CommonSpot™
Summer 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. Railo is a product of Railo Technologies GmbH, Bern, Switzerland.

This document was last updated September 18, 2012.
6.1. Securing HTTP Server Access ........................................................................................................48
6.2. Encrypting CommonSpot User Passwords .....................................................................................49
   6.2.1. Encryption Module .................................................................................................................50
   6.2.2. Special Notes on Encryption ...................................................................................................50
6.3. SQL Injection Issues .....................................................................................................................50
6.4. Controlling Access to CommonSpot Modules (URL Tampering)......................................................51
   6.4.1. Direct Requests ......................................................................................................................52
   6.4.2. Loader Requests ....................................................................................................................52
   6.4.3. Configuring CommonSpot Security Access ..............................................................................52
6.4.4. CommonSpot Security Logging ................................................................................................55
Chapter 1 About the Installation Guide

The CommonSpot Summer 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 Summer 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.

<table>
<thead>
<tr>
<th>I have verified that my ColdFusion Settings are correct</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have verified that my JVM Settings are correct</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>I have read the Release Notes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>My ColdFusion Administrator Password:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I know not to download my license keys until prompted to do so</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Directory to store license keys under:

I want to install an Authoring Server

I want to install a Read-Only Production Server (ROPS)

I want to install a Cache Server

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

I want to enable persistent cookies

CommonSpot Directory location:

Web Server Document Directory location:

Parent Directory of New Sites location:
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Data Directory location:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferred Image Library:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image Manipulation Directory location:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message timeout setting:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator's email address for CS email notifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outgoing mail server for CS email notifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email UserID for CS email notifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Password for CS email notifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Port For CS Email Notifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Timeout For CS Email Notifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The type of DB for my 'Sites' Database:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The type of DB for my 'Users' Database:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The type of DB for my new databases:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>‘Sites’ Data source will be CommonSpot-Configured</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>‘Sites’ Data source will be Manually Configured (not recommended)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>‘Sites’ DB Name:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>‘Sites’ DB Server:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 9.0.2 is supported on the Adobe Application Server only
   - ColdFusion 10 is only supported on the Application Server shipped with it.
   - Java 1.6 Update 33 for all ColdFusion versions
   
   Railo 3.3.4.003
   - Java SE 6 Update 24 or greater (excluding update 29) for Railo

   **Note:** ColdFusion 8.0.0,9.0.0, and 9.0.1 are not supported.

   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:

   **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. The zip file contains a /commonspot/ directory. Unzip the zip archive file into the target 
directory for CommonSpot. Be sure to preserve the directory structure when extracting 
the archive, and make sure ColdFusion or Railo is OFF first.

Extracted files are often unpacked with the ReadOnly attribute that needs to be cleared. In Windows 
right-click the commonspot folder, select Properties, and clear the read-only checkbox.

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-v80-ACF.zip

For Railo (Unix only):

    unzip cs-v80-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.

1. To manually change the file, locate the ColdFusion Application Server runtime folder for 
ColdFusion.

2. Navigate to the /bin folder.

3. Make a backup of the configuration file. For example, copy the jvm.config file, and save it to 
jvm-config-orig.bak (or another name). 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. Copy/paste operations may include 
characters that cause the ColdFusion startup to fail.
For ColdFusion 9, the path to the commonspot/java folder needs to be appended to the end of the ClassPath line. The list of class paths must be comma-delimited, not space comma-delimited.

For ColdFusion 10, the path to the commonspot/java folder needs to be added to the end of the server args line and not the class path line. Make sure to make a backup copy of the jvm.config before making any changes.

On Windows note that all file directory delimiters must expressed as ‘/’ and not ‘\’.

Save and close the file.

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

**To Configure Railo:**

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

In Web Administrator – Archives & Resources – Mappings, create a /commonspot/ mapping.
Configure Railo by extracting commonspot resources and the archive file and mapping the archive through the Railo Administrator.

Unpack the cs-v80-Railo.zip and save the /commonspot directory and the cs-v80.ras archive to the Railo server. In the example below, both commonspot and the archive are extracted to C:/cs-railo/.
From the Railo Web Administrator, manually set the /commonspot mapping to use the cs-v80.ras archive, and make sure that **Primary** is set to **Resource**, as shown below.

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.

Uncheck use time server.
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 Summer 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 /commonsport/installation/index.htm in a compatible browser (Firefox, Internet Explorer, Safari or Chrome). The first page in the CommonSpot installation wizard is a Welcome screen, explaining installation steps.
Welcome to the CommonSpot Summer 2012 installation.

CommonSpot is an award-winning, distributed Web publishing, content management and knowledge sharing application. 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 CommonSpot.

- **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 phase allows you to optionally install a copy of the CommonSpot demonstration site.
## 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.

### Before You Begin

Before you begin the installation and configuration of CommonSpot, please verify the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the ColdFusion Application Server is installed and running</td>
<td><img src="image" alt="What version of ColdFusion do I need?" /> <img src="image" alt="How do I verify that ColdFusion is running?" /></td>
</tr>
<tr>
<td>Verify that your system meets or exceeds CommonSpot’s System Requirements</td>
<td><img src="image" alt="View requirements for Windows" /> <img src="image" alt="View requirements for Linux" /> <img src="image" alt="View requirements for Solaris" /> <img src="image" alt="View browser requirements for authoring" /></td>
</tr>
<tr>
<td>Verify that your database meets or exceeds CommonSpot’s Requirements</td>
<td><img src="image" alt="View requirements for SQL Server" /> <img src="image" alt="View requirements for Oracle" /> <img src="image" alt="View requirements for MySQL" /></td>
</tr>
<tr>
<td>Configure your ColdFusion and JVM settings</td>
<td><img src="image" alt="View recommended ColdFusion and JVM settings" /></td>
</tr>
<tr>
<td>Read the Release Notes, and perform any other configuration changes or modifications as specified</td>
<td><img src="image" alt="View Release Notes" /></td>
</tr>
</tbody>
</table>
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.
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.

A shared database read only server uses the same keys as the authoring server, but has its own validation code. When installing a shared database server keys, the keys should be updated on all servers. Replication read only servers have separate keys for each server.

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.

<table>
<thead>
<tr>
<th>CommonSpot™ Content Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phase 1: Install CommonSpot (Step 2 of 4)</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**ColdFusion Administrator Settings:**

### Server Settings > Settings Section:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Recommended</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Enable Whitespace Management</td>
<td>Checked</td>
<td>Checked</td>
</tr>
<tr>
<td>✓ Timeout requests after (seconds)</td>
<td>300</td>
<td>300</td>
</tr>
</tbody>
</table>

### Server Settings > Caching Section:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Recommended</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Maximum number of cached templates</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>✓ Trusted cache</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td>✓ Save Class Files</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
</tbody>
</table>

### Server Settings > Memory Variables:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Recommended</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Enable Application Variables</td>
<td>Checked</td>
<td>Checked</td>
</tr>
<tr>
<td>✓ Enable Session Variables</td>
<td>Checked</td>
<td>Checked</td>
</tr>
</tbody>
</table>
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.

**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: 2FJR5C1QC3ASBM25D3B29WGSE
   
   Navigate to [http://www.paperthin.com/support/downloads/license-keys.htm](http://www.paperthin.com/support/downloads/license-keys.htm), 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 '/commonspotkeys' directory. If this directory does not exist, please create it now.
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.
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.

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.
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.

[Image of phase 2 configuration dialog]

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.
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.

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.
### 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:/commonspt/
- **Web Server Document Directory**: E:/web/clins
- **Parent Directory of New Sites**: E:/web/clins
- **Local Data Directory**: E:/commonspt-data/

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.
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.

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.

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.
**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-pthin-automation.cfm
  - Customer License: c-508730-pthin-automation.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/
  - 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.
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.

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Description</th>
<th>Requirement</th>
<th>You Have</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Direct Driver Version</td>
<td>3.50 or greater</td>
<td>3.60</td>
</tr>
<tr>
<td></td>
<td>SQL Server Database Version</td>
<td>2005</td>
<td>To be determined after datasource is configured</td>
</tr>
<tr>
<td>Oracle:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ColdFusion Product Level</td>
<td>Enterprise/Developer</td>
<td>Enterprise</td>
</tr>
<tr>
<td></td>
<td>Data Direct Driver Version</td>
<td>3.60 or greater</td>
<td>3.60</td>
</tr>
<tr>
<td></td>
<td>Oracle Database Version</td>
<td>10g (10.2.0.1 or greater)</td>
<td>To be determined after datasource is configured</td>
</tr>
<tr>
<td>MySQL:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Direct Driver Version</td>
<td>3.50 or greater</td>
<td>3.60</td>
</tr>
<tr>
<td></td>
<td>MySQL Database Version</td>
<td>5.6 (5.0.26 or greater)</td>
<td>To be determined after datasource is configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**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:**
  - Oracle
  - SQL Server
  - MySQL
  
  Select the database type for the ‘Sites’ database.

- **Database Type for the ‘Users’ database:**
  - Oracle
  - SQL Server
  - MySQL
  
  Select the database type for the ‘Users’ database.

- **Default database type for the new site database:**
  - Oracle
  - SQL Server
  - 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.
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.
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.

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

Initial Database Configuration is complete.

The following databases have been successfully configured:

<table>
<thead>
<tr>
<th>Database</th>
<th>Data Source Name</th>
<th>Database Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>commonspot-sites</td>
<td>db-mssql2005//Freshinstall-sites</td>
<td>Microsoft SQL Server 2005</td>
</tr>
<tr>
<td>Users</td>
<td>commonspot-users</td>
<td>db-mssql2005//Freshinstall-users</td>
<td>Microsoft SQL Server 2005</td>
</tr>
</tbody>
</table>

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://example.com/comonspot/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.
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.

![Install Demo Site (Step 1 of 3) Dialog](image)

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.

![Install Demo Site (Step 2 of 3) Dialog](image)
When you click **Configure** next to each of the databases, the wizard presents you with the following dialog box.

![Data Source configuration dialog box](image)

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

![Install Demo Site](image)
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.

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

Please wait while CommonSpot configures the demo site...

This process may take a few minutes. Please be patient.

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.

If there are issues, testing reports the following.

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 to new hardware, 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. Installing CommonSpot on an additional server requires a new key. Contact your account representative to purchase additional keys.

Call the Support line 617–471–4440 option 3
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.

<table>
<thead>
<tr>
<th>Site Jobs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebuild Cache</td>
</tr>
<tr>
<td>(Non-Cache Server)</td>
</tr>
<tr>
<td>Detects and updates changes to stored files.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site Jobs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebuild Cache</td>
</tr>
<tr>
<td>(Cache Server)</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site Jobs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebuild Cache</td>
</tr>
<tr>
<td>for Saved Search Results</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site Jobs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Broken Link Notifications</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Server Jobs</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>Send Content Freshness Reminders</td>
</tr>
<tr>
<td>Generate Static Content</td>
</tr>
<tr>
<td>Update Social Media Post Data</td>
</tr>
<tr>
<td>Analyze Performance</td>
</tr>
</tbody>
</table>

**Server Jobs**

<table>
<thead>
<tr>
<th>Server Job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebuild Stale Cache</td>
<td>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).</td>
</tr>
<tr>
<td>Check Replication</td>
<td>For sites licensed for CommonSpot Replication, detects whether real-time or scheduled replication is required.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>Continuously processes remote requests for this server. Installing on all CommonSpot servers is recommended.</td>
</tr>
</tbody>
</table>

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](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:
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/](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 Summer 2012 Release Notes and visit: [http://www.paperthin.com/support/tech-specs.cfm](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](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](http://mozilla.org) and the Rich Text Editor sections of the Site Administration 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. Note that 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
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.

- **TrustedIPLList** (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

- **NoParseIPLList** (default=[none]) – Page input from IP addresses in this list is not parsed (wildcard * allowed) Syntax: Comma–delimited list of IP addresses

- **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.