identity Server, select **Yes**. You will later see an additional screen where you will need to verify the LDAP settings.
      - If you are not using LDAP, or if you have configured an external LDAP, such as Netscape Directory Server, Active Directory or any other external LDAP, select **No** for this option.
   d. Click **Next**.
3. In the "SAS Configuration" screen, verify that the following values are correct (all the values in this screen should match the existing installation of CS 5.x or CS 6.x), then click **Next**.
   - The domain name in which the application will be deployed
   - The server name
   - The application name
4. In the "LDAP Integration" screen (which will only appear if you selected **Yes** for LDAP), your existing LDAP settings are filled in if you integrated with LDAP when you installed CS 5.x or CS 6.x. Verify these settings and click **Next** to continue.

5. If you are upgrading a Content Server installation, proceed to step 12 on page 9.
If you are upgrading a Spark installation, proceed to step 9 on page 21.

WebLogic Portal Server

1. In the "WebLogic Directory" screen, the directory in which WebLogic is installed is filled in by default from your existing installation. Make sure the directory is correct, then click **Next**.
2. In the "WebLogic Parameters" screen, the values for the WebLogic parameters are filled in from your existing installation (do not change the values, unless they have changed since the original installation). Verify that all the WebLogic parameters are correct, then click **Next**.
3. In the "WebLogic Application Configuration" screen, do the following:
   a. Select **Yes** or **No** to indicate if you are running WebLogic as a managed server.
   b. For the **CS-LDAP Integration** option:
      - If you are using BEA's integrated LDAP, select **Yes**.
      - If you are not using LDAP, or if you have configured an external LDAP, such as Netscape Directory Server, Active Directory or any other external LDAP, select **No** for this option.
4. In the "Database Configuration" screen, do the following:
   a. Select the database you are using (make sure you select the version that you are currently using.)
   b. Verify the JNDI name.
   c. Click **Next**.
5. If you are using WebLogic's bundled server, ensure that the correct values are shown in the "LDAP Integration" screen. Enter the correct password in the "JNDI Password" field and its verification fields. Click **Next**.
6. If you are running WebLogic as a managed server, proceed to the next step. If you are not running WebLogic as a managed server:
   - Proceed to step 12 on page 9 to continue the Content Server upgrade.
   - Proceed to step 9 on page 21 to continue the Spark upgrade.
7. In the "WebLogic Admin Server Integration" screen, the values are automatically filled in from your existing installation. Verify that the values are correct and click **Next**.
8. In the "WebLogic Admin Server Integration" screen, the value for the **WebLogic Server Administrator Account Name** is automatically filled in from your existing installation. Enter the correct password; you should have a record of the password in the installation worksheets for your existing installation. Click **Next**.
9. If you are upgrading a Content Server installation, proceed to step 12 on page 9.
If you are upgrading a Spark installation, proceed to step 9 on page 21.

Sun Portal Server on WebServer

1. In the “Sun Installation Directory” screen, do the following:
   a. Verify that the path to your Sun Application Server is correct and that it corresponds to your existing installation.
   b. Verify that the WebApplication URI is correct; it must be the WebApplication URI from the existing installation.
   c. Click **Next**.
2. In the “Database Configuration” screen, do the following:
   a. Select the database you are using (make sure it is the correct version that you are currently using.
   b. Verify the JNDI name.
   c. For the **CS-LDAP Integration** option:
      - If you are using the Sun ONE Identity Server select **Yes** for this option. You will see later see a screen where you will need to verify the LDAP settings.
      - If you are not using LDAP, or if you have configured an external LDAP, such as Netscape Directory Server, Active Directory or any other external LDAP, select **No** for this option.
      - Click **Next**.
3. In the “LDAP Integration” screen (which will appear only if you selected **Yes** for LDAP), your existing LDAP settings are filled in if you integrated with LDAP when you installed CS 5.x or CS 6.x. Verify these settings and click **Next** to continue.
4. If you are upgrading a Content Server installation, proceed to step 12 on page 9.
   If you are upgrading a Spark installation, proceed to step 9 on page 21.

JES Sun Portal Server on Sun Application Server

1. In the “Sun Installation Directory” screen, do the following:
   a. Verify that the path to your Sun Application server is correct and that it corresponds to your current installation.
   b. Verify that the WebApplication URI is correct; it must be the WebApplication URI from the existing installation.
   c. Click **Next**.
2. In the “Database Configuration” screen, do the following:
   a. Select the database you are using. Make sure it is the correct version that you are currently using.
   b. Verify the JNDI name.
   c. For the **CS-LDAP Integration** option:
      - If you are using the Sun ONE Identity Server, select **Yes** for this option. You will see later see a screen that displays the existing LDAP settings.

- If you are not using LDAP, or if you have configured an external LDAP, such as Netscape Directory Server, Active Directory or any other external LDAP, select **No** for this option.

d. Click **Next**.

3. In the "SAS Configuration" screen, verify that the following values are correct, then click **Next** (all the values in this screen should match the existing installation of CS 5.x or CS 6.x).
   - the domain name in which the application will be deployed
   - the server name
   - the application name
4. In the "LDAP Integration" screen (which will only appear if you selected **Yes** for LDAP), your existing LDAP settings are filled in if you integrated with LDAP when you installed CS 5.x or CS 6.x. Verify these settings and click **Next** to continue.
5. If you are upgrading a Content Server installation, proceed to step 12 on page 9.
   If you are upgrading a Spark installation, proceed to step 9 on page 21.

Appendix B

Testing Content Server and Spark

In this appendix, you will test your upgraded installation by running the HelloCS and pingdb tests.

This appendix contains the following sections:

Follow the steps in the section that applies to the application server or portal server your installation is using.

WebLogic Application Server or Portal Server

1. Start the administration server and the managed server (if you are using a managed server).
2. Go to the WebLogic Console.
3. Redeploy the Content Server web application or the Spark application.
4. Restart the WebLogic administration server and managed server.
5. Verify that the following URLs are working:

   HelloCS:

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

   pingDB:

   ```
   http://<hostname>:<port>/<context root>/
   CatalogManager?ftcmd=pingdb
   ```

   Note

   If either URL fails, you cannot proceed with the upgrade. See Appendix C, "Troubleshooting HelloCS and pingdb Test Failures" for suggestions on how to resolve the issue that may be causing test failure.

6. If both of the above URLs are working, complete the upgrade as follows:
   a. Click **OK** in the "Warning" dialog.
   b. Edit `futuretense.ini` by re-setting the properties `secure.CatalogManager` and `ft.sync` to their original values (see step 4 on page 6).
   c. Test your system by logging in.

WebSphere Application Server

1. Start the WebSphere Application Server.
2. Go to the WebSphere Administrative Console and stop the existing Content Server (Spark) application.
3. Uninstall the Content Server (Spark) application.
4. Save the Master Configuration.
5. Install a new Enterprise Application by completing the following steps:
   a. In the left-hand tree, select **Applications > Install New Application**.
   b. In the "Specify EAR/WAR/JAR module" screen, do the following, browse for the `contentserver.ear` file (located in `<ContentServer root directory>/ominstallinfo/app/`), then select **Next**.
   c. Click through the remaining screens, accepting the default options for each screen.

6. Change the classloader priority for the application server by completing the following steps:
   a. In the left-hand tree, select **Applications > Enterprise Applications**.
   b. Click on the Content Server (Spark) application.
   c. Change the **Classloader Mode** to **PARENT_LAST**.
   d. Change the **WAR Classloader Policy** to **Application**.
   e. Click **Apply** and save the Master Configuration.
7. Restart the WebSphere server.
8. Log in to the WebSphere Administrative Console and verify that the Content Server (Spark) application is running.
9. Verify that the following URLs are working:

   HelloCS:

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

   pingDB:

   ```
   http://<hostname>:<port>/<context root>/
   CatalogManager?ftcmd=pingdb
   ```

   Note

   If either URL fails, you cannot proceed with the upgrade. See Appendix C, “Troubleshooting HelloCS and pingdb Test Failures” for suggestions on how to resolve the issue that may be causing test failure.

10. If both of the above URLs are working, complete the upgrade as follows:
    a. Click **OK** in the “Warning” dialog.
    b. Edit `futuretense.ini` by re-setting the properties `secure.CatalogManager` and `ft.sync` to their original values (see step 4 on page 6).
    c. Test your system by logging in.

Sun Application Server

1. Start the Sun Application Server.
2. Redeploy the Content Server (Spark) application.
3. Restart the application server or the web server, depending on which one you are using.
4. Verify that the following URLs are working:

   HelloCS:

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

pingDB:

```
http://<hostname>:<port>/<context root>/
CatalogManager?ftcmd=pingdb
```

Note

If either URL fails, you cannot proceed with the upgrade. See Appendix C, "Troubleshooting HelloCS and pingdb Test Failures" for suggestions on how to resolve the issue that may be causing test failure.

5. If both of the above URLs are working, complete the upgrade as follows:
   a. Click **OK** in the "Warning" dialog.
   b. Edit `futuretense.ini` by re-setting the properties `secure.CatalogManager` and `ft.sync` to their original values (see step 4 on page 6).
   c. Test your system by logging in.

Sun Portal Server

1. Start the Sun application server or the web server.
2. Use the `pdeploy` command to uninstall the old Content Server (Spark) application; for example:

```
/opt/SUNWps/bin/pdeploy undeploy -u
"uid=amAdmin,ou=People,dc=fatwire,dc=com" -v -w password -d
"dc=fatwire,dc=com" -p password cs
```

3. Deploy the new `war` file; for example:

```
/opt/SUNWps/bin/pdeploy deploy -u
"uid=amAdmin,ou=People,dc=fatwire,dc=com" -v -w password -d
"dc=fatwire,dc=com"
-p password /opt/fatwire/ominstallinfo/app/cs.war
```

4. Restart the application server or the web server, depending on which one you are using.
5. Verify that the following URLs are working:

   HelloCS:

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

   pingDB:

   ```
   http://<hostname>:<port>/<context root>/
   CatalogManager?ftcmd=pingdb
   ```

Note

If either URL fails, you cannot proceed with the upgrade. See Appendix C, "Troubleshooting HelloCS and pingdb Test Failures" for suggestions on how to resolve the issue that may be causing test failure.

6. If both of the above URLs are working, complete the upgrade as follows:
   a. Click **OK** in the "Warning" dialog.
   b. Edit `futuretense.ini` by re-setting the properties `secure.CatalogManager` and `ft.sync` to their orignal values (see step 4 on page 6).
   c. Test your system by logging in.

Appendix C

Troubleshooting HelloCS and pingdb Test Failures

If either the HelloCS test or the pingdb test failed during the upgrade process, this appendix may be helpful. It provides suggestions on how to resolve the problem that may be causing test failure.

This appendix contains the following sections:

HelloCS Test

If the HelloCS test fails (HelloCS page is not displayed), there could be a configuration error or a web application deployment error. Completing the following steps may help determine the cause of the failure:

1. Run HelloCS directly on the application server to isolate any issues in the bridge between the web server and the application server.
2. Verify that the web application context root you are specifying in the URL is correct. For example, if `/CS` is the web application context root, then your URL would be:
   `http://<hostname>:<port>/CS/HelloCS`
3. Try redeploying the application, then restarting the application server. In some cases the previous application settings might be cached by the application server.

pingdb Test

Completing the following steps may help determine the problem:

1. Run the pingdb test directly on the application server to isolate any issues in the bridge between the web server and the application server.
2. Verify that the web application context root you are specifying in the URL is correct. For example, if `/CS` is the web application context root, then your URL would be:
   `http://<hostname>:<port>/CS/HelloCS`
3. Try redeploying the application, then restarting the application server. In some cases the previous application settings might be cached by the application server.
4. Verify that the connection pool is working correctly by testing the pool using the application server console.
5. Verify that the JNDI name that you specified during the upgrade process matches the one in the application server console.

   If the JNDI names do not match, cancel the “Warning” dialog, re-run the upgrade, and enter the correct values in the installer.