

CommonSpot™ Winter 2012 Installation Guide

This CommonSpot Installation Guide, as well as the software described with it, is provided under the CommonSpot License Agreement and may be used, copied and distributed only in accordance with the terms of the license. The content outlined in this manual is for informational purposes only and is subject to change without notice. By no means should the information contained herein be construed, as a commitment by PaperThin, Inc. PaperThin assumes no responsibilities or liability for errors or inaccuracies found in this documentation.

ColdFusion, Acrobat, and Flash are registered trademarks of Adobe Systems Incorporated. Microsoft, Windows, Microsoft SQL Server, Microsoft Word, Excel and PowerPoint, FrontPage and Windows NT are all registered trademarks of Microsoft Corporation. MySQL, Solaris, and Oracle are registered trademarks of Oracle Corporation, and Verity is a trademark of Autonomy, Inc. Railo is a product of Railo Technologies GmbH, Bern, Switzerland.

This document was last updated March 15, 2012.

Chapter 1 About the Installation Guide	5
Chapter 2 Pre-Installation Requirements and Considerations.....	6
2.1. Requirements	6
2.2. Worksheet for Settings and Configurations	6
2.3. Unzip Issues	9
2.4. Perform Pre-Installation Steps	10
Chapter 3 Installing CommonSpot.....	15
3.1. The Welcome Page.....	15
3.2. The “Before You Begin” Page.....	17
3.3. Phase 1: Install CommonSpot	18
3.3.1. Phase 1: Install CommonSpot (Step 1 of 4)	18
3.3.2. Phase 1: Install CommonSpot (Step 2 of 4)	19
3.3.3. Phase 1: Install CommonSpot (Step 3 of 4)	20
3.3.4. Phase 1: Install CommonSpot (Step 4 of 4)	21
3.4. Phase 2 – Configure Your Servers	22
3.4.1. Phase 2: Configure Servers (Step 1 of 8) Dialog	22
3.4.2. Phase 2: Configure Servers (Step 2 of 8) Dialog	23
3.4.3. Phase 2: Configure Servers (Step 3 of 8) Dialog	24
3.4.4. Phase 2: Configure Servers (Step 4 of 8) Dialog	24
3.4.5. Phase 2: Configure Servers (Step 5 of 8) Dialog	25
3.4.6. Phase 2: Configure Servers (Step 6 of 8) Dialog	26
3.4.7. Phase 2: Configure Servers (Step 7 of 8) Dialog	26
3.4.8. Phase 2: Configure Servers (Step 8 of 8) Dialog	27
3.5. Phase 3 – Configure Your Databases.....	29
3.5.1. Phase 3: Configure Databases (Step 1 of 5) Dialog	29
3.5.2. Phase 3: Configure Databases (Step 2 of 5) Dialog	30
3.5.3. Phase 3: Configure Databases (Step 3 of 5) Dialog	31
3.5.4. Phase 3: Configure Databases (Step 4 of 5) Dialog	32
3.5.5. Phase 3: Configure Databases (Step 5 of 5) Dialog	32
3.6. Phase 4 – Install the Demo Site and ADF Demo	34
3.6.1. Install Demo Site (Step 1 of 3) Dialog.....	35
3.6.2. Install Demo Site (Step 2 of 3) Dialog.....	35
3.6.3. Install Demo Site (Step 3 of 3) Dialog.....	37
Chapter 4 License Keys	39
4.1. Download and Install License Keys from PaperThin.com	39
4.2. The Activate License Key Dialog.....	39
4.3. Changing Servers.....	39
Chapter 5 Post-Installation Considerations	41
5.1. Back Up CommonSpot Databases.....	41
5.2. Create Scheduled Jobs	41
5.3. For Shared Database Environments, “Unmap” the Read-Only Production Server(s)	42
5.4. Installation Issues	42
5.5. CommonSpot Resources and Information	42
5.5.1. Microsoft Office Considerations.....	44
Chapter 6 Securing CommonSpot	45
6.1. Securing HTTP Server Access	45

- 6.2. Encrypting CommonSpot User Passwords 46
 - 6.2.1. Encryption Module..... 47
 - 6.2.2. Special Notes on Encryption 47
- 6.3. SQL Injection Issues 47
- 6.4. Controlling Access to CommonSpot Modules (URL Tampering) 48
 - 6.4.1. Direct Requests 49
 - 6.4.2. Loader Requests 49
 - 6.4.3. Configuring CommonSpot Security Access 49
 - 6.4.4. CommonSpot Security Logging 52

Chapter 1 About the Installation Guide

The *CommonSpot Winter 2012 Installation Guide* provides requirements and step-by-step instructions for installing the current version of CommonSpot. It is intended for those responsible for performing the installation and requires a good understanding of ColdFusion applications, Web server configuration, access to the ColdFusion Administrator, access to file system for CommonSpot installation, and the ability to create necessary databases.

If you have already installed CommonSpot and plan to upgrade to this release, please refer to the *CommonSpot Winter 2012 Upgrade Guide*.

This guide contains the following:

- [Pre-Installation Requirements and Considerations](#)
- [Installing CommonSpot](#)

Chapter 2 Pre-Installation Requirements and Considerations

This chapter specifies all hardware and software requirements for installing CommonSpot. This information reflects the information provided in this section of the installation Wizard.

Important Note: *This version of CommonSpot requires that all data sources run under UTF-8. Make sure that your environment supports this character set standard before installing.*

2.1. Requirements

Before installing this release of CommonSpot, please review all system requirements. You can find a full and up-to-date listing of requirements at <http://www.paperthin.com/support/tech-specs.cfm> You will need to make sure that you are running supported versions of the following:

- Operating System (Windows, Linux or Solaris)
- ColdFusion
- Database (SQL Server, Oracle or MySQL)
- Browser (Internet Explorer or Firefox)
- JVM

2.2. Worksheet for Settings and Configurations

You can use the worksheet below, or your own equivalent, to ensure that you have all the information you need before you proceed to the actual CommonSpot installation.

I have verified that my ColdFusion Settings are correct	Yes	No
I have verified that my JVM Settings are correct	Yes	No
I have read the Release Notes	Yes	No
My ColdFusion Administrator Password:		
I know not to download my license keys until prompted to do so	Yes	No

Directory to store license keys under:

I want to install an Authoring Server Yes No

I want to install a Read-Only Production Server (ROPS) Yes No

I want to install a Cache Server Yes No

Server License:

Customer License:

Server Name (spaces, dashes, and underscores are not allowed in the server name):

Server IP Address:

Proxy Server Address:

Proxy Server Port:

Date/Time settings

Password for the CommonSpot Administrator Account:

I want to enable client variables Yes No

I want to enable persistent cookies Yes No

CommonSpot Directory location:

Web Server Document Directory location:

Parent Directory of New Sites location:

Local Data Directory location:

Preferred Image Library:

Image Manipulation Directory location:

Message timeout setting:

Administrator's email address for CS email notifications:

Outgoing mail server for CS email notifications:

Email UserID for CS email notifications:

Email Password for CS email notifications:

Email Port For CS Email Notifications:

Email Timeout For CS Email Notifications:

The type of DB for my 'Sites' Database:

The type of DB for my 'Users' Database:

The type of DB for my new databases:

'Sites' Data source will be CommonSpot-Configured

Yes

No

'Sites' Data source will be Manually Configured (not recommended)

Yes

No

'Sites' DB Name:

'Sites' DB Server:

'Sites' DB Port:

'Sites' DB User ID:

'Sites' DB Password:

'Users' Data source will be CommonSpot-Configured

Yes

No

'Users' Data source will be Manually Configured (not recommended)

Yes

No

'Users' DB Name:

'Users' DB Server:

'Users' DB Port:

'Users' DB User ID:

'Users' DB Password:

Note: Your server name cannot contain any spaces, dashes, or underscores. CommonSpot returns an error for server names containing these special characters.

2.3. Unzip Issues

Microsoft security enhancements to the native Windows unzip utility disables JavaScript file extraction by default. Please ensure that you use an unzip utility that does not block JavaScript files.

If your installation uses this utility, you may discover missing, incomplete, or corrupted files after unzipping the CommonSpot archive, or you may find that CommonSpot user interface menus display but do not work.

You can usually correct this problem by trying again or using a different unzip utility.

2.4. Perform Pre-Installation Steps

Before you attempt to install CommonSpot, please review the important information in this section. The two tables under [Requirements](#) and [Worksheet for Settings and Configurations](#) above may also be helpful as you go through each part of this section.

Important: If you are upgrading from an older version of CommonSpot, please read the *CommonSpot Upgrade Guide* instead of this guide. This *Installation Guide* is designed specifically for new installations of CommonSpot.

1. Confirm that a supported version of ColdFusion or Railo is installed.

CommonSpot supports:

Adobe ColdFusion

- ColdFusion 8.0.1 with Cumulative Hot Fix 4
- ColdFusion 9.0.1 with Cumulative Hot Fix 1
- Adobe JRun 4 Application Server only
- Java SE 6 Update 24 for ColdFusion 8.0.1
- Java SE 6 Update 24 for ColdFusion 9.0.1

Railo 3.3.2

- Java SE 6 Update 24 or greater (excluding update 29) for Railo

Note: ColdFusion 8.0.0 and 9.0.0 are *not supported*.

Application Servers other than JRUN are *not supported in Adobe ColdFusion*.

To view the version of ColdFusion installed on your server, open the ColdFusion Administrator and click the System Information link. The resulting page displays the installed version of ColdFusion.

For the latest ColdFusion configuration settings, see:

<http://www.paperthin.com/support/knowledgebase/articles/configuration-settings.cfm>

2. Turn off ColdFusion and JRUN if they are running.

3. Download the most recent release of CommonSpot.

If you have not already done so, download the most recent CommonSpot release from the Support section of the PaperThin Web site:

<http://www.paperthin.com/support/downloads>

Note: To access the /downloads section of the PaperThin site, you must be registered as a Designated Support Representative.

4. Extract the CommonSpot release archive to your server.

After downloading the most recent CommonSpot archive, complete the following steps based on your operating system:

Note: Do not download the keys until you are presented with your server's validation code during the installation process and have placed the code into your keys.

For Windows:

1. Create a `\commonspot` directory at the root of your Web server or under an alias; for example, `c:\inetpub\wwwroot\commonspot`. Whether this directory is actually at the Web root or simply mapped is not important, as long as navigating to `{servername}/commonspot` in your Web browser is a valid path.
2. Unzip the zip archive file into the empty `\commonspot` directory. Be sure to preserve the directory structure when extracting the archive, and make sure ColdFusion and JRUN are OFF first.

For Linux and Solaris:

Create a `/commonspot` directory under the Web root directory or under a Web root alias. For example, `/var/apache/htdocs/commonspot`. Copy the archive file into the new `/commonspot` directory and extract it into the empty `/commonspot` directory. Make sure ColdFusion or Railo is OFF first.

Be sure to preserve the directory structure when extracting the archive. For example,

For ColdFusion (Unix only):

```
unzip cs-v70-ACF.zip
```

For Railo (Unix only):

```
unzip cs-v70-Railo.zip
```

Verify that the ColdFusion user has proper file permissions to the CommonSpot modules. For example, issue the following commands but replace *username* and *groupname* with the appropriate values for your server:

```
chown -R username:groupname *  
chmod -R 775 *
```

5. Configure your Web server.

You will need to configure your Web server appropriately to access CommonSpot. Refer to your Web server documentation and/or the ColdFusion documentation, for more information.

Also note that the Web server shipped with ColdFusion is not supported by PaperThin. This server is for development purposes and not intended for production.

6. Configure ColdFusion or Railo

You will need to configure your ColdFusion Server to appropriately access CommonSpot. You can do this through the ColdFusion Admin interface or you can manually alter the `jvm.config` file. To manually change the file, locate the JRUN folder for ColdFusion. Navigate to the `/bin` folder. Copy the `jvm.config` file, and save it to `jvm-config-orig.bak` (or another name) to make a backup copy of this file. Then edit the `jvm.config` file, add the full path to the `/commonspot/java` folder to the `java.class.path` line.

Note: Type this in, do not copy and paste in this file. Use only forward slashes (`/`). Save and close the file. Copy/paste operations may include characters that cause the ColdFusion startup to fail.

Make sure to make a backup copy of the `jvm.config` before making any changes.

Important Note: Make sure that ColdFusion does *not serve HTM or HTML files from within the CommonsSpot directory*. Configure ColdFusion to process *only site files as HTM or HTML, not files inside CommonsSpot*.

To Configure Railo:

In Server Administrator – Security – Access – General Access, set **Access Read** to **open**.

The screenshot shows the 'General Access' configuration window. It has two tabs: 'General' and 'Individual'. The 'General' tab is selected. Below the tabs, there is a description: 'Define the General Access for administrator and tag cfadmin'. Underneath, there is a link for 'General Access' and another description: 'Define the General Access for administrator and tag cfadmin'. At the bottom, there is a section for 'Access Read' with a dropdown menu set to 'open' and a label 'define the access for reading data'.

In Web Administrator – Archives & Resources – Mappings, create a `/commonsSpot` mapping.

The screenshot shows the 'Archives & Resources - Mappings' configuration window. It has a title bar 'Archives & Resources - Mappings'. Below the title bar, there is a description: 'Here you can edit a certain mapping or create a Railo archive out of an existing one.' Below the description, there is a table with the following fields:

Virtual	/commonsSpot
Resource	C:\wwwroot\commonsSpot
Archive	C:\wwwroot\cs-v70.ras
Primary	Resource
Inspect Templates (CFM/CFC)	<input checked="" type="radio"/> Never (Best Performance) When checked, any requested files found to currently reside in the template cache will not be inspected for potential updates. For sites where templates are not updated during the life of the server, this minimizes file system overhead. <input type="radio"/> Always (Bad) When checked, any requested files found to currently reside in the template cache will always be inspected for potential updates. For sites where templates are updated during the life of the server or within request.
Top Level	<input checked="" type="checkbox"/> Make this mapping web-accessible (i.e., accessible via a browser or remote HTTP call)

At the bottom of the window, there are two buttons: 'save' and 'cancel'.

Configure Railo by extracting commonsSpot resources and the archive file and mapping the archive through the Railo Administrator.

Unpack the `cs-v70-Railo.zip` and save the `/commonsSpot` directory and the `cs-v70.ras` archive to the Railo server. In the example below, both commonsSpot and the archive are extracted to `C:/cs-railo/`.

Server Administrator
Web Administrator

Archives & Resources - Mappings
Logout

Please note, that only pages processed by Railo are aware of these mappings (cfm, cfml, cfc). If you want to use files not processed by Railo for these special mapping directories, you have to add virtual mappings to these directories to your application server.

<input type="checkbox"/>	Virtual	Resource	Archive	Primary	Inspect
	/railo-context	{railo-web}/context/	{railo-web}/context/railo-context.ra	physical	Never
<input type="checkbox"/>	/_local_mssql	C:/cs-railo/commonsport-data/cu		Resource	Always
<input type="checkbox"/>	/commonsport	c:\cs-railo\commonsport\	c:\cs-railo\cs-v70.ras	Resource	Never
<input type="checkbox"/>	/mssql	C:/cs-railo/webroot/mssql		Resource	Always
<input type="checkbox"/>				Resource	Always

From the Railo Web Administrator, manually set the /commonsport mapping to use the cs-v70.ras archive, and make sure that **Primary** is set to **Resource**, as shown below.

Archives & Resources - Mappings

Here you can edit a certain mapping or create a Railo archive out of an existing one.

Virtual	/commonsport
Resource	c:\cs-railo\commonsport\
Archive	c:\cs-railo\cs-v70.ras
Primary	Resource
Inspect Templates (CFM/CFML/CFJC)	<input checked="" type="radio"/> Never (Best Performance) <small>When checked, any requested files found to currently reside in the template cache will not be inspected for potential updates. For sites where templates are not updated during the life of the server, this minimizes file system overhead.</small>
	<input type="radio"/> Always (Bad) <small>When checked, any requested files found to currently reside in the template cache will always be inspected for potential updates. For sites where templates are updated during the life of the server or within request.</small>
Top Level	<input checked="" type="checkbox"/> Make this mapping web-accessible (i.e., accessible via a browser or remote HTTP call)

In addition:

- Railo Web Administrator – Settings – Application: Script-protect must be set to **none**.

- Railo Web Administrator – Settings – Application: Request timeout in URL must be true.

Server Administrator Web Administrator

Settings - Application Logout

Here you can define several default settings for the application context. These settings can be overridden with the tag cfapplication or the Application.cfc.

Script-protect The configuration of Script protect, secures your system from "cross-site scripting"

Script-protect: none (selected), all, custom

Request timeout: Days: 0, Hours: 0, Minutes: 0, Seconds: 300

Request timeout in URL: When the URL parameter [RequestTimeout] is passed in the URL obey it

update cancel Reset to Server Administrator Setting

7. Read the Release Notes and related documents.

After downloading and extracting the CommonSpot archive, you will find copies of the most recent Release Notes and several other guides in the /commonspot/docs directory.

PaperThin strongly recommends that you read the Release Notes for any last-minute installation changes.

If you are planning to install CommonSpot in a Shared Database server environment, read the *CommonSpot Winter 2012 Shared Database Configuration Guide*.

8. Restart ColdFusion and run the installation, completing the Installing CommonSpot instructions in the next chapter.

Chapter 3 Installing CommonSpot

This chapter covers the actual installation procedure for a stand-alone Authoring server using the CommonSpot installation wizard. If you are installing an Authoring server or a Read-only Production Server or Cache Server in a Shared Database cluster configuration, please see the *Shared Database Configuration Guide*.

Before beginning the CommonSpot installation, please read the [Pre-Installation Requirements and Considerations](#) and complete all the steps outlined there.

The CommonSpot installation consists of [The Welcome Page](#), [The “Before You Begin” Page](#), and the following four phases:

- [Phase 1: Install CommonSpot](#)
- [Phase 2 - Configure Your Servers](#)
- [Phase 3 - Configure Your Databases](#)
- [Phase 4 - Install the Demo Site](#)

3.1. The Welcome Page

Open `/commonspot/installation/index.htm` in a compatible browser (Firefox or Internet Explorer). The first page in the CommonSpot installation wizard is a welcome screen, explaining installation steps.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | **Phase 1** Install CommonSpot | **Phase 2** Configure Servers | **Phase 3** Configure Databases | **Phase 4** Install Demo Site

Welcome to the CommonSpot Winter 2012 installation for Windows, Linux, and Sun Solaris.

CommonSpot is an award-winning, distributed Web publishing, content management and knowledge sharing application built on top of ColdFusion Application Server. The installation will be performed in four (4) phases, as listed below and in the toolbar above. Each phase will walk you through a series of steps, providing instructions as you go. The toolbar will be updated to show your progress through the phases.

The installation of CommonSpot is straightforward, however if you have any questions or problems you can [contact PaperThin](#) directly for installation support.

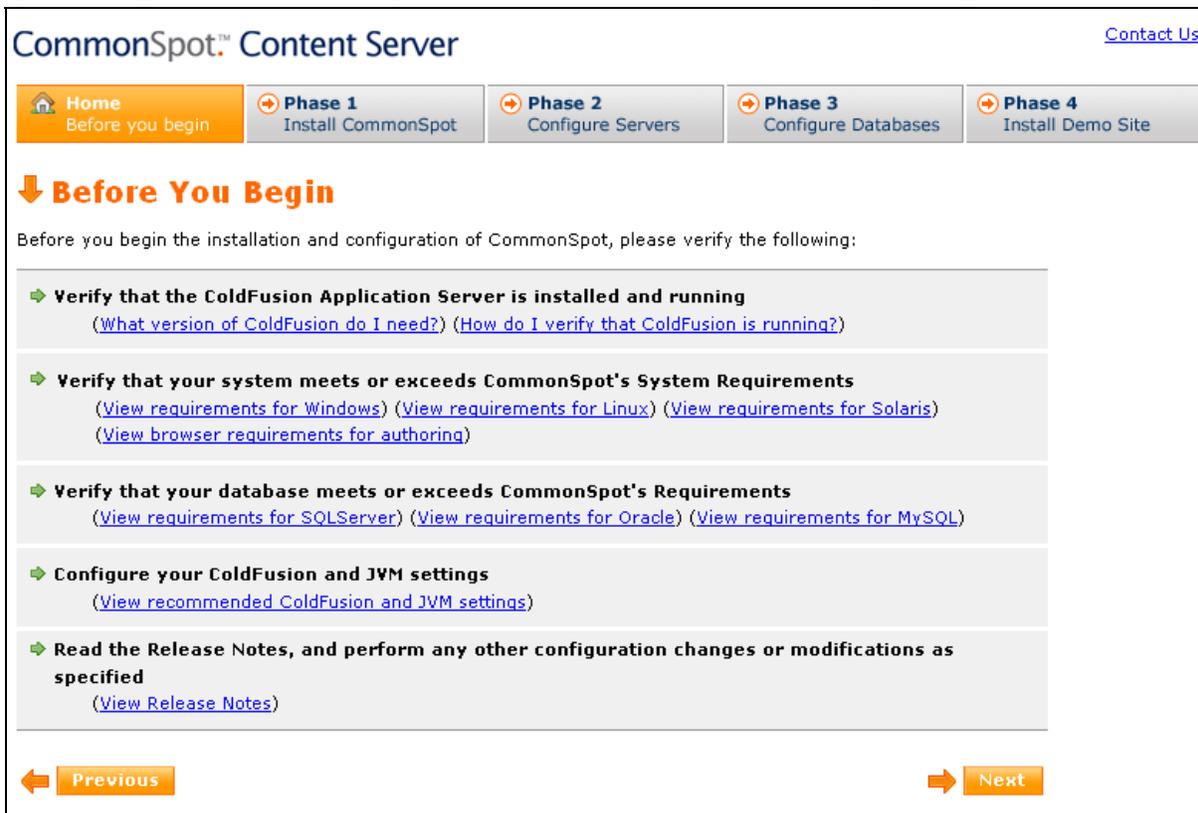
- **Phase 1. Install CommonSpot Modules and License Keys.** This phase will walk you through installing the CommonSpot modules and License Keys, as well as configuring the ColdFusion Application Server for use with Commonsport.
- **Phase 2. Configure the CommonSpot Server.** The second phase will walk you through the configuration of the CommonSpot Server.
- **Phase 3. Configure CommonSpot's Databases.** Next you will specify database and/or datasource information in order to create your CommonSpot databases.
- **Phase 4. Install Demo Site.** The last phases allows you to optionally install a copy of the CommonSpot demonstration site.

[Next](#)

Copyright © 1998-2012 PaperThin, Inc. All Rights Reserved.

3.2. The “Before You Begin” Page

The second window in the CommonSpot installation wizard reminds you to check that your system meets important requirements. The links provide additional details on how to verify the requirements.



3.3. Phase 1: Install CommonSpot

The first phase is the installation of CommonSpot itself. There are four steps to Phase 1 as described below. Instructions are specific to ColdFusion or Railo..

3.3.1. Phase 1: Install CommonSpot (Step 1 of 4)

In Step 1, simply enter the ColdFusion Administrator password under which CommonSpot will be running. CommonSpot needs this to configure the proper ColdFusion data sources and mappings. This password is not stored within CommonSpot.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin **Phase 1 Install CommonSpot** Phase 2 Configure Servers Phase 3 Configure Databases Phase 4 Install Demo Site

Phase 1: Install CommonSpot (Step 1 of 4)

At this point CommonSpot should have been copied to the appropriate location on your server, and ColdFusion minimally configured. Next please provide your ColdFusion administrator password so that the installation program can continue with the setup.

Please enter and verify the following:

- 1. ColdFusion Administrator Password:

.....

← Previous Next →

3.3.2. Phase 1: Install CommonSpot (Step 2 of 4)

Step 2 displays a table comparing your ColdFusion settings with CommonSpot's recommended settings. Those settings that differ are highlighted. Note that the installation will alter any of your settings if they do not meet the minimum requirements recommended for CommonSpot. Out-of-date settings may be automatically changed to the recommended setting when you click **Next**.

Note: The Timeout setting changes only if it is currently less than 300 seconds. CommonSpot does not change this if the current setting equals or exceeds the recommended setting

CommonSpot™ Content Server
[Contact Us](#)

Home
Before you begin

Phase 1
Install CommonSpot

Phase 2
Configure Servers

Phase 3
Configure Databases

Phase 4
Install Demo Site

Phase 1: Install CommonSpot (Step 2 of 4)

The following tables display the recommended and current values for various settings within the ColdFusion Administrator. Those settings that are out of sync with the recommended values are indicated with the icon. Note that the CommonSpot installation will modify these settings automatically if you click the 'Next' button.

ColdFusion Administrator Settings:

➤ **Server Settings > Settings Section:**

Setting Name	Recommended	Current
✔ Enable Whitespace Management	Checked	Checked
✔ Timeout requests after (seconds)	300	300

➤ **Server Settings > Caching Section:**

Setting Name	Recommended	Current
✔ Maximum number of cached templates	1000	1000
✔ Trusted cache	Unchecked	Unchecked
✔ Save Class Files	Unchecked	Unchecked

➤ **Server Settings > Memory Variables:**

Setting Name	Recommended	Current
✔ Enable Application Variables	Checked	Checked
✔ Enable Session Variables	Checked	Checked

← Previous
Next →

3.3.3. Phase 1: Install CommonSpot (Step 3 of 4)

In Step 3, you register your server and activate, download, and install your license keys. CommonSpot requires your servers to be registered with PaperThin. To register your server and download new keys, you will need to provide a Server Validation Code for the License Keys section of the PaperThin Support site. This is a one-time process for each server license you have. For information on how to download and install the CommonSpot License Keys, refer to [License Keys](#).

CommonSpot™ Content Server [Contact Us](#)

[Home](#) Before you begin **➔ Phase 1** Install CommonSpot ➔ Phase 2 Configure Servers ➔ Phase 3 Configure Databases ➔ Phase 4 Install Demo Site

Phase 1: Install CommonSpot (Step 3 of 4)

Register, Download and Install the CommonSpot License Keys:

- ➔ 1. Register this Server with PaperThin.com.**
The validation code for this server is: **2FJR5CIQC3A5BM25D3B29WG5E**
Navigate to <http://www.paperthin.com/support/downloads/license-keys.cfm>, login (if necessary) and locate the corresponding Server Key section on the page, and click the link that says, "Click here to activate the key". In the resulting dialog, copy and paste the key provide above into the 'Validation Code' field, and press the 'OK' button.
- ➔ 2. Download and Install the License Keys from PaperThin.com.**
Once the validation code has been accepted, download the appropriate License Keys for this server and extract the downloaded zip file into the '/commonspot/keys/' directory. If this directory does not exist, please create it now.

[← Previous](#) [Next →](#)

3.3.4. Phase 1: Install CommonSpot (Step 4 of 4)

Step 4 displays a list of the license keys found in your `/commonspot/keys` directory.

These license keys will be used for your installation of CommonSpot.

Additionally, if you are installing a server that will be part of a Shared Database cluster configuration, your license keys will prompt the display of an informational message for **Multi-Server Shared Database Configuration** with a checkmark beside it. If your license keys enable a replication configuration, the screen will display an informational message for **Multi-Server Replication Configuration** with a checkmark.

The screen below depicts an installation where the license keys are configured for a shared database configuration.

CommonSpot™ Content Server [Contact Us](#)

[Home](#) Before you begin | **Phase 1** Install CommonSpot | [Phase 2](#) Configure Servers | [Phase 3](#) Configure Databases | [Phase 4](#) Install Demo Site

Phase 1: Install CommonSpot (Step 4 of 4)

Finalizing Phase 1 of the Commonspot Installation

The following License Keys have been detected in the 'C:/workspaces/cs60/cs/web/commonspot/keys' directory:

- s-504983-w2k3-base.cfm
- c-504985-wk3-base.cfm
- c-505479-hostingcustomer_1.cfm
- c-505677-hostingcustomer_2.cfm
- c-506314-edu.cfm
- c-506320-500w2k3cf8-EDU.cfm

These license keys support the following configuration(s):

- ✓ **Multi-Server Shared Database Configuration**
This server can be configured as either the Master Authoring Server, a Read-Only Production Server, or as a Cache Server

Note: Under a Shared Database Configuration, you must copy the license keys to all Read-Only Production Servers and Cache Servers in the shared database cluster.

This concludes Phase 1 of the installation. Click 'Next' to continue to Phase 2.

[← Previous](#) [Next →](#)

Copyright © 1998-2011, PaperThin, Inc. All Rights Reserved.

3.4. Phase 2 – Configure Your Servers

Phase 2 of the installation wizard walks you through configuring your CommonSpot server or servers. There are eight steps in Phase 2 of the installation, as outlined below.

3.4.1. Phase 2: Configure Servers (Step 1 of 8) Dialog

The first screen in Phase 2 outlines steps required for running the CommonSpot Administrator to configure CommonSpot Server.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | Phase 1 Install CommonSpot | **Phase 2 Configure Servers** | Phase 3 Configure Databases | Phase 4 Install Demo Site

Phase 2: Configure Servers (Step 1 of 8)

CommonSpot is now minimally installed and configured.

The next phase is to run the CommonSpot Administrator to set initial passwords, configure the databases, and create your first CommonSpot site. You may access the CommonSpot Administrator at any time after the installation is complete by navigating to <http://qa-ins-master/commonsport/admin/index.cfm>.

The first time the CommonSpot Administrator is run, it gathers information about the configuration of the server and requires certain DataSources and ColdFusion settings to be enabled.

The following steps are performed the first time the Administrator is run:

1. The master 'admin-commonspot' user account and password is created.
2. General administration information about company and server is collected.
3. The root Web and Database directories are specified.
4. Other server configuration options are specified such as session duration, SMTP mail server, etc.

← Previous | Next →

If your license key enables you to install servers in a cluster configuration, the first screen of Phase 2 presents options for choosing the type of server to install:

- Authoring
- Read-Only Production
- Cache

Note: For instructions on installing a Read-Only Production server or a Cache Server in a shared database configuration, please refer to the *Shared Database Configuration Guide*.

3.4.2. Phase 2: Configure Servers (Step 2 of 8) Dialog

In Step 2, you will enter specifics for this CommonSpot server, such as the server name, its IP Address or alias, and date/time configuration settings.

Note: Your server name cannot contain any spaces, dashes, or underscores. CommonSpot returns an error for server names containing these special characters.

In most cases, only one customer key is needed per server. If, however, multiple customer keys are licensed, you will see a selection list of customer keys. Choose the appropriate Customer License key to use as the CommonSpot Administrator.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | Phase 1 Install CommonSpot | **Phase 2 Configure Servers** | Phase 3 Configure Databases | Phase 4 Install Demo Site

Phase 2: Configure Servers (Step 2 of 8)

Manage the server license keys, proxy settings and access to the ColdFusion Administrator.

Server and License Information

Server License: s-507467-mindfire-cluster.cfm

Customer License: c-507469-mindfire-cluster.cfm

* **Server Name:**
Specify the name of this server.

* **Server IP Address:** **Port:**
Specify the IP address (or alias) and port for this server.

Proxy Server Address:
Specify the Proxy Server address if applicable.

Proxy Server Port:
Specify the Proxy Server port if applicable.

[← Previous](#) [Next →](#)

3.4.3. Phase 2: Configure Servers (Step 3 of 8) Dialog

Step 3 creates an account for the server-level administrator. By default, this user has access to all administrative functions within CommonSpot, as well as all sites built on the CommonSpot Server. Enter and verify a password to use for the *admin-commonspot* account. Passwords must have a minimum of four characters.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin Phase 1 Install CommonSpot Phase 2 Configure Servers Phase 3 Configure Databases Phase 4 Install Demo Site

Phase 2: Configure Servers (Step 3 of 8)

In order to access the CommonSpot Administrator module, an administrator account needs to be created. The User ID for the account is **'admin-commonspot'**. Please specify a password for the account.

Administrator Account

* Password:
Specify the password for the account.

* Verify Password:
Verify the password by typing it again.

← Previous Next →

3.4.4. Phase 2: Configure Servers (Step 4 of 8) Dialog

In Step 4, you can choose whether you want to enable ColdFusion client variables, persistent cookies, or both.

Enabling client variables allows proper functioning of integrated applications that use ColdFusion client variables when they are executed from within a CommonSpot page. If you have already implemented, or intend to implement, applications that use client variables, you should check this box. Otherwise, you can leave this box unchecked.

If you enable persistent cookies, authenticated visitors to your CommonSpot site can maintain a CommonSpot session through browser open/close (within the session timeout period).

Note: Persistent cookies do not allow anyone with Contributor rights to maintain sessions. Contributors must always log in, regardless of settings for persistent cookies.

CommonSpot™ Content Server
[Contact Us](#)

[Home](#)
Before you begin

[Phase 1](#)
Install CommonSpot

[Phase 2](#)
Configure Servers

[Phase 3](#)
Configure Databases

[Phase 4](#)
Install Demo Site

Phase 2: Configure Servers (Step 4 of 8)

Enable ColdFusion Client variables & ColdFusion persistent Cookies for sites on this server.

Client Variables & Cookies

Enable client variables
 Client variables should only be enabled if they are in use within templates or Custom ColdFusion scripts. Client variables are not used by CommonSpot.

Enable persistent cookies
 Enable ColdFusion persistent cookies for sites on this server.

← Previous
Next →

3.4.5. Phase 2: Configure Servers (Step 5 of 8) Dialog

In Step 5, enter the paths that you have chosen for CommonSpot, your Web server documents, the parent directory for new sites, and your local data.

CommonSpot™ Content Server
[Contact Us](#)

[Home](#)
Before you begin

[Phase 1](#)
Install CommonSpot

[Phase 2](#)
Configure Servers

[Phase 3](#)
Configure Databases

[Phase 4](#)
Install Demo Site

Phase 2: Configure Servers (Step 5 of 8)

Specify CommonSpot directories. If content or data is moved on the server, these directories may need to be updated.

Directories

CommonSpot Directory: E:/commonsspot/

* **Web Server Document Directory:**

* **Parent Directory of New Sites:**

* **Local Data Directory:**
 Specify the directory where local CommonSpot data and server-specific configuration files will be stored.
Please note that for security reasons this directory should not be directly accessible via the HTTP Server.

← Previous
Next →

a.

Note: If the parent directory for new sites is not the same as the Web root directory, you may need to create Web server mappings for your site.

3.4.6. Phase 2: Configure Servers (Step 6 of 8) Dialog

In Step 6, enter the period of inactivity (in minutes) to allow before automatically logging users out of CommonSpot. Note that this number should be less than or equal to the maximum timeout value set in the ColdFusion Administrator. If the timeout value specified in CommonSpot is greater than the ColdFusion maximum value, the ColdFusion value applies.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | Phase 1 Install CommonSpot | **Phase 2 Configure Servers** | Phase 3 Configure Databases | Phase 4 Install Demo Site

Phase 2: Configure Servers (Step 6 of 8)

Manage CommonSpot's session timeout setting.

Session Timeout

Based on security settings, users may need to be authenticated in order to access certain pages. CommonSpot manages user login sessions on a per server basis. Please enter the following session parameters:

Session Timeout: minutes

Specify the number of minutes of inactivity before an authenticated user is logged out. Default: 60. Note that the maximum timeout for 'Session Variables' (set in the 'Variables' page of the ColdFusion Administrator) will take precedence if it is less than the value specified here.

[← Previous](#) [Next →](#)

3.4.7. Phase 2: Configure Servers (Step 7 of 8) Dialog

Your site can optionally use email to receive CommonSpot messages or to notify users of:

- Approval requests or refer-backs
- Content change notifications
- New account creation

To activate these options, enter the CommonSpot administrator's email address, the outgoing SMTP mail server, the SMTP connection port, and the timeout for SMTP connections. If your site routes email through a secure server, enable the encryption protocol you use.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | **Phase 1** Install CommonSpot | **Phase 2** Configure Servers | **Phase 3** Configure Databases | **Phase 4** Install Demo Site

Phase 2: Configure Servers (Step 7 of 8)

Manage settings for email notifications sent by CommonSpot

Email Notifications

When appropriate, CommonSpot sends e-mail notifications of certain actions. Please specify the administrator's email address and the SMTP mail server to use for these notifications.

Administrator's Email address:
Specify the email address of the CommonSpot administrator

Outgoing Mail Server:
Specify the SMTP mail server to be used for outgoing messages.

UserID:
Specify the UserID for the SMTP server.

Password:
Specify the corresponding password for the SMTP server.

Port:
Specify the port to be used for SMTP connections (default=25).

Timeout:
Specify the timeout (in seconds) for SMTP connections.

Use SSL:
Specify whether to use SSL for SMTP connections.

Use TLS:
Specify the whether to use TLS for SMTP connections.

[← Previous](#) [Next →](#)

For details on these settings, see “Email Notifications” in the *CommonSpot Administrator's Reference*.

3.4.8. Phase 2: Configure Servers (Step 8 of 8) Dialog

In Step 8, the installation wizard presents you with all of the information and configuration settings specified so far for your verification. If any are incorrect, click the **Previous** button until you get to the appropriate screen, then change the setting. Otherwise, click **Next** to continue to Phase 3 of the installation.

CommonSpot™ Content Server [Contact Us](#)

[Home](#) Before you begin | [Phase 1](#) Install CommonSpot | **[Phase 2](#) Configure Servers** | [Phase 3](#) Configure Databases | [Phase 4](#) Install Demo Site

Phase 2: Configure Servers (Step 8 of 8)

The following configuration options have been selected. Please verify these options before continuing.

Finalizing Phase 2 of the Commonspot Installation

- Server and License Information:**
 - Server License: s-508729-ptthin-automation.cfm
 - Customer License: c-508730-VM-automaiton.cfm
 - Server Name: offshoredev6
 - Server IP Address: offshoredev6
 - Port: 9085
 - Proxy Server Address:
 - Proxy Server Port:
 - Date/Time settings:
- Administrator account:**
 - Password: *****
- Client Variables & Cookies:**
 - Enable client variables: NO
 - Enable persistent cookies: YES
- Directories:**
 - CommonSpot Directory: C:/workspaces/cs-environments/cs/web/commonspot/
 - Web Server Document Directory: C:/workspaces/cs-environments/cs/web/
 - Parent Directory of New Sites: C:/workspaces/cs-environments/cs/web/
 - Local Data Directory: C:/commonspot-data/
- Session Timeout:**
 - Session Timeout: 60
- EMail Notifications:**
 - Administrator's Email address:
 - Outgoing Mail Server:
 - UserID:
 - Password:
 - Port: 25
 - Timeout: 5
 - Use SSL: NO
 - Use TLS: NO

This concludes Phase 2 of the installation. Click 'Next' to go to Phase 3.

[← Previous](#) [Next →](#)

3.5. Phase 3 – Configure Your Databases

Phase 3 walks you through creating data source connections for the databases used with CommonSpot. These requirements depend on your database type.

For Oracle installations, each data source requires a separate Oracle user on a compliant database instance (see [Requirements](#)). Each Oracle user must be granted at least 'Connect, Resource, and Create View' permissions, and have sufficient quota available in its default table space.

This installation process automatically creates the ColdFusion data sources for you.

3.5.1. Phase 3: Configure Databases (Step 1 of 5) Dialog

In Step 1 of Phase 3, confirm that you have met the database requirements for CommonSpot.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | Phase 1 Install CommonSpot | Phase 2 Configure Servers | **Phase 3 Configure Databases** | Phase 4 Install Demo Site

Phase 3: Configure Databases (Step 1 of 5)

The following outlines the minimum requirements for the supported databases (at the time this version of CommonSpot was released). If any of the databases fail the minimal requirements below you may not be able to use databases of this type. Please check the PaperThin Web site for the most up-to-date list of database requirements.

Confirm database requirements:

SQL Server:	Description	Requirement	You have
✓	Data Direct Driver Version	3.50 or greater	3.60
	SQL Server Database Version	2005	To be determined after datasource is configured

Oracle:	Description	Requirement	You have
✓	ColdFusion Product Level	Enterprise/Developer	Enterprise
✓	Data Direct Driver Version	3.50 or greater	3.60
	Oracle Database Version	10g (10.2.0.1 or greater)	To be determined after datasource is configured

MySQL:	Description	Requirement	You have
✓	Data Direct Driver Version	3.50 or greater	3.60
	MySQL Database Version	5.0 (5.0.25 or greater) Must use INNODB storage engine.	To be determined after datasource is configured

← Previous | Next →

If you are not going to use one or more of the database types listed, you can ignore any warnings that appear pertaining to them.

3.5.2. Phase 3: Configure Databases (Step 2 of 5) Dialog

In Step 2, choose the database type for each required database:

- **Sites** (please note that this name is *plural*). This is the database that stores information regarding all sites.
- **Users**. This is the database used to store user and group information.
- **Site** (please note that this name is *singular*). This is the default databases type for each site.

Important Note: CommonSpot does not back up databases. Backups are the database administrator's responsibility. In the event of failure, you cannot recover CommonSpot Web sites without a backup of the required databases.

CommonSpot™ Content Server [Contact Us](#)

[Home](#) Before you begin [Phase 1](#) Install CommonSpot [Phase 2](#) Configure Servers **[Phase 3](#) Configure Databases** [Phase 4](#) Install Demo Site

Phase 3: Configure Databases (Step 2 of 5)

A CommonSpot installation uses at least three (3) databases. The 'Sites' database manages the configuration of all of the sites created and managed on this server. The 'Users' database manages user profile and group information, and a separate 'Site' database is created to hold the content and permissions for each site.

Select the database types for the appropriate databases below:

Database Type for the 'Sites' database:	<input type="text" value="MySQL"/> Oracle SQLServer MySQL	Select the database type for the 'Sites' database.
Database Type for the 'Users' database:	<input type="text" value="MySQL"/> Oracle SQLServer MySQL	Select the database type for the 'Users' database.
Default database type for the new site database:	<input type="text" value="MySQL"/> Oracle SQLServer MySQL	Specify the default database type for any 'Content' database. Note that a 'Content' database is created for each site after this initial installation is complete.

[← Previous](#) [Next →](#)

3.5.3. Phase 3: Configure Databases (Step 3 of 5) Dialog

In Step 3, configure the required Sites database:

You must also supply a name, server, port, User ID, and password for the Sites database. Additional information may be required, depending on the database type.



Phase 3: Configure Databases (Step 3 of 5)

CommonSpot requires the creation of an empty SQL Server **Sites** database prior to initial configuration. During the configuration, CommonSpot will programmatically create all of the necessary tables and indexes. If you do not have a empty SQL Server Sites database, please create one now before proceeding.

Please enter the following information for the Sites database

* Database Name:	<input type="text" value="FreshInstall-sites"/>	Enter the SQL Server database name for the commonspot-sites data source
* Database Server:	<input type="text" value="db-mssql2005"/>	Enter the server name where the SQL Server database resides
* Database Port:	<input type="text" value="1433"/>	Enter the IP port for the SQL Server database connection
Database User ID and Password are REQUIRED:		
* Database User ID:	<input type="text" value="sa"/>	
* Database Password:	<input type="password" value="*****"/>	

← Previous

Next →

3.5.4. Phase 3: Configure Databases (Step 4 of 5) Dialog

Fields for Step 4 for the Users database are the same as fields in Step 3.

You must also supply a name, server, port, User ID, and password for the 'Users' database. Additional information may be required, depending on the database type.

CommonSpot™ Content Server [Contact Us](#)

[Home](#) Before you begin
 [Phase 1](#) Install CommonSpot
 [Phase 2](#) Configure Servers
 [Phase 3](#) Configure Databases
 [Phase 4](#) Install Demo Site

Phase 3: Configure Databases (Step 4 of 5)

CommonSpot requires the creation of an empty **SQL Server 'Users' database** prior to initial configuration. During the configuration, CommonSpot will programmatically create all of the necessary tables and indexes. If you do not have a empty SQL Server Users database, please create one now before proceeding.

Please enter the following information for the Users database

* **Database Name:**
 Enter the SQL Server database name for the commonspot-users data source

* **Database Server:**
 Enter the server name where the SQL Server database resides

* **Database Port:**
 Enter the IP port for the SQL Server database connection

Database User ID and Password are REQUIRED:

* **Database User ID:**

* **Database Password:**

[← Previous](#)
[Next →](#)

The following screen displays for successful completion.

3.5.5. Phase 3: Configure Databases (Step 5 of 5) Dialog

Step 5 prompts you to confirm the names, data sources, and database software versions of the Sites and Users databases.

CommonSpot™ Content Server

[Contact Us](#)

Phase 3: Configure Databases (Step 5 of 5)

Initial Database Configuration is complete.

The following databases have been successfully configured:

Database	Data Source Name	Database Name	Version
Sites	commonspot-sites	db-mssql2005//FreshInstall-sites	Microsoft SQL Server 2005
Users	commonspot-users	db-mssql2005//Freshinstall-users	Microsoft SQL Server 2005

This concludes Phase 3 of the installation.

At this point CommonSpot has been successfully installed. You may access the CommonSpot Administrator at any time by navigating to <http://sunyp/commonspot/admin>, or by pressing the 'Open Administrator' button below. To install a copy of the demo site click the 'Next' button.



3.6. Phase 4 – Install the Demo Site and ADF Demo

Phase 4 of the installation wizard gives you the option to install the CommonSpot University demonstration site and a demonstration version of the CommonSpot Application Development Framework for rapidly developing rich web applications in CommonSpot. The demo site is a working CommonSpot installation that implements many of CommonSpot's features. The CommonSpot documentation set includes a *Demo Site Guide* that outlines how the site was built and a map of all of its features. We recommend using this site, along with the *Demo Site Guide*, to learn how to work with CommonSpot.

You have the option of installing the demo site during this phase of the installation or finishing CommonSpot installation and installing the Demo site at a later date. The URL for the demo site installer is /commonspot/installation/install_demo.cfm.

For detailed instructions on installing the demonstration site, please refer to the Installation section of the *Demo Site Guide*.

A special sandboxed version of the ADF is installed as part of demo installation. This sandboxed version will not interfere with any ADF version you may have already installed.

Note: Before you install the demo site, make sure you have created the three empty databases (or database users for Oracle installations) required by the [Install Demo Site \(Step 2 of 3\) Dialog](#).

Refer to *Getting Started* and the *CommonSpot Demo Site Guide* for more information.

The screenshot shows the 'CommonSpot™ Content Server' installation wizard. At the top right is a 'Contact Us' link. Below it is a progress bar with five phases: 'Home Before you begin', 'Phase 1 Install CommonSpot', 'Phase 2 Configure Servers', 'Phase 3 Configure Databases', and 'Phase 4 Install Demo Site'. The 'Phase 4' button is highlighted in orange. Below the progress bar, the heading 'Phase 4: Install Demo Site' is displayed in orange. Underneath, the text reads: 'To install the demo site' followed by a grey box containing instructions: 'PaperThin provides a demonstration site to assist you in understanding CommonSpot. Installation of this demo site is optional. If you choose not to install the demo site at this time, you may do so later by navigating to "/commonspot/installation/install_demo.cfm". Please refer to the "Getting Started" and "CommonSpot Demo Site" documents, located in the /commonspot/docs directory, for more information about preparation for the Demo Site install.' At the bottom, there are 'Previous' and 'Next' buttons with arrows.

3.6.1. Install Demo Site (Step 1 of 3) Dialog

In Step 1, simply enter your ColdFusion Administrator password and select the type of database to use for the demo site.

CommonSpot™ Content Server [Contact Us](#)

Home Before you begin | Phase 1 Install CommonSpot | Phase 2 Configure Servers | Phase 3 Configure Databases | Phase 4 Install Demo Site

Install Demo Site (Step 1 of 3)

PaperThin provides a demonstration site to assist you in understanding CommonSpot. If you choose not to install the demo site at this time, you may do so later by navigating to `/commonspot/installation/install_demo.cfm`. Please refer to the "Getting Started" and "CommonSpot Demo Site" documents, located in the `/commonspot/docs` directory, for more information about preparation for the Demo Site install.

Please provide the following information

Database type for the new demo site databases:
 MySQL
 Oracle

[Next](#)

3.6.2. Install Demo Site (Step 2 of 3) Dialog

In Step 2, the wizard presents links for configuring data source connections to three required databases.

Note: You must first create three empty databases (or three database users for Oracle installations) for these data sources:

- **commonspot-demo** – The data source connecting to the Site (or Content) database. This database contains all of the data/content for the site.
- **commonspot-users-demo** – The data source connecting to the Users database. This database contains user and group information.
- **commonspot-demo-custom** – The data source connecting to a *custom*, non-Commonspot database used to demonstrate authentication against a third-party database.

CommonSpot™ Content Server [Contact Us](#)

Step 1 Installation Information | Step 2 Setup Data Sources | Step 3 Finalize Demo Site Installation

Install Demo Site (Step 2 of 3)

Please create three empty databases to configure the following data sources.

Data Sources Setup

Datasource Name	Type	Status
commonspot-demo	Content	✘ Configure
commonspot-users-demo	Users	✘ Configure
commonspot-demo-custom	External Data and Users	✘ Configure

[Previous](#) [Next](#)

When you click **Configure** next to each of the databases, the wizard presents you with the following dialog box.

Please provide the following information about the 'commonspot-demo' (MySQL) data source.

Data Source configuration - 'commonspot-demo'

* **Database Name:**
Enter the MySQL database name for the commonspot-demo data source

* **Database Server:**
Enter the IP address or host name of the server on which the database resides.

* **Port:**
Enter the port that is used to access the database server.

Database User ID and Password are REQUIRED:

* **Database Username:**

* **Database Password:**
Enter the database user ID and password for this data source. Please note that this username cannot be shared with any other CommonSpot data sources.

Once your databases are configured, the dialog refreshes and green check marks  replace red X marks in the **Status** column, as shown below.

CommonSpot™ Content Server [Contact Us](#)

[Home](#) Before you begin |
 [Phase 1](#) Install CommonSpot |
 [Phase 2](#) Configure Servers |
 [Phase 3](#) Configure Databases |
 [Phase 4](#) Install Demo Site

Install Demo Site (Step 2 of 3)

Please create three empty databases to configure the following data sources.

Data Sources Setup

Datasource Name	Type	Status	
commonspot-demo	Content		Configure
commonspot-users-demo	Users		Configure
commonspot-demo-custom	External Data and Users		Configure

[← Previous](#)
[Next →](#)

3.6.3. Install Demo Site (Step 3 of 3) Dialog

The dialog box in Step 3 first reports progress, as shown below, then confirms successful installation and provides a link to the home page of your new demo site.

The screenshot shows the 'CommonSpot™ Content Server' interface. At the top right is a 'Contact Us' link. Below it is a progress bar with five phases: 'Home Before you begin', 'Phase 1 Install CommonSpot', 'Phase 2 Configure Servers', 'Phase 3 Configure Databases', and 'Phase 4 Install Demo Site'. The 'Phase 4' button is highlighted in orange. The main heading is 'Install Demo Site (Step 3 of 3)'. Below this is the sub-heading 'Configuring Demo Site ...'. The main content area contains the text: 'Please wait while CommonSpot configures the demo site...' and 'This process may take a few minutes. Please be patient.'

This part of the process populates the databases created in the preceding steps with Demo site content.

The screenshot shows the 'CommonSpot™ Content Server' interface. At the top right is a 'Contact Us' link. Below it is a progress bar with five phases: 'Home Before you begin', 'Phase 1 Install CommonSpot', 'Phase 2 Configure Servers', 'Phase 3 Configure Databases', and 'Phase 4 Install Demo Site'. The 'Phase 4' button is highlighted in orange. The main heading is 'Install Demo Site (Step 3 of 3)'. Below this is the sub-heading 'Demo Site installed successfully'. The main content area contains the text: 'The Demo Site has been successfully installed.' followed by instructions: 'You must create a web server mapping for the demo site. Its path should be '/demo', and should point to C:/web/demo/. Once you have setup the '/demo' mapping, you can test it by clicking the button below.' Below this is a button labeled 'Test Site Web Server Mapping' with 'Status: Unknown' to its right. The next paragraph says: 'You must create a web server mapping for the demo site Application Development Framework (ADF). Please note that the demo site ADF is a version of the ADF specific for the demo site. It can not be used for other sites. If you are already running the ADF, this copy of the ADF will not conflict with the existing version.' Below this is another button labeled 'Test ADF Web Server Mapping' with 'Status: Unknown' to its right. The final instruction is: 'Once all mappings are configured, click 'Next' to go to the home page of the demo site.' At the bottom right is a 'Next' button with a right-pointing arrow.

Note: If the parent directory defined for new sites is not the same as the Web root directory, you may need to create Web server mappings for new sites, including the demo site and the ADF, before launching.

Click the **Test** buttons to check your mappings. The Install screen verifies mappings, as shown below.



The screenshot shows the 'CommonSpot™ Content Server' installation wizard. At the top right is a 'Contact Us' link. Below it is a progress bar with five steps: 'Home Before you begin', 'Phase 1 Install CommonSpot', 'Phase 2 Configure Servers', 'Phase 3 Configure Databases', and 'Phase 4 Install Demo Site'. The 'Phase 4' button is highlighted in orange. The main heading is 'Install Demo Site (Step 3 of 3)'. Below this, it says 'Demo Site installed successfully'. A message box states: 'The Demo Site has been successfully installed. You must create a web server mapping for the demo site. Its path should be '/demo', and should point to C:/web/demo/. Once you have setup the '/demo' mapping, you can test it by clicking the button below.' Below this message is a button labeled 'Test Site Web Server Mapping' with a status of 'OK'. Another message follows: 'You must create a web server mapping for the demo site Application Development Framework (ADF). Please note that the demo site ADF is a version of the ADF specific for the demo site. It can not be used for other sites. If you are already running the ADF, this copy of the ADF will not conflict with the existing version. Its path should be '/ADFdemo', and it should point to C:/web/ADFdemo/. Once you have setup the '/ADFdemo' mapping, you can test it by clicking the button below.' Below this is a button labeled 'Test ADF Web Server Mapping' with a status of 'OK'. At the bottom right, there is a 'Next' button with a right-pointing arrow.

If there are issues, testing reports the following.



The screenshot shows a button labeled 'Test ADF Web Server Mapping' with a status of 'Incorrect web server mapping'.

Check your configuration files, make corrections, and retest.

Chapter 4 License Keys

This chapter provides information on how to download and register your CommonSpot License keys.

4.1. Download and Install License Keys from PaperThin.com

New server and customer license keys are required whenever upgrading to a major or minor version of CommonSpot, or when installing on a new server. You can download license keys from:

<http://www.paperthin.com/support/downloads/license-keys.cfm>

Note: In a Shared Database Cluster environment, license keys on Read-Only Production Servers (ROPS) are exactly the same as the keys used on the Authoring Server. However, administrators must validate, on the PaperThin Web site, the same set of license keys for each server (once for the Authoring server and once for each ROPS or Cache server).

For both new installations and upgrades, the full product archive is required.

4.2. The Activate License Key Dialog

Once you have your validation code, you can activate and download the keys from the License Keys section of the PaperThin Support site: <http://www.paperthin.com/support/downloads/license-keys.cfm>:

1. Locate your server key on the Support License Keys page, then click **Click here to activate the key**. The **Activate License Key** Dialog appears.
2. Enter and save the validation code from the local server and click **OK**. On the key listing page, click the **Download** button so this set of keys can be downloaded and copied to your `/commonspot/keys` directory.

Note: Once you have entered and saved a validation code, you cannot change the code without help from PaperThin Support.

For servers in a Shared Database configuration, more than one Validation Code is allowed, and a Validation Code for each server in the Shared Database configuration is entered.

4.3. Changing Servers

The server key file is valid only for the server that generated the validation code. If the CommonSpot installation is transferred to a new server, the validation code is no longer valid and you will not be able to log in to CommonSpot until the proper validation code is placed in the key and re-downloaded to your server.

To migrate a server or to create an additional installation using the same server key, please contact PaperThin Support to deactivate the current validation code. Once the key is inactive, you can enter a new validation code and download new keys.

Chapter 5 Post-Installation Considerations

This chapter reviews important tasks and other items to consider after installing CommonSpot.

5.1. Back Up CommonSpot Databases

CommonSpot does not back up databases. Server administrators are responsible for backing up CommonSpot data. In the event of failure, you cannot recover CommonSpot Web sites without a backup of the required databases. Make sure you maintain a regular backup schedule for CommonSpot databases.

5.2. Create Scheduled Jobs

This release of CommonSpot includes a job manager for creating and managing all CommonSpot jobs from a single authoring server interface. Administrators at any level can create XML job definitions and run jobs at the server, customer, or site level. The Scheduled Job function takes care of all of the details of inserting jobs and managing changes in the ColdFusion Administrator.

You must explicitly enable and schedule jobs in order to run them. With the exception of the Heartbeat job for the CommonSpot Cache Server, described below, CommonSpot does not automate job creation or insertion.

Access this new functionality on an authoring server, from the Server, Site, or Customer Administration dashboards by expanding **Utilities** in the administrator left panel and selecting **Scheduled Jobs**.

CommonSpot includes the following jobs. For details, see “Scheduled Jobs” in the *CommonSpot Administrator’s Reference*.

Site Jobs

Rebuild Cache <i>(Non-Cache Server)</i>	Detects and updates changes to stored files.
Rebuild Cache <i>(Cache Server)</i>	Sites running CommonSpot Cache Servers in a Shared Database environment can use this utility to automatically update cache for all target servers in a cluster.
Rebuild Cache for Saved Search Results	Selectively rebuilds cache for the set of pages returned in a saved search. Used in combination with Site Performance Option 5 (no automatic cache rebuild) this job can help to minimize the performance impact of rebuilding all cache during heavy authoring use or other high-demand processing.
Send Broken Link Notifications	Examines system links to both internal pages and external URLs, determines if any are invalid, and reports status. Optionally emails content owners or authors when invalid links are detected.

Send Content Freshness Reminders	Monitors the content expiration date of pages, and sends an email reminder to users who request notification.
Generate Static Content	For sites licensed for Static Content Generation, this job detects and outputs static content to one or more target servers.
<i>Server Jobs</i>	
Rebuild Stale Cache	Detects and regenerates recently viewed expired content on target servers. Use this utility to find a balance between the performance benefits of temporarily serving expired content and the content freshness requirements of your site(s).
Check Replication	For sites licensed for CommonSpot Replication, detects whether real-time or scheduled replication is required.
Heartbeat	Continuously processes remote requests for this server. We recommend installing on all CommonSpot servers.

Administrators can also use the Scheduled Jobs interface to define jobs using any of the CommonSpot API “commands.” See the CommonSpot API component of online Help, or use the interactive versions linked from: <http://community.paperthin.com/articles/2010/07/30/About-the-CommonSpot-API.cfm>

5.3. For Shared Database Environments, “Unmap” the Read-Only Production Server(s)

After installation of a shared-database ROPS, the ROPS no longer needs read access to the authoring server (read access is required for installation only). Post-installation, remove this mapping from the ROPs.

5.4. Installation Issues

For the most up-to-date information on issues related to installing this release of CommonSpot, review Release Notes, and these PaperThin Support resources:

<http://www.paperthin.com/support/knowledgebase/>

<http://www.paperthin.com/support/downloads/>

5.5. CommonSpot Resources and Information

The following information will help your CommonSpot installation to run smoothly:

- **Review CommonSpot Documentation and Support Resources.** You will find a great deal of useful information in the CommonSpot online Help system and in documents available from the PaperThin Support site at <http://www.paperthin.com/support/>
- **Authoring Browser Settings.** For this release of CommonSpot, you should be aware of the following and related considerations:

- **Supported Browsers** – CommonSpot’s content management interface is entirely browser-based; there is no need to install or maintain client software. Pages are viewable from most standard browsers including Mozilla-based browsers and Microsoft Internet Explorer.

To author using CommonSpot, you must use one of the supported Web browsers. This release supports the Extended Support Release of Firefox 10 and Internet Explorer 9, as well as Chrome and Safari on the Mac. For details, review the Winter 2012 Release Notes and visit:

<http://www.paperthin.com/support/tech-specs.cfm>

- **Paste Operations** – CommonSpot supports full authoring capabilities from Windows, Mac, Linux, and Solaris computers. The authoring and approval functionality is nearly identical across the browsers. However, there are differences in the behavior when used with the WYSIWYG Rich Text Editor: For security reasons, both Mozilla-based browsers and Chrome disallow cut, copy, and paste operations unless you configure the browser to explicitly grant JavaScript-access to the Clipboard. PaperThin strongly recommends that you enable this functionality for contributors.

When using Chrome for authoring, the Rich Text Editor (RTE) cut-and-paste operations require PaperThin’s Chrome Extension. When not installed, CommonSpot automatically prompts users to download and install on first use. Clipboard functions become active after browser restart.

Mozilla requires a Clipboard helper to enable cut, copy, and paste. See:

<http://community.paperthin.com/articles/2010/03/15/firefox-paste-into-rte.cfm>

To avoid the interruption this may cause, contributors using either Chrome or Firefox should create a sample instance of cut-and-paste in the RTE to invoke the download in advance of using the clipboard for actual content creation.

Also note that because authoring in Safari restricts all cut-and-paste to right-click operations, RTE toolbar options for these functions and keyboard shortcuts are not available.

In addition, both Chrome and Safari require a third-party extension (like xml tree for Chrome) to correctly display XML. If you are using either of these browsers for authoring, download the appropriate extension to view XML for CommonSpot Elements.

For more information, review support information at mozilla.org and the Rich Text Editor sections of the *Administrator’s Reference* and the *Contributor’s Reference*.

- **Pop-up Blocking** – Most Web browsers include an option for preventing Web sites from programmatically opening new browser windows, to block unwanted pop-up windows. While such pop-up windows, particularly advertisements, have become a too-common annoyance, there are legitimate uses of pop-up windows.

CommonSpot uses pop-up windows for many contextual information and action dialogs. For example, while a CommonSpot page remains open in the main browser window, you can view and modify corresponding Page Properties in separate browser windows. Similarly, you can add content Elements to a page or edit them using dialogs that open in separate browser windows while the current version of the page remains visible in the main browser window. As you execute various functions in separate dialog windows, the view of the page in the main window is updated.

Pop-up windows greatly enhance multi-level action dialogs and are an essential design feature of CommonSpot.

Browsers that include pop-up blocking features also allow you to selectively disable pop-up blocking. Disabling pop-up blocking for a CommonSpot site will not affect the blocking of unwanted pop-up windows for other web sites. For CommonSpot to work properly, pop-up blocking must be disabled for contributors on each CommonSpot site.

To set pop-up blocking exceptions for CommonSpot, see Help for your Browser. You will typically find this option associated with Tools, Privacy, Security, or Internet Options.

5.5.1. Microsoft Office Considerations

To use Microsoft Word and PowerPoint elements, you must have the Microsoft applications installed. CommonSpot supports Office 2003 and 2007. The PowerPoint element does not function in 64-bit environments.

Chapter 6 Securing CommonSpot

This chapter addresses best practices for securing CommonSpot. CommonSpot provides configuration settings to increase security in the vital areas of SQL injection and direct calls to CommonSpot modules.

To best protect your CommonSpot environment, please review the following:

- [Securing HTTP Server Access](#)
- [Encrypting CommonSpot User Passwords](#)
- [SQL Injection Issues](#)
- [Controlling Access to CommonSpot Modules \(URL Tampering\)](#)

6.1. Securing HTTP Server Access

If it is not possible to restrict access to the entire /commonspot tree, you should restrict access to at least the following directories within the CommonSpot application directory, since they may contain sensitive data or be easily compromised.

Note: If you block access by restricting IP addresses, remember not to block the CommonSpot server itself because it needs access to perform automatic tasks, such as replication, static content generation, automatic cache serving, and indexing.

- /commonspot/installation *
- /commonspot/upgrade **
- /commonspot/demo ***
- /commonspot/bug-report/packets
- /commonspot/dbconvert
- /commonspot/docs
- /commonspot/logs
- /commonspot/keys
- /commonspot/newsite
- /commonspot/patches
- /commonspot/pubtools ****
- /commonspot/samples
- /commonspot/schema **
- /commonspot/security/access/custom
- /commonspot/static/background
- /commonspot/sync/packets

- /commonspot/sync/packets_created
 - /commonspot/sync/packets_received
 - /commonspot/sync/wddx
 - /commonspot-data
- * un-block for installation
- ** un-block for upgrades
- *** un-block if installing demo site
- **** un-block if running any of the CommonSpot Tools

To avoid direct manipulation of uploaded files intended to be secure, restrict web access to /_cs_upload in the Site directory and consider restricting web access to at least the following directories, which also reside in the Site folder:

- /_cs_apps
- /_cs_xmlpub
- /_cs_upload
- /customcf
- /datasheet-modules
- /renderhandlers
- /templates

6.2. Encrypting CommonSpot User Passwords

To make your CommonSpot installation more secure, you can encrypt the passwords for all of the users contained in the Users data source. To enable this feature, execute the **Set Password Encryption Module tool**, available by selecting **Server Tools** from the **Utilities** section of the Server Administration left panel. This utility sets the password encryption method for the server and encrypts all CommonSpot passwords stored on the server.

6.2.1. Encryption Module

You can use the default implementation (/commonspot/security/default-password-encrypt.cfm), or you can specify a custom-written module in the **Set Password Encryption Module** dialog. CommonSpot will pass the following variables to your encryption module:

- The given username: `Attributes.username`
- The given password: `Attributes.password`

Your custom algorithm module must declare the following variable:

- `caller.enc_password` - the password after your encryption algorithm has been applied

Once encryption is in place, new passwords entered via the CommonSpot Administrator will automatically be encrypted with this method. Passwords supplied by users requesting authentication will be encrypted and compared against the records in the database.

Note: For additional information regarding a custom encryption module, please visit the PaperThin Knowledgebase (<http://www.paperthin.com/support/knowledgebase>).

6.2.2. Special Notes on Encryption

Please carefully note the following restrictions before you proceed:

- This process cannot be undone without restoring database backups!
- This process cannot be reversed. No decryption algorithm is available for the encryption module provided.
- This process will affect ALL CommonSpot Users databases on this server.
- If this server participates in CommonSpot replication with any other servers, you must repeat this process on all servers before any subsequent replication. Failure to set identical password encryption methods for all related servers will result in login failures and password corruption on this and other related servers.
- If this server is the Authoring server in a shared-database cluster, this process will disable all login activity on all Read-Only Production Servers until the ColdFusion service is restarted on each server where encryption was applied..

6.3. SQL Injection Issues

A SQL injection attack typically involves a malicious user attempting to pass SQL code into an application that violates the original intent of the page. Microsoft SQL Server is most vulnerable, as ColdFusion allows the execution of multiple SQL statements using string-binding techniques in a single CFQUERY.

CommonSpot uses a two-pronged approach to eliminating potential SQL Injection errors. First, an internal security review was conducted on CommonSpot code and pages with potential issues were modified with strict input validation. Second, a configurable parsing mechanism added to CommonSpot allows administrators to turn on extra parsing logic contained in various entry point modules to detect and remove SQL injection threats.

To enable the extra parsing logic, follow the procedure described in [Configuring CommonSpot Security Access](#) below. Please note that enabling the parsing logic incurs a minor performance penalty on each request.

6.4. Controlling Access to CommonSpot Modules (URL Tampering)

If you do not adhere to proper security guidelines, an intruder might be able to directly access certain CommonSpot modules to add unwanted content or to delete, deface, or disable them. To prevent this type of intruder access, CommonSpot implements a global restriction mechanism that prohibits access to CommonSpot modules on the basis of user state (Anonymous, Authenticated, and/or Contributor). This facility prohibits direct calls to any unauthorized CommonSpot modules and ensures that all HTTP targets are valid. Pages accessed via the CommonSpot Loader are also verified.

6.4.1. Direct Requests

A “Direct Request” is an attempt to navigate from the browser to a module within the /commonspot directory. For instance, someone may type in the following URL:

```
http://www.paperthin.com/commonspot/about.cfm.
```

The Direct Request module in the example above is /commonspot/about.cfm.

By default, CommonSpot secures all of the necessary Direct Request modules within the /commonspot directory. CommonSpot requires that a number of files be available for direct access. The “unprotected” files have been secured through coding measures to ensure that URL tampering cannot cause a security leak.

6.4.2. Loader Requests

A “Loader Request” is an attempt to navigate to a module within the /commonspot directory using a Site/Subsite Loader. For instance, someone may type in the following URL:

```
http://www.paperthin.com/loader.cfm?csmodule=about
```

The Loader Request module in the above example is /commonspot/about.cfm.

CommonSpot is configured to protect all modules that should not be accessible through a Loader Call, but because a number of modules must be accessible via the Loader, internal coding measures have been implemented to prevent URL tampering.

6.4.3. Configuring CommonSpot Security Access

The internal security process handles each attempt to access files differently, depending on the authentication level of the user making the request (Anonymous, Authenticated, or Contributor). By default, CommonSpot will load required files into the Security Access process at start-up time. You can specify additional files to protect by modifying CommonSpot configuration files.

There are several files in the /commonspot/security/access/custom directory that control how security checks are performed (see below for the complete list of files and their intended use). With a standard CommonSpot installation, all of these files will have a prefix default_ (for example, default_.security-config.dat).

Note: PaperThin recommends that you copy the default.filename.dat file to filename.dat and modify it for your own purposes, instead of creating one “from scratch.” You can then maintain custom files without worrying about overwriting them during a product upgrade. The files and their purposes are listed below:

CommonSpot first looks for a filename *without* the default. prefix, then looks for one *with* a .dat extension.

Except for the security-config.dat file, all security configuration files are modified by placing modules into the file separated by a carriage return (one module specified per line). Module paths should be relative to the /commonspot root directory, and should not include the .cfm extension.

For example:

about

admin/index

The comments at the top of the configuration file can remain intact.

Note: Any changes to these files will not take effect until ColdFusion has been restarted.

Security-config.dat

This file is the main control file for the entire Security Access configuration. The file controls the ability to turn on and off these additional security checks, and also controls parsing and logging options based on the user's IP address or UserID. Below is a list of options available for this file:

- **LoaderCheckOn** (default=1 [on]) – When this setting is on, only registered modules can be called through the CommonSpot loader. See **loaderrequest.dat** to customize the list of registered modules.
- **DirectCheckOn** (default=1 [on]) – When this setting is on, only registered modules can be called directly. See 'default.directrequest.dat' to customize the list of registered modules.
- **ParseOn** (default=0 [off]) – When this setting is on, parameters passed to CommonSpot modules (specified in the *-parse.dat files below) are scanned for potential SQL injection threats.
- **TrustedIPList** (default=[none]) – IP addresses in this list are excluded from module security checks (wildcard * allowed). Syntax: Comma-delimited list of IP addresses with mask
- **TrustedUserIDList** (default=[none]) – User IDs in this list are excluded from module security checks. Syntax: Comma-delimited list of user IDs
- **NoParseIPList** (default=[none]) – Page input from IP addresses in this list is not parsed (wildcard * allowed) Syntax: Comma-delimited list of user IDs
- **NoParseUserIDList** (default=[none]) – Page input from User IDs in this list is not parsed
- **NoLogIPList** (default=[none]) – IP addresses in this list are excluded from the security exception log (wildcard * allowed) Syntax: Comma-delimited list of IP addresses with mask
- **NoLogUserIDList** (default=[none]) – Users IDs in this list are excluded from the security exception log

Loaderrequest.dat

This file contains modules that are available for execution via the loader.cfm file for **anonymous users**. These files will be called without any specific security check parsing.

Loaderrequest-parse.dat

This file contains modules that are available for execution via the loader.cfm file for **anonymous users**. These files will be parsed for SQL injection. When a file from this list is accessed, the query parameters will be parsed, which may produce a noticeable performance downgrade.

Loaderrequest-auth.dat

This configuration file contains a list of modules available for execution via the loader.cfm file. However, modules specified in this configuration file will verify that the user is “Authenticated” before executing. Unauthenticated users attempting to access a file from this list will be presented with a security exception dialog. Upon execution, these files will also have parsing performed to check for potential SQL Injection attacks.

Directrequest.dat

This file contains a list of CommonSpot modules that can be directly called from the URL. The modules listed in this file will be “blindly” allowed for execution. That is, there will be no security checks made against these modules.

Directrequest-parse.dat

This file contains a list of CommonSpot modules that can be directly called from the URL. These files will be parsed for SQL injection. When a file from this list is accessed the query parameters will be parsed, which may produce a noticeable performance downgrade.

Optional Modules

To enable the CommonSpot URL and Image field types for a simple form accessible by anonymous users, you need to add the following entries to the Loaderrequest.dat file:

CommonSpot URL

- /commonspot/controls/linkcommon/docgallery.cfm
- /commonspot/dhtmltree/body.cfm
- /commonspot/controls/linkcommon/docgallery-action.cfm

Image Element

- /commonspot/controls/imagecommon/image-summary.cfm
- /commonspot/controls/imagecommon/image-gallery-summary.cfm
- /commonspot/controls/imagecommon/image-gallery-display.cfm

Note: By enabling these three modules, you will allow anonymous users to list all pages and/or public images on your site.

6.4.4. CommonSpot Security Logging

When a request is made to an inaccessible page, a record is added to the security exception log in the CommonSpot logs directory. As for other CommonSpot log files, security exception file names include a time-date stamp prefix (for example, 20110101-security-exception.log) and contain the following structure:

```
Direct access to /{some-commonspot-module} was denied.  
USER: unavailable  
IP: 192.168.1.99  
DATE/TIME: Thu 01-Jan-2004 10:24:26  
Request Parameters (form):  
Request Parameters (url):
```

This log file is recycled each night like other CommonSpot log files.