CommonSpot™ Release 10.0 Installation Guide

Paper | Thin

This document was last updated February 16, 2016.

Chapter 1 About the Installation Guide

The *CommonSpot 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/LuceeLucee applications and Web server configuration
- Access to the ColdFusion or LuceeLucee Administrator
- Access to the file system for CommonSpot installation
- The ability to create necessary databases

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

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/Lucee
- Database (SQL Server, Oracle or MySQL)
- Browser (Internet Explorer, Chrome, Safari or Firefox)
- JVM

If you are running CommonSpot on a virtual machine (VM), you must use a static MAC address.

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 (**Note:** All VMs must use a static MAC address):

Proxy Server Address:

Proxy Server Port:

Date/Time settings

Password for the CommonSpot Administrator Account:

I want to enable client variables (not recommended) 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

A Microsoft security enhancement 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 the Windows 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 Lucee is installed.**

   For the most up-to-date requirements see the Tech Specs on http://www.paperthin.com/support

   For this release CommonSpot supports:

   - ColdFusion 11
   - Coldfusion 10
   - Lucee 4.5
   - Latest Javascript Libraries
   - Java 8

For the latest platform requirements and resource and operating system details, see:

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

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 or Lucee 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 (DSR).

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. You will install CommonSpot at the root of your Web server or under an alias; for example, c:\inetpub\wwwroot\. 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 Lucee is OFF first.

Extracted files are often unpacked with a 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:

Install under the Web root directory or alias. For example, /var/apache/htdocs/. Copy the archive file into the target directory and extract it. Make sure ColdFusion or Lucee is OFF first.

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

For ColdFusion (Unix only):

```
unzip cs-v100-ACF.zip
```

For Lucee (Unix only):

```
unzip cs-v100-Lucee.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. IIS will need virtual directory for /commonspot; Apache will need an Alias for /commonspot.

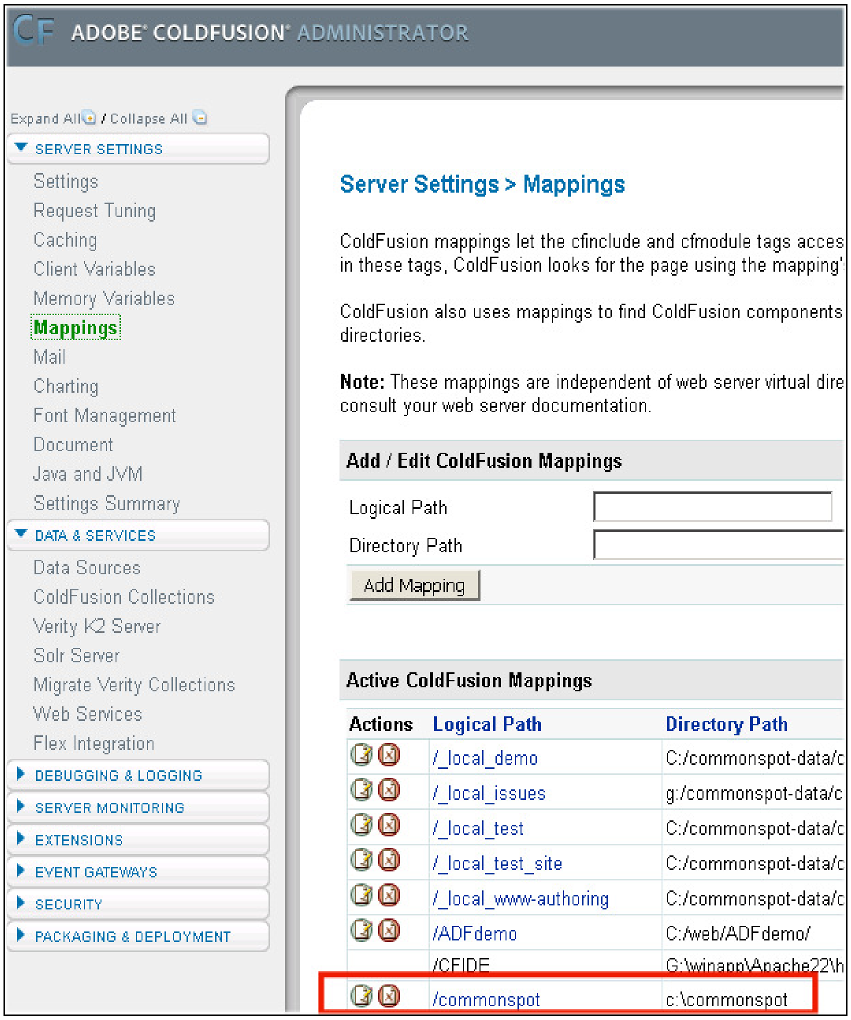
Also note that the Web server shipped with ColdFusion is not supported by PaperThin. This server is for development purposes and not intended for production.

6. **Configure ColdFusion or Lucee**

You also need to configure your ColdFusion Server to appropriately access CommonSpot.

To Configure ColdFusion:

1. Create a ColdFusion mapping to CommonSpot in the ColdFusion Administrator.



Server Settings > Mappings

ColdFusion mappings let the cfinclude and cfmodule tags acces in these tags, ColdFusion looks for the page using the mapping'

ColdFusion also uses mappings to find ColdFusion components directories.

Note: These mappings are independent of web server virtual dire consult your web server documentation.

Add / Edit ColdFusion Mappings

Logical Path

Directory Path

Add Mapping

Active ColdFusion Mappings

Actions	Logical Path	Directory Path
	/_local_demo	C:/commonspot-data/c
	/_local_issues	g:/commonspot-data/c
	/_local_test	C:/commonspot-data/c
	/_local_test_site	C:/commonspot-data/c
	/_local_www-authoring	C:/commonspot-data/c
	/ADFdemo	C:/web/ADFdemo/
	/CFIDE	G:\winapp\Apache22\h
	/commonspot	c:\commonspot

2. You also need to configure jvm access. You do this through the ColdFusion Admin interface or you can manually alter the jvm.config file. To manually change the file, locate the ColdFusion Application Server runtime folder for ColdFusion.

3. Navigate to the /bin folder.

4. 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

5. 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.

Note: Type this in, do not copy and paste this file. Copy/paste operations may include characters that cause the ColdFusion startup to fail.

- For ColdFusion, the path to the commonspot/java folder needs to be added to the end of the server args line as one of the classPath entries. The entries are comma delimited – not space comma. Make sure to make a backup copy of the jvm.config before making any changes. Modify java.args (Dcoldfusion.classPath=…)
- On Windows note that all file directory delimiters must be expressed as '/' and not '\'.

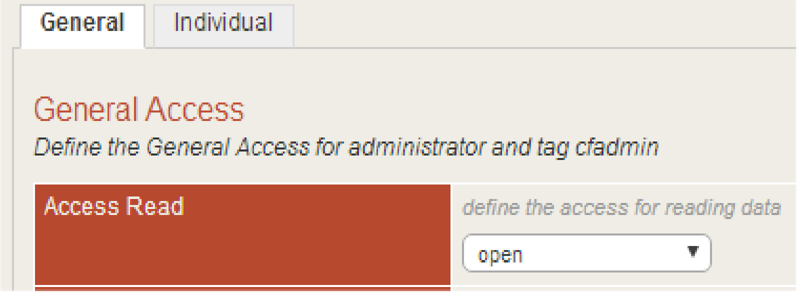
Check the following under **Security**. CommonSpot assumes a single admin signon. Check the first option.

6. 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 Lucee:

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



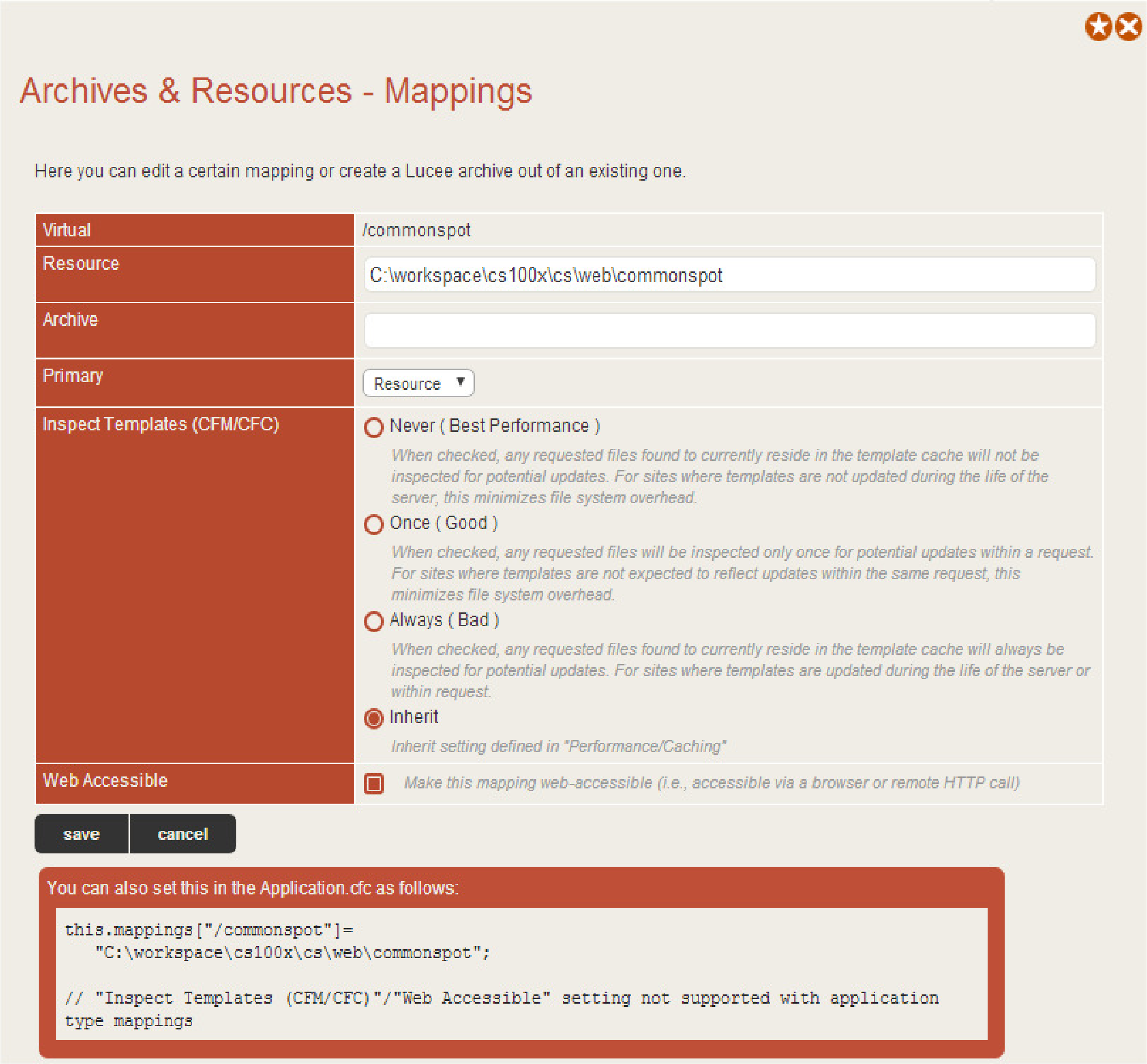
General Access

Define the General Access for administrator and tag cfadmin

Access Read: open

define the access for reading data

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



Archives & Resources - Mappings

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

Virtual	/commonspot
Resource	C:\workspace\cs100x\cs\web\commonspot
Archive	
Primary	Resource ▼
Inspect Templates (CFM/CFC)	○ 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.* ○ Once (Good) *When checked, any requested files will be inspected only once for potential updates within a request. For sites where templates are not expected to reflect updates within the same request, this minimizes file system overhead.* ○ 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.* ● Inherit *Inherit setting defined in "Performance/Caching"*
Web Accessible	□ *Make this mapping web-accessible (i.e., accessible via a browser or remote HTTP call)*

You can also set this in the Application.cfc as follows:

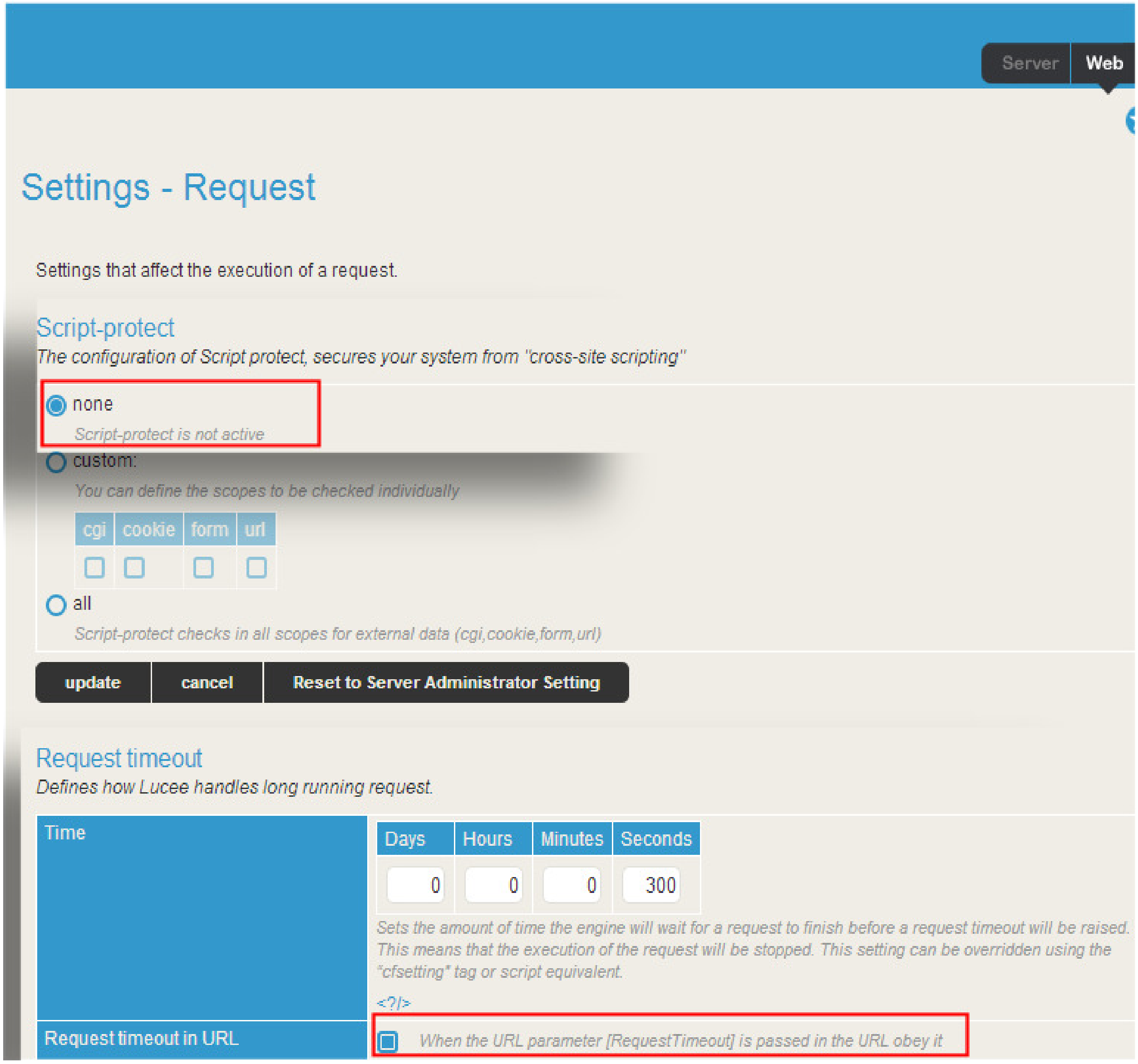
```
this.mappings["/commonspot"]=
   "C:\workspace\cs100x\cs\web\commonspot";

// "Inspect Templates (CFM/CFC)"/"Web Accessible" setting not supported with application
type mappings
```

Configure Lucee by extracting commonspot resources and the archive file and mapping the archive through the Lucee Administrator.

Unpack the cs-v100-Lucee.zip and save the /commonspot directory and the cs-v100.ras archive to the Lucee server. In the example below, both commonspot and the archive are extracted to C:/cs-Lucee/.

From the Lucee Web Administrator, manually set the /commonspot mapping to use the cs-v100.ras archive, and make sure that **Primary** is set to **Resource**.
In addition:

- Lucee Web Administrator – Settings – Request: Script-protect must be set to **none.**
- Lucee Web Administrator – Settings – Request: Request timeout in URL must be true.



Settings - Request

Settings that affect the execution of a request.

Script-protect

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

● none

Script-protect is not active

○ custom:

You can define the scopes to be checked individually

cgi	cookie	form	url
□	□	□	□

○ all

Script-protect checks in all scopes for external data (cgi,cookie,form,url)

Request timeout

Defines how Lucee handles long running request.

Time

Days	Hours	Minutes	Seconds
0	0	0	300

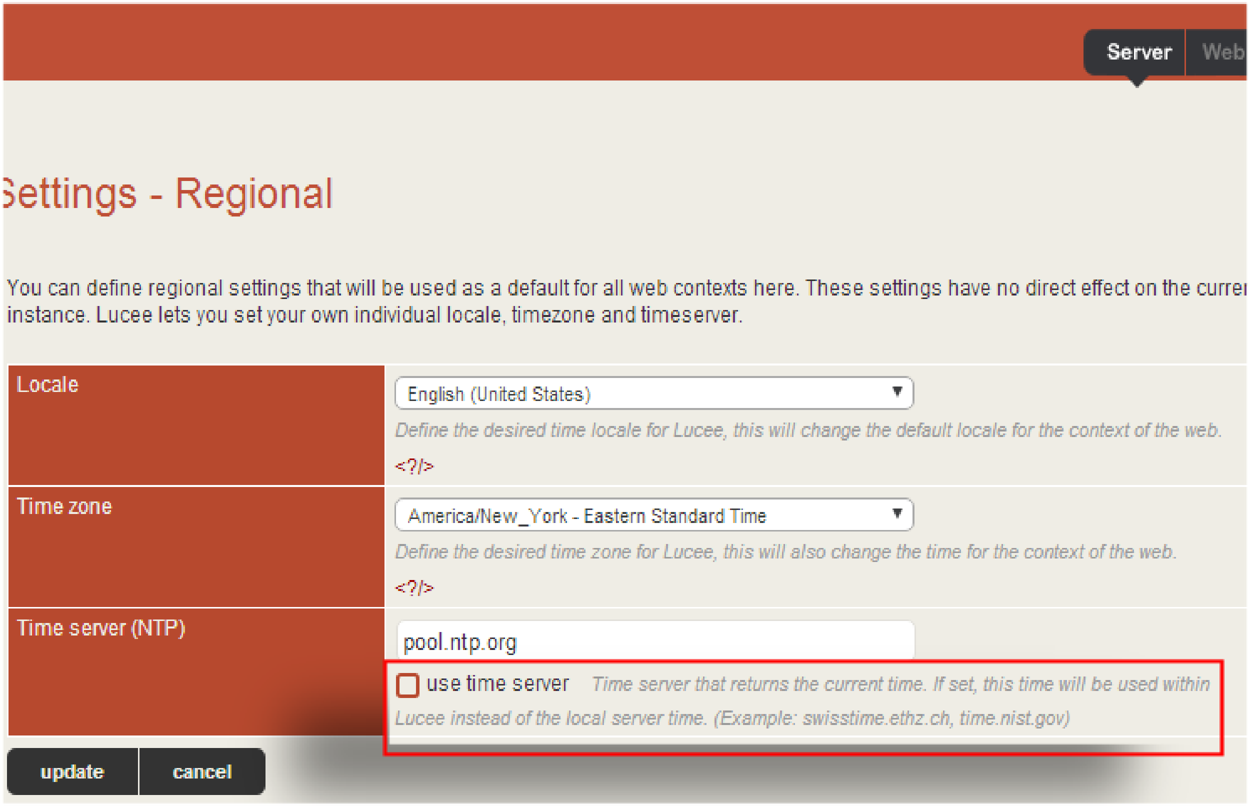
Sets the amount of time the engine will wait for a request to finish before a request timeout will be raised. This means that the execution of the request will be stopped. This setting can be overridden using the "cfsetting" tag or script equivalent.

<?/>

Request timeout in URL

□ *When the URL parameter [RequestTimeout] is passed in the URL obey it*

Uncheck **use time server.**



ettings - Regional

You can define regional settings that will be used as a default for all web contexts here. These settings have no direct effect on the curre
instance. Lucee lets you set your own individual locale, timezone and timeserver.

Locale	English (United States) ▼ *Define the desired time locale for Lucee, this will change the default locale for the context of the web.* <?/>
Time zone	America/New_York - Eastern Standard Time ▼ *Define the desired time zone for Lucee, this will also change the time for the context of the web.* <?/>
Time server (NTP)	pool.ntp.org □ use time server *Time server that returns the current time. If set, this time will be used within Lucee instead of the local server time. (Example: swisstime.ethz.ch, time.nist.gov)*

In the directory: [Lucee install]\tomcat\conf\catalina.properties

Add: path to

…/commonspot/java/*.jar from root of drive to the “common.loader=” line

Must be forward slashes

7. Decide which database type to use for your CommonSpot installation. Create three empty UTF-8 databases for this initial installation.

    1. Microsoft SQL Server

    2. MySQL. - see CommonSpot configuration requirements at http://www.paperthincom/support/knowledgebase/articles/Supported-MySQL-Versions.cfm

    3. Oracle

8. **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 10 Shared Database Configuration Guide*.

9. **Restart the Lucee or ColdFusion service 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*.

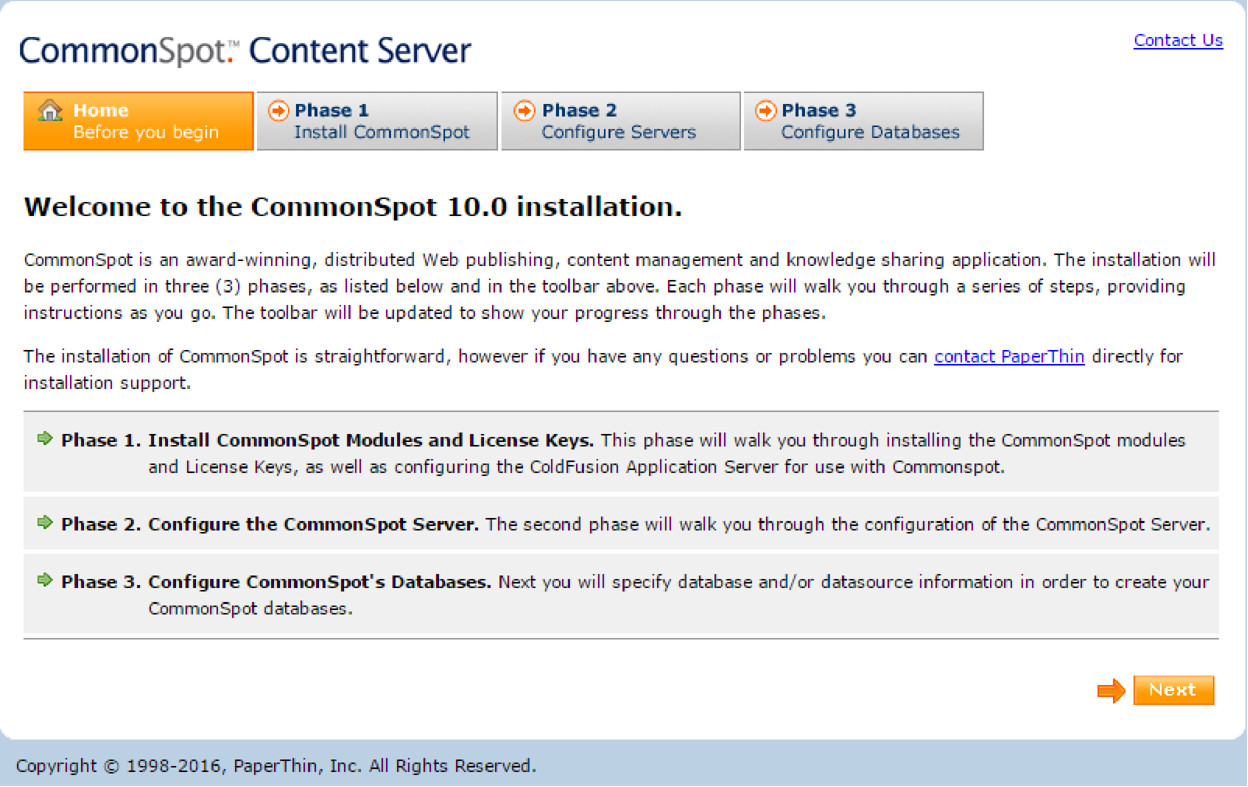
Before beginning the CommonSpot installation, please read the Pre-Installation Requirements and Considerations and complete all the steps outlined there.

The CommonSpot installation consists of The Welcome Page, The "Before You Begin" Page, and the following three phases:

- Phase 1: Install CommonSpot
- Phase 2 - Configure Your Servers
- Phase 3 - Configure Your Databases

3.1. The Welcome Page

Open **/commonspot/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 10.0 installation.

CommonSpot is an award-winning, distributed Web publishing, content management and knowledge sharing application. The installation will be performed in three (3) 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.

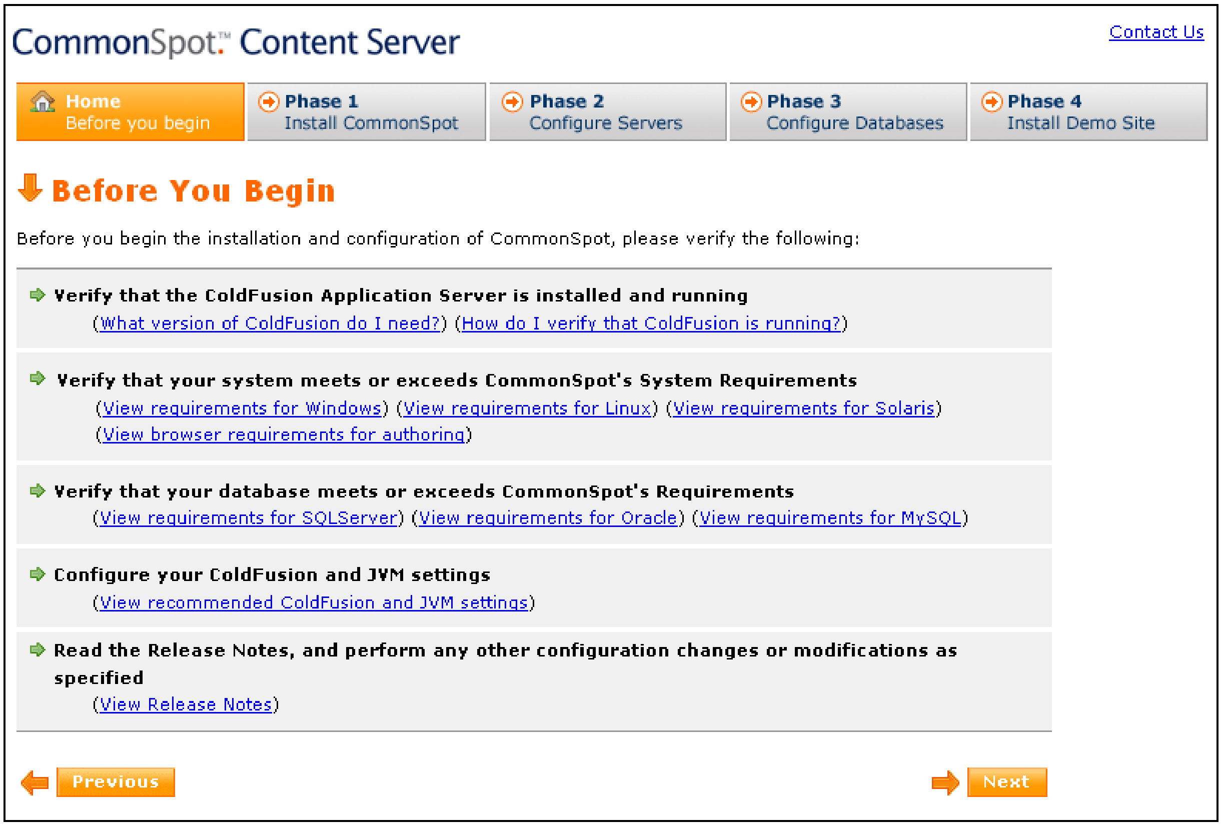
Phase 2. Configure the CommonSpot Server. The second phase will walk you through the configuration of the CommonSpot Server.

Phase 3. Configure CommonSpot's Databases. Next you will specify database and/or datasource information in order to create your CommonSpot databases.

Copyright © 1998-2016, 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.



Before You Begin

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

Verify that the ColdFusion Application Server is installed and running
(What version of ColdFusion do I need?) (How do I verify that ColdFusion is running?)

Verify that your system meets or exceeds CommonSpot's System Requirements
(View requirements for Windows) (View requirements for Linux) (View requirements for Solaris)
(View browser requirements for authoring)

Verify that your database meets or exceeds CommonSpot's Requirements
(View requirements for SQLServer) (View requirements for Oracle) (View requirements for MySQL)

Configure your ColdFusion and JVM settings
(View recommended ColdFusion and JVM settings)

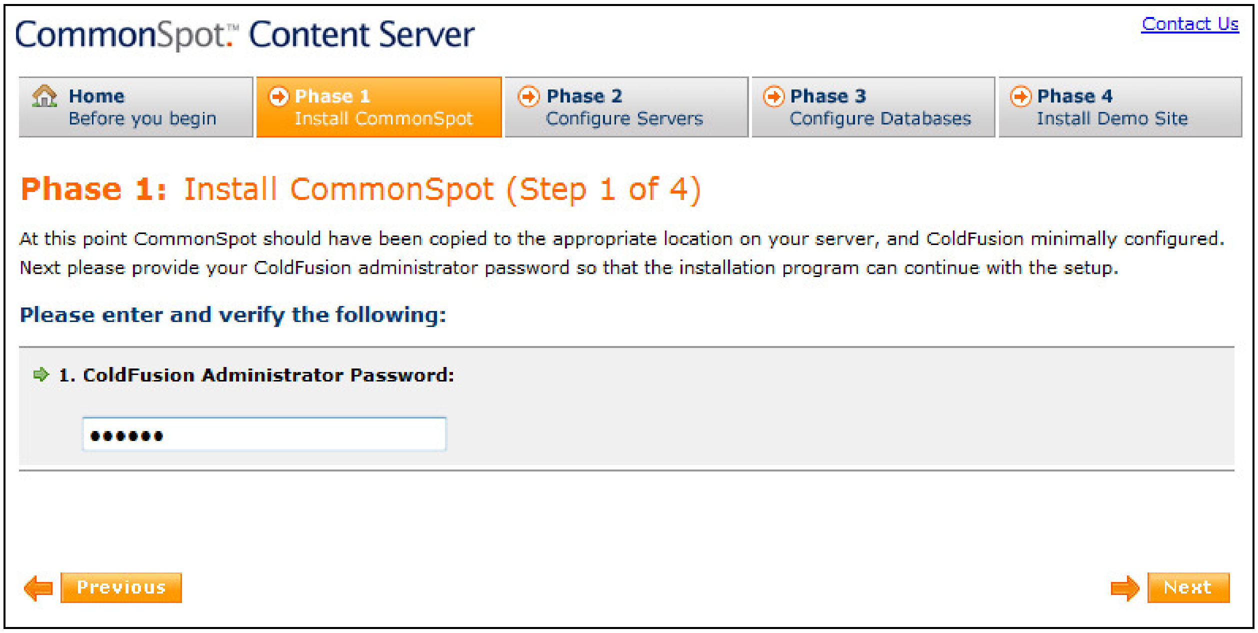
Read the Release Notes, and perform any other configuration changes or modifications as specified
(View Release Notes)

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 Lucee..

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

In Step 1, simply enter the ColdFusion or Lucee Administrator password under which CommonSpot will be running. CommonSpot needs this to configure the proper 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
Previous
Next

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:

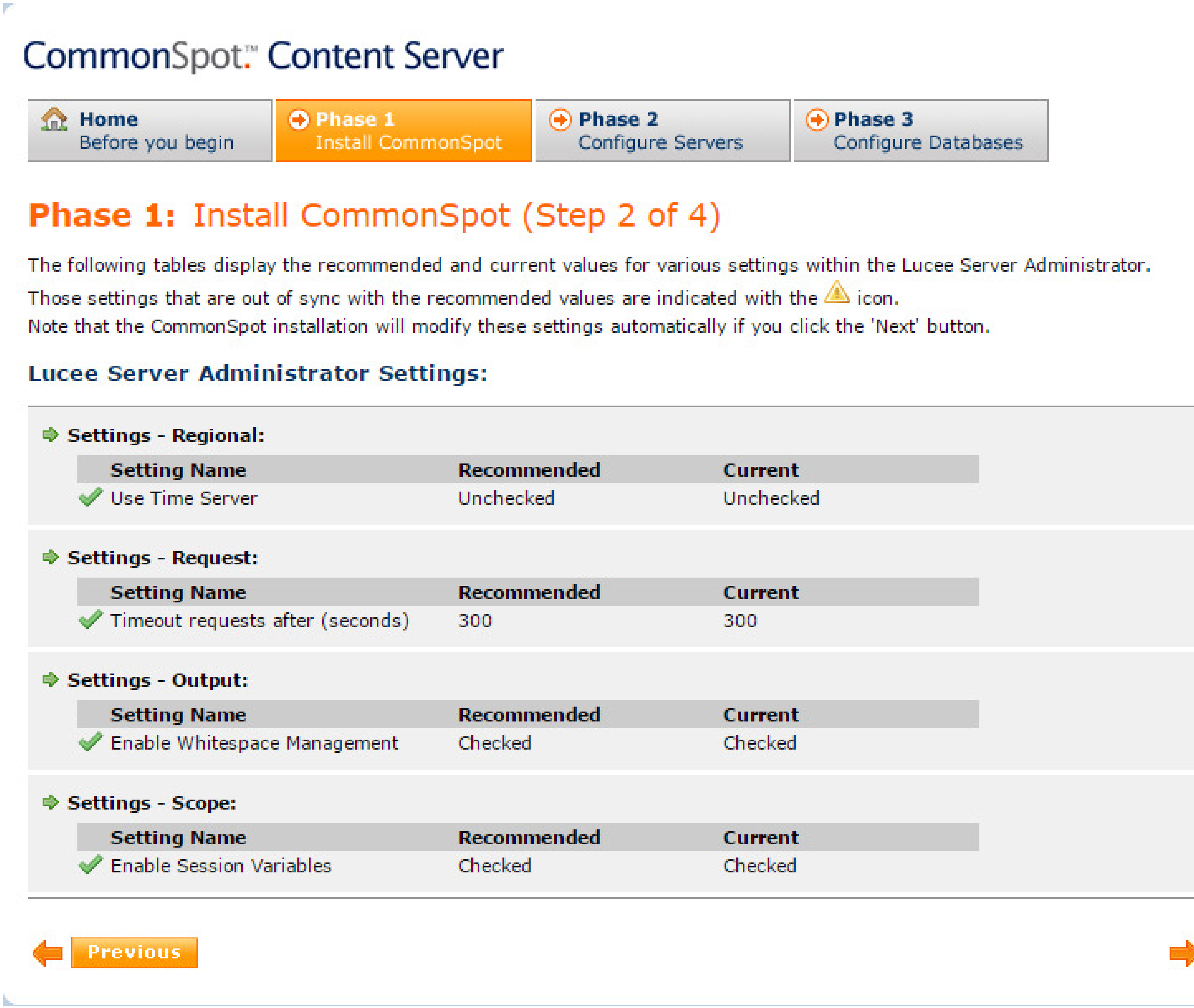
1. ColdFusion Administrator Password: ••••••

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 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



Phase 1: Install CommonSpot (Step 2 of 4)

The following tables display the recommended and current values for various settings within the Lucee Server 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.

Lucee Server Administrator Settings:

Settings - Regional:

	Setting Name	Recommended	Current
✓	Use Time Server	Unchecked	Unchecked

Settings - Request:

	Setting Name	Recommended	Current
✓	Timeout requests after (seconds)	300	300

Settings - Output:

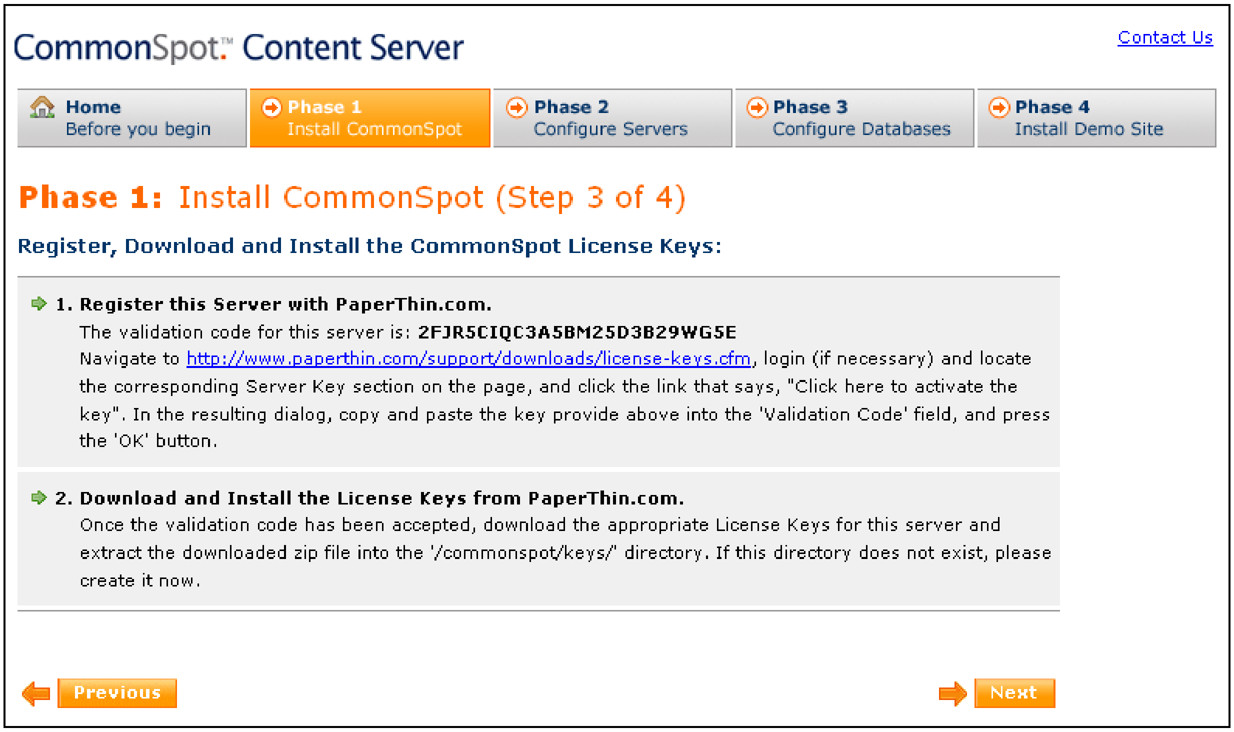
	Setting Name	Recommended	Current
✓	Enable Whitespace Management	Checked	Checked

Settings - Scope:

	Setting Name	Recommended	Current
✓	Enable Session Variables	Checked	Checked

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.



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.

3.3.4. Download and Install License Keys from PaperThin.com

New server and customer license keys are required when installing on a new server or when upgrading to a major or minor version of CommonSpot. 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.

3.3.5. 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.

3.3.6. 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.

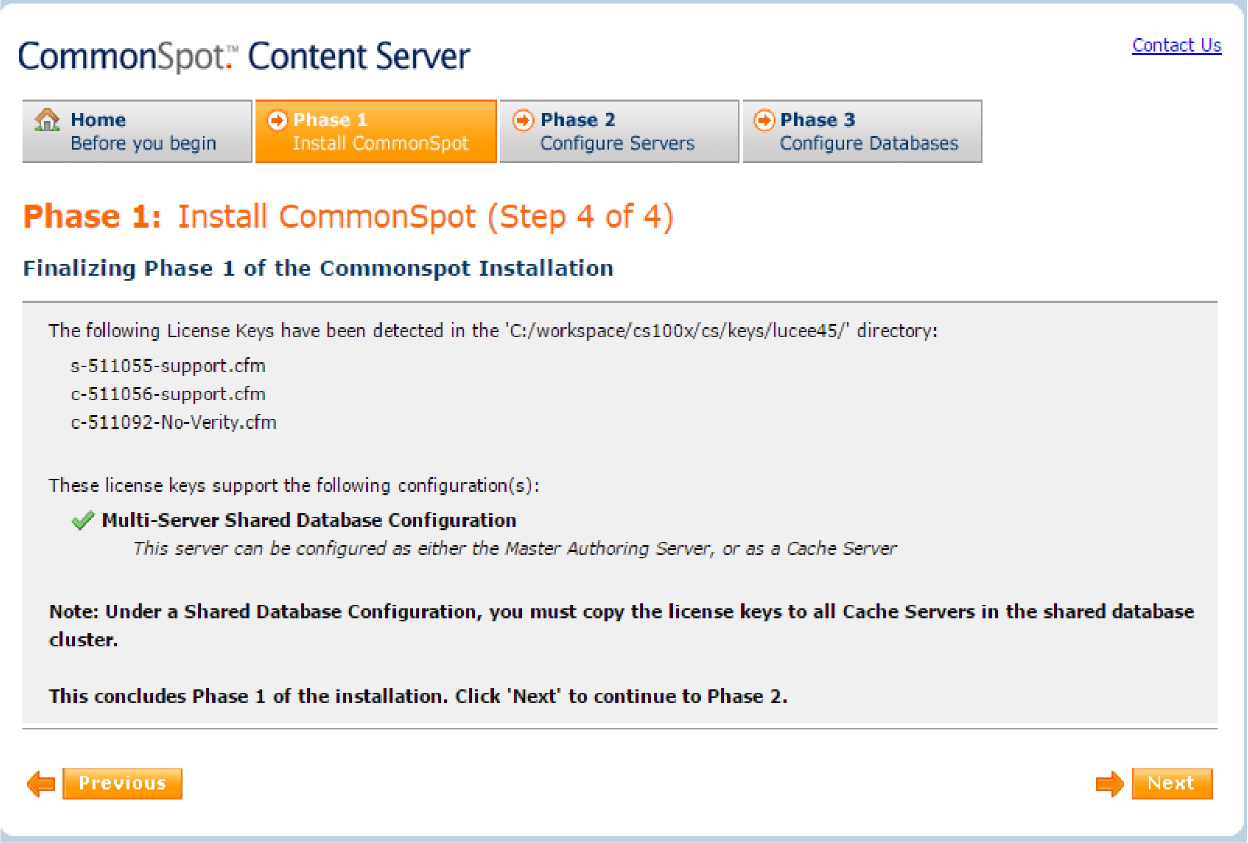
3.3.7. Phase 1: Install CommonSpot (Step 4 of 4)

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
Previous
Next

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:/workspace/cs100x/cs/keys/lucee45/' directory:

s-511055-support.cfm
c-511056-support.cfm
c-511092-No-Verity.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, or as a Cache Server

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

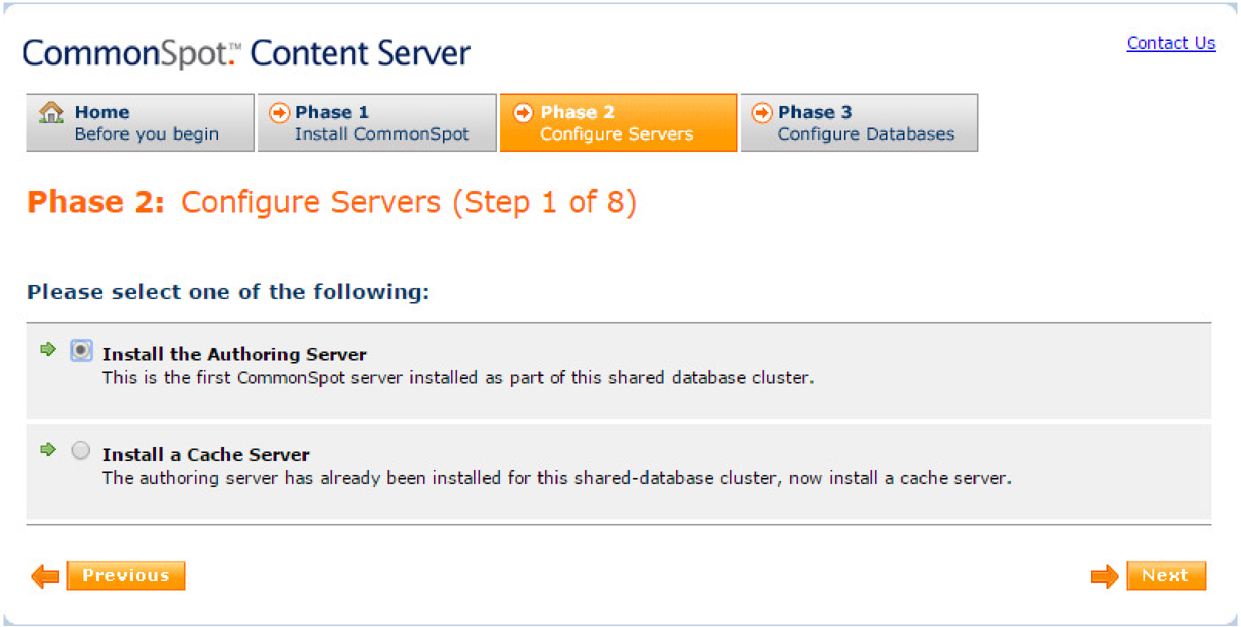
This concludes Phase 1 of the installation. Click 'Next' to continue to Phase 2.

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
Previous
Next

Phase 2: Configure Servers (Step 1 of 8)

Please select one of the following:

● **Install the Authoring Server**
This is the first CommonSpot server installed as part of this shared database cluster.

○ **Install a Cache Server**
The authoring server has already been installed for this shared-database cluster, now install a cache 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

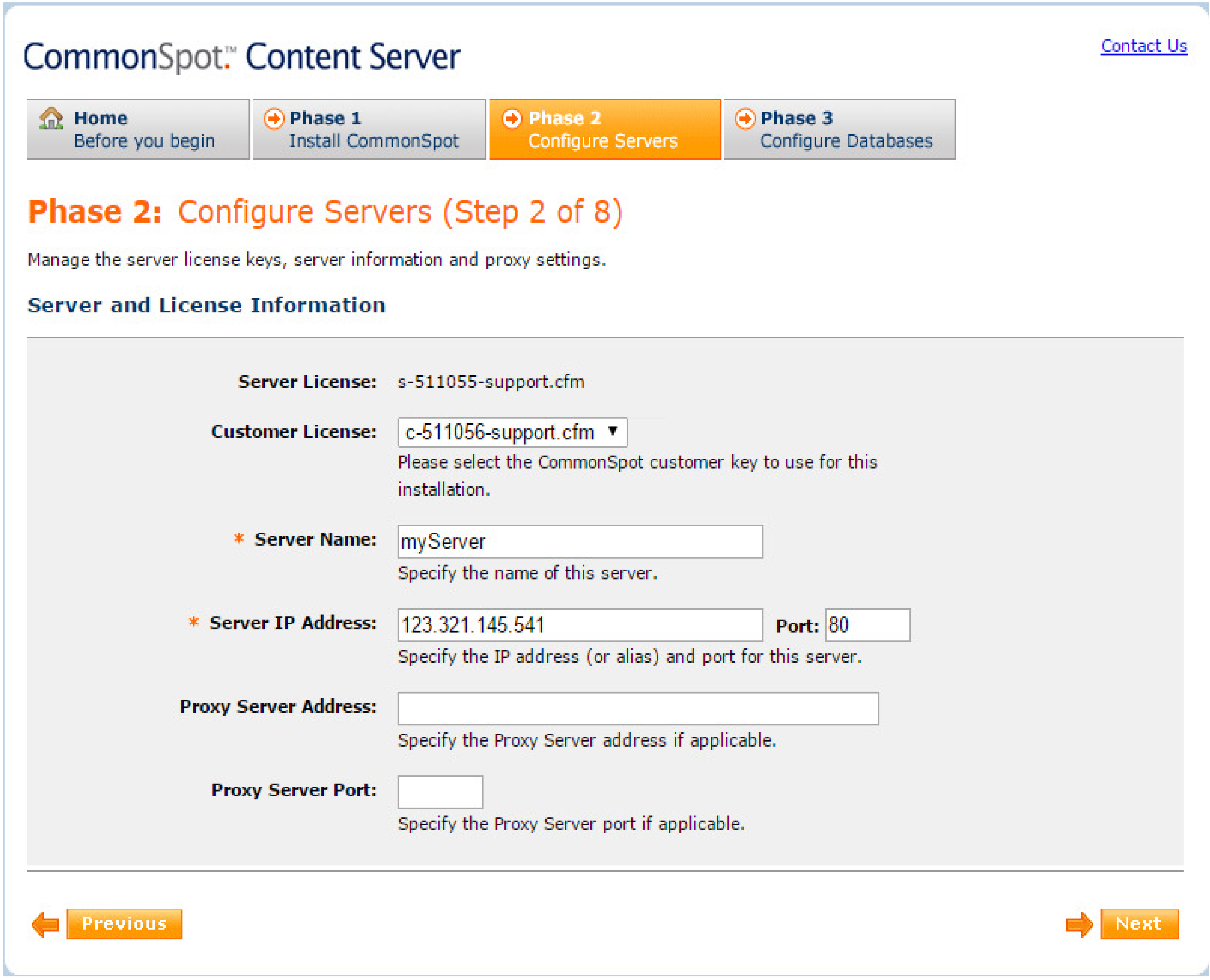
Note: For instructions on installing a Read-Only Production server or a Cache Server in a shared database configuration, please refer to the *Shared Database Configuration Guide*.

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 (recommended), 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
Previous
Next

Phase 2: Configure Servers (Step 2 of 8)

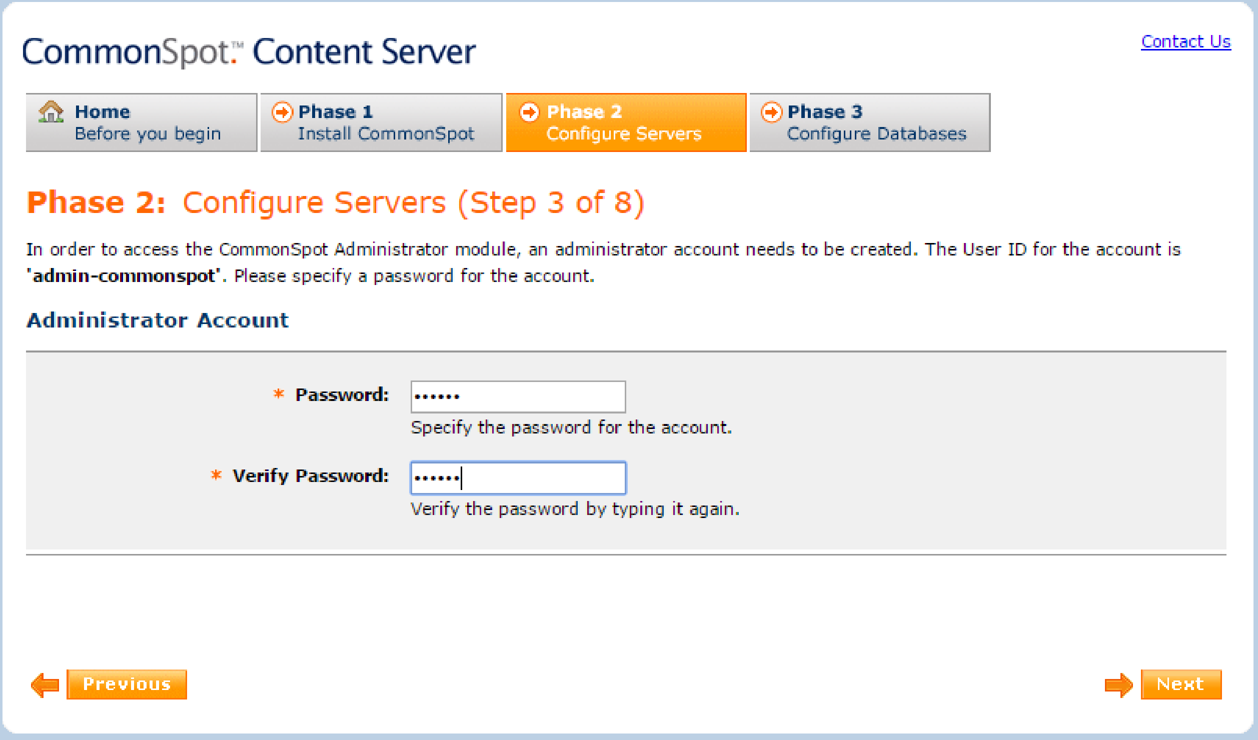
Manage the server license keys, server information and proxy settings.

Server and License Information

Server License:	s-511055-support.cfm
Customer License:	c-511056-support.cfm ▼ Please select the CommonSpot customer key to use for this installation.
* Server Name:	myServer Specify the name of this server.
* Server IP Address:	123.321.145.541 Port: 80 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.

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 same customer key. Enter and verify a password to use for the *admin-commonspot* account. Passwords must have a minimum of four characters.



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.

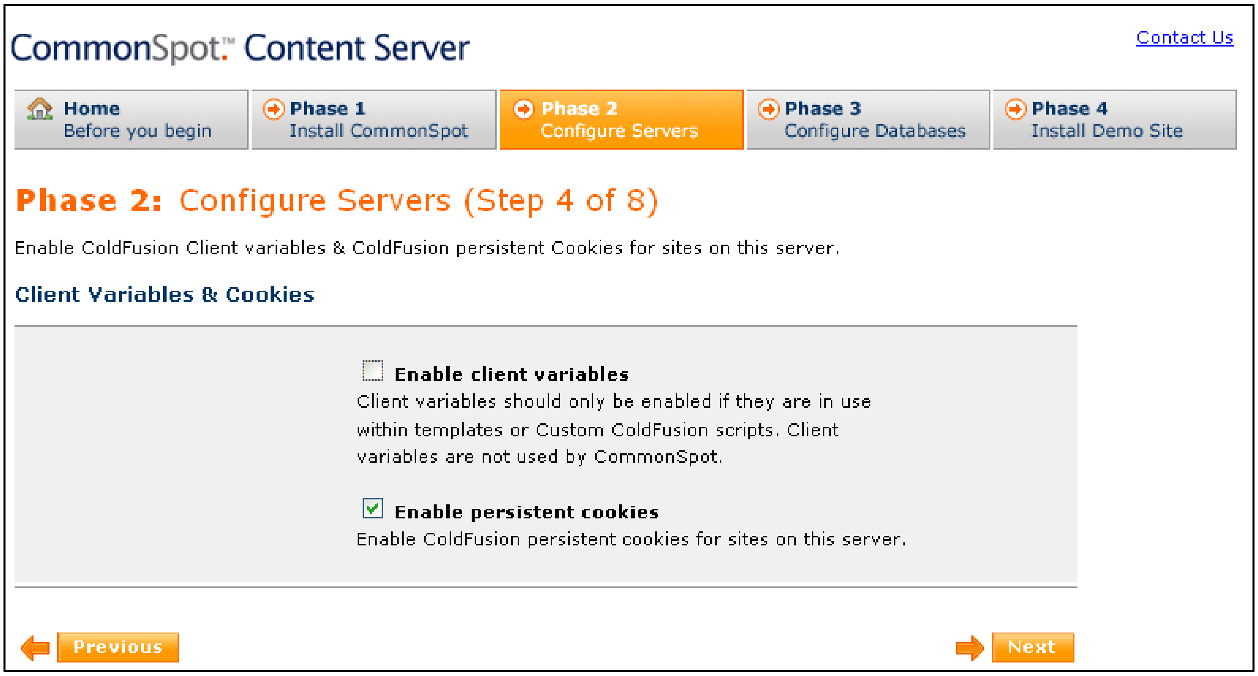
3.4.4. Phase 2: Configure Servers (Step 4 of 8) Dialog

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.

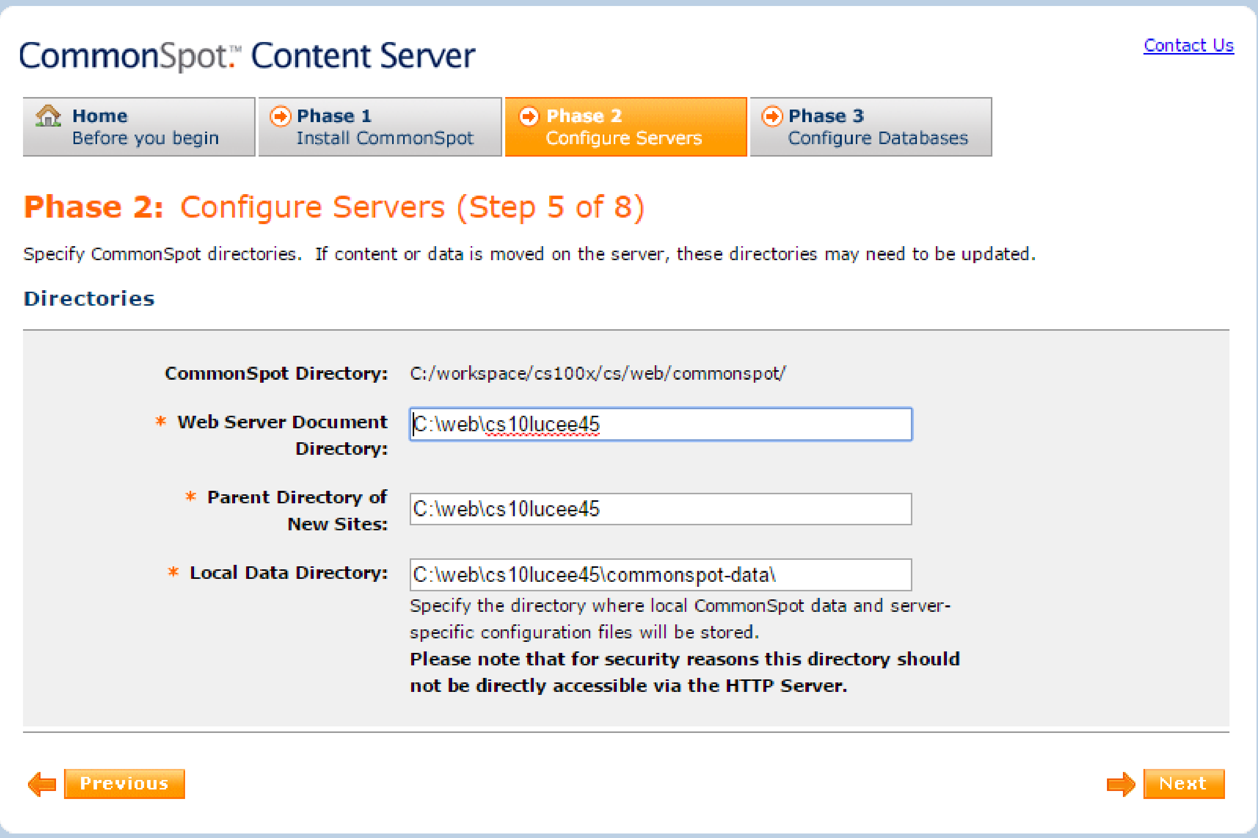
Client Variables & Cookies

☐ **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.

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 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

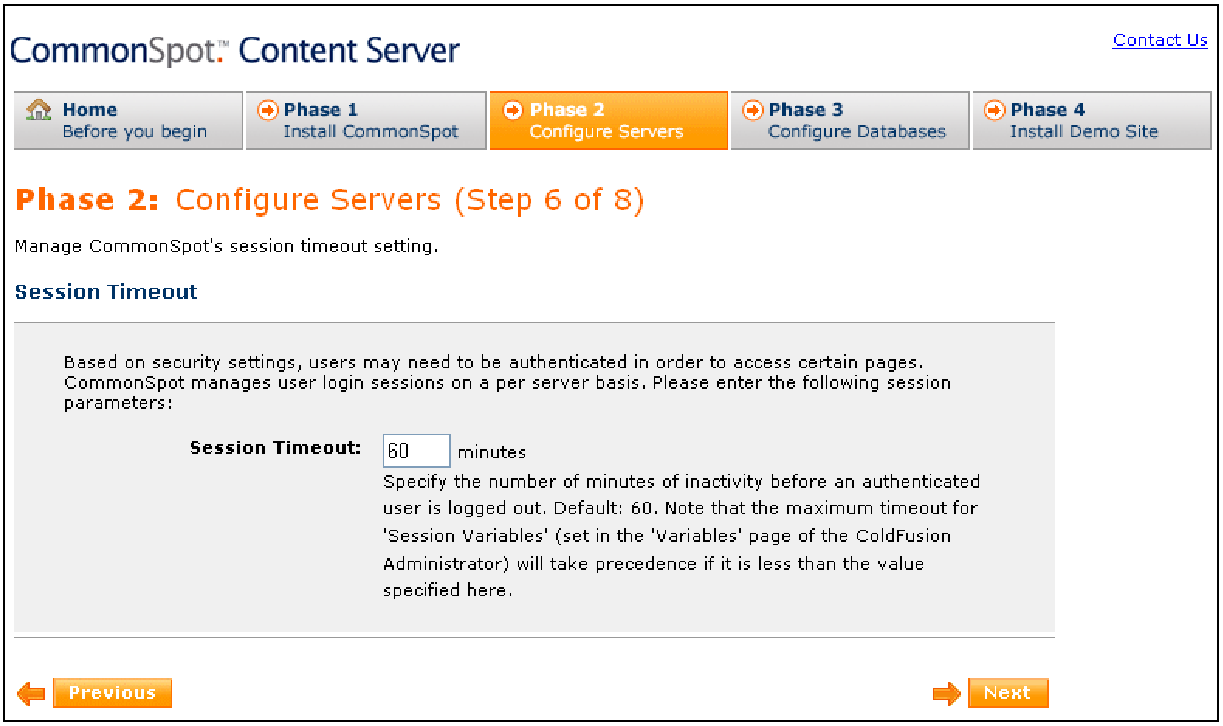
CommonSpot Directory:	C:/workspace/cs100x/cs/web/commonspot/
* **Web Server Document Directory:**	C:\web\cs10lucee45
* **Parent Directory of New Sites:**	C:\web\cs10lucee45
* **Local Data Directory:**	C:\web\cs10lucee45\commonspot-data\

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.


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
Previous
Next

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: 60 minutes

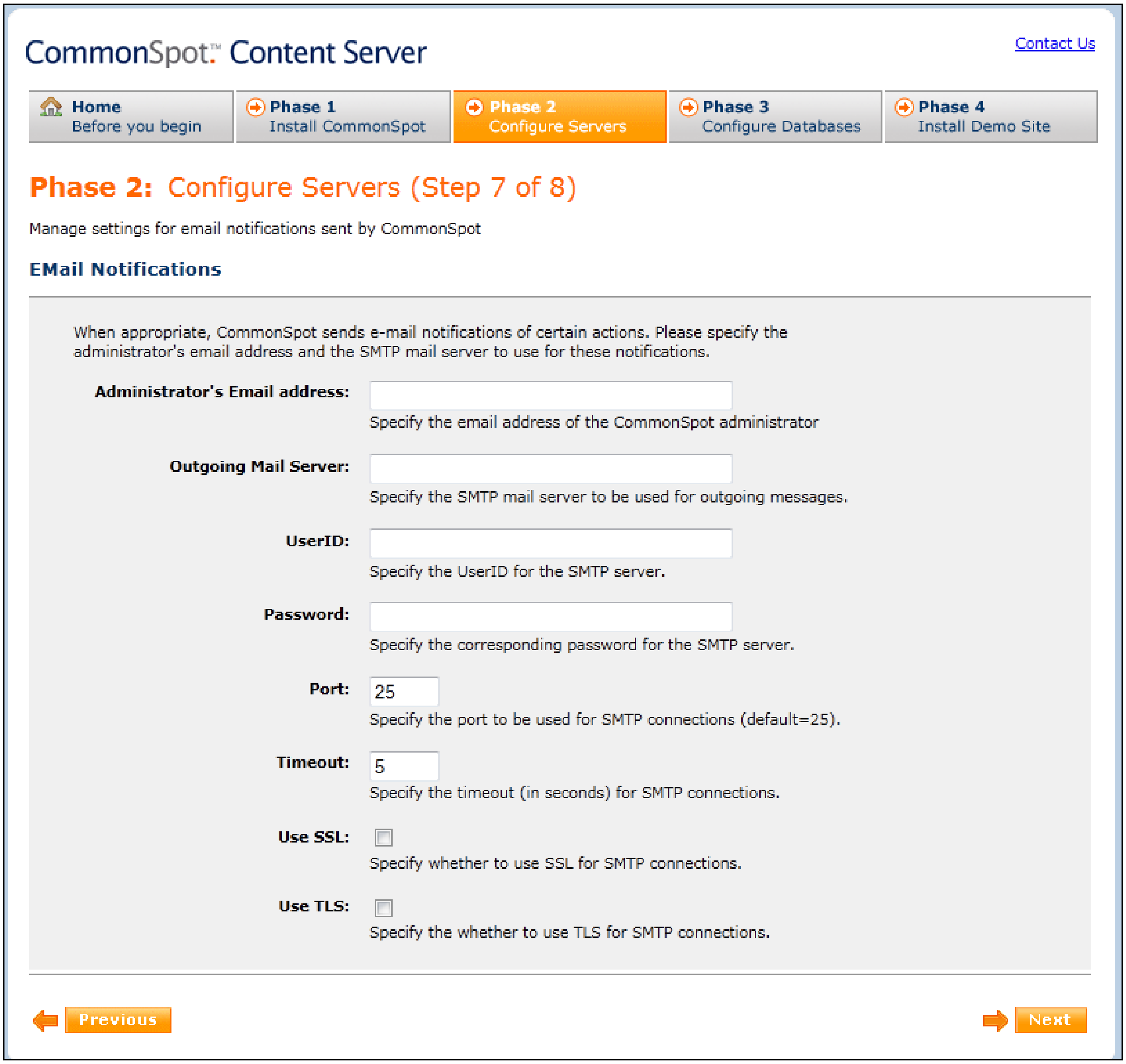
Specify the number of minutes of inactivity before an authenticated user is logged out. Default: 60. Note that the maximum timeout for 'Session Variables' (set in the 'Variables' page of the ColdFusion Administrator) will take precedence if it is less than the value specified here.

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
- Error messages to admin accounts

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. You can do this now, or configure email later through Server Administration.– Configuration – Email Notifications.



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

Timeout: 5
Specify the timeout (in seconds) for SMTP connections.

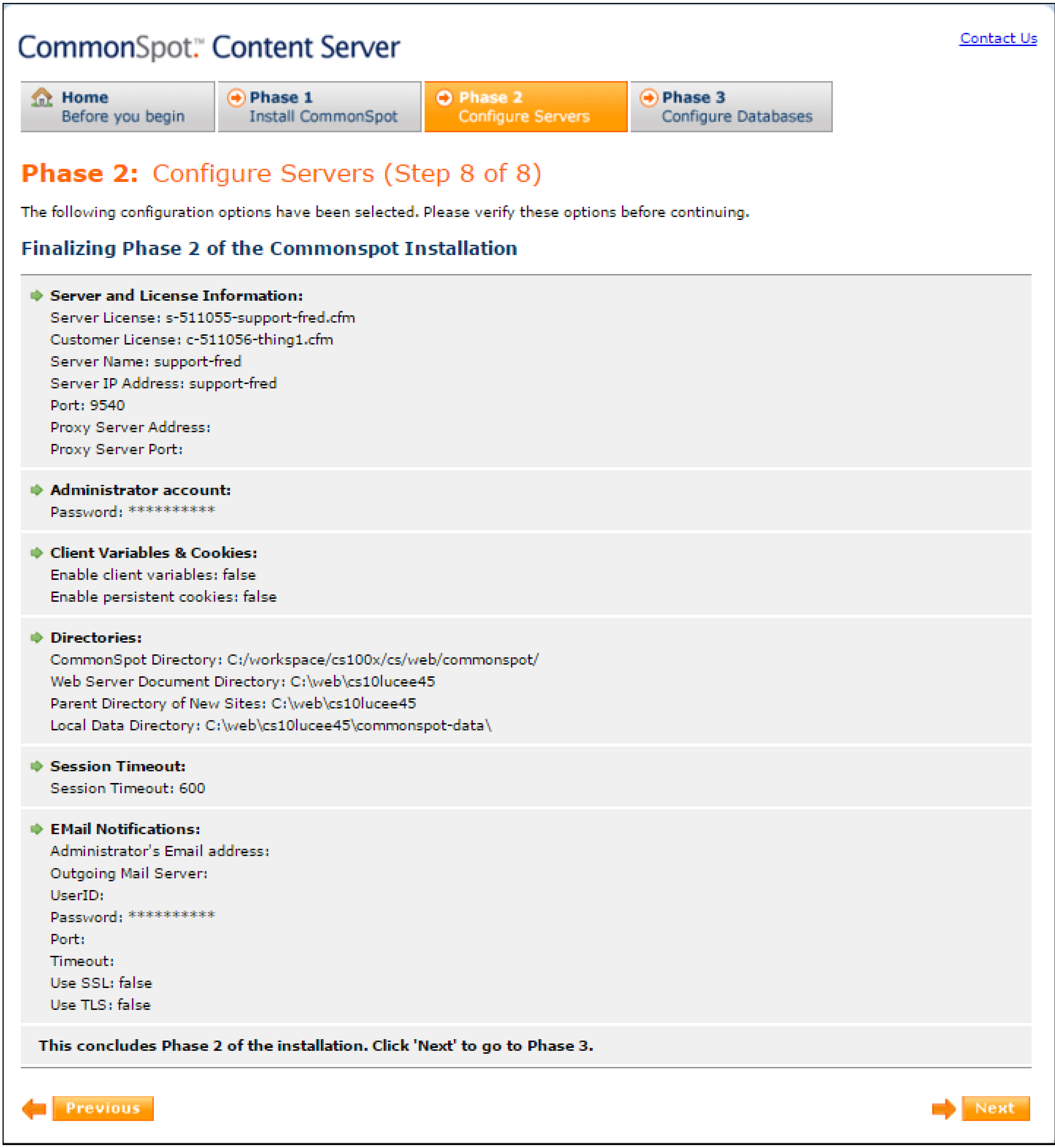
Use SSL: □
Specify whether to use SSL for SMTP connections.

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

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-511055-support-fred.cfm
Customer License: c-511056-thing1.cfm
Server Name: support-fred
Server IP Address: support-fred
Port: 9540
Proxy Server Address:
Proxy Server Port:

Administrator account:
Password: **********

Client Variables & Cookies:
Enable client variables: false
Enable persistent cookies: false

Directories:
CommonSpot Directory: C:/workspace/cs100x/cs/web/commonspot/
Web Server Document Directory: C:\web\cs10lucee45
Parent Directory of New Sites: C:\web\cs10lucee45
Local Data Directory: C:\web\cs10lucee45\commonspot-data\

Session Timeout:
Session Timeout: 600

EMail Notifications:
Administrator's Email address:
Outgoing Mail Server:
UserID:
Password: **********
Port:
Timeout:
Use SSL: false
Use TLS: false

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

3.5. Phase 3 – Configure Your Databases

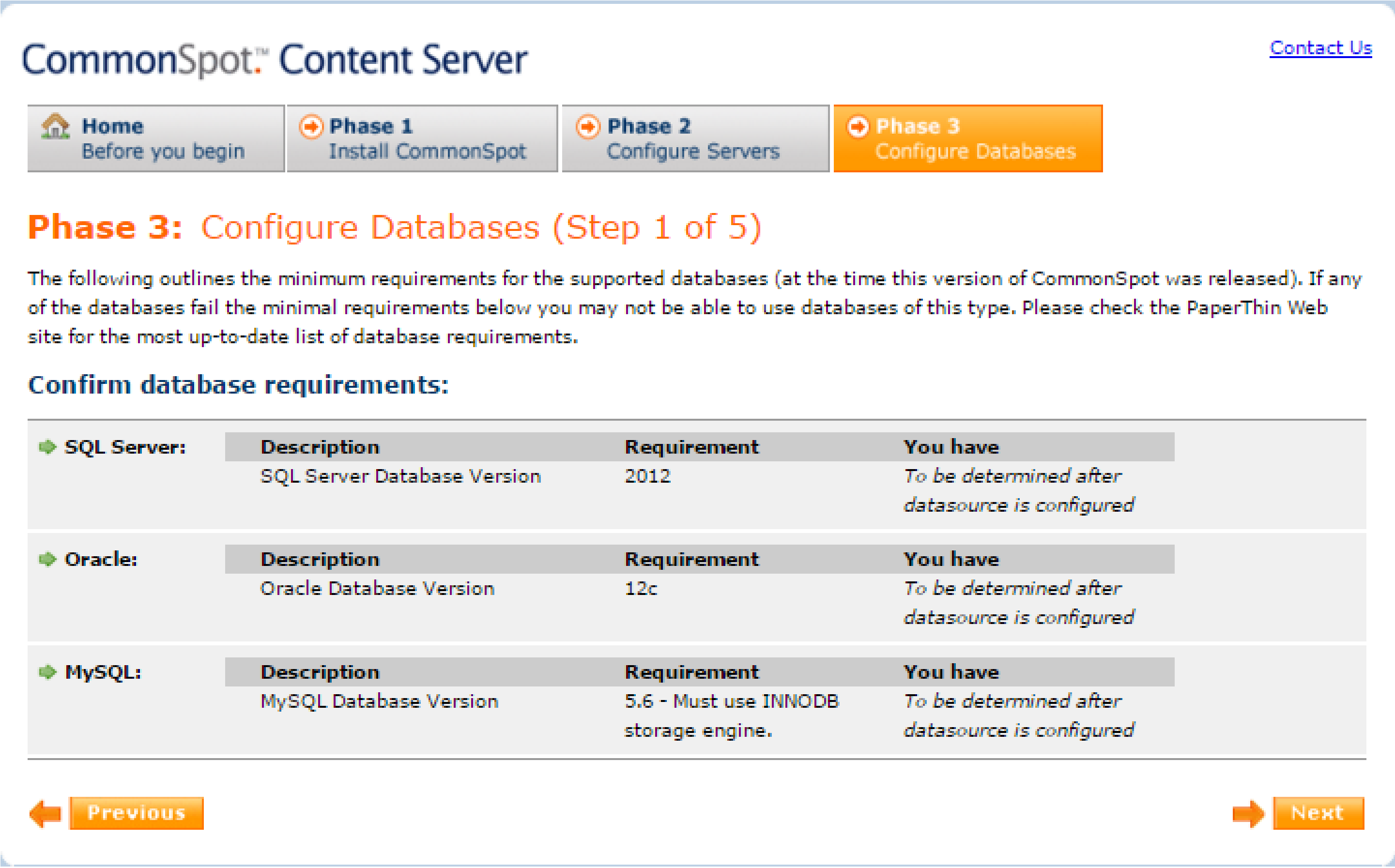
Phase 3 walks you through creating data source connections for the databases used with CommonSpot. These requirements depend on your database type.

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.



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:

	Description	Requirement	You have
SQL Server:	SQL Server Database Version	2012	*To be determined after datasource is configured*
Oracle:	Oracle Database Version	12c	*To be determined after datasource is configured*
MySQL:	MySQL Database Version	5.6 - Must use INNODB storage engine.	*To be determined after datasource is configured*

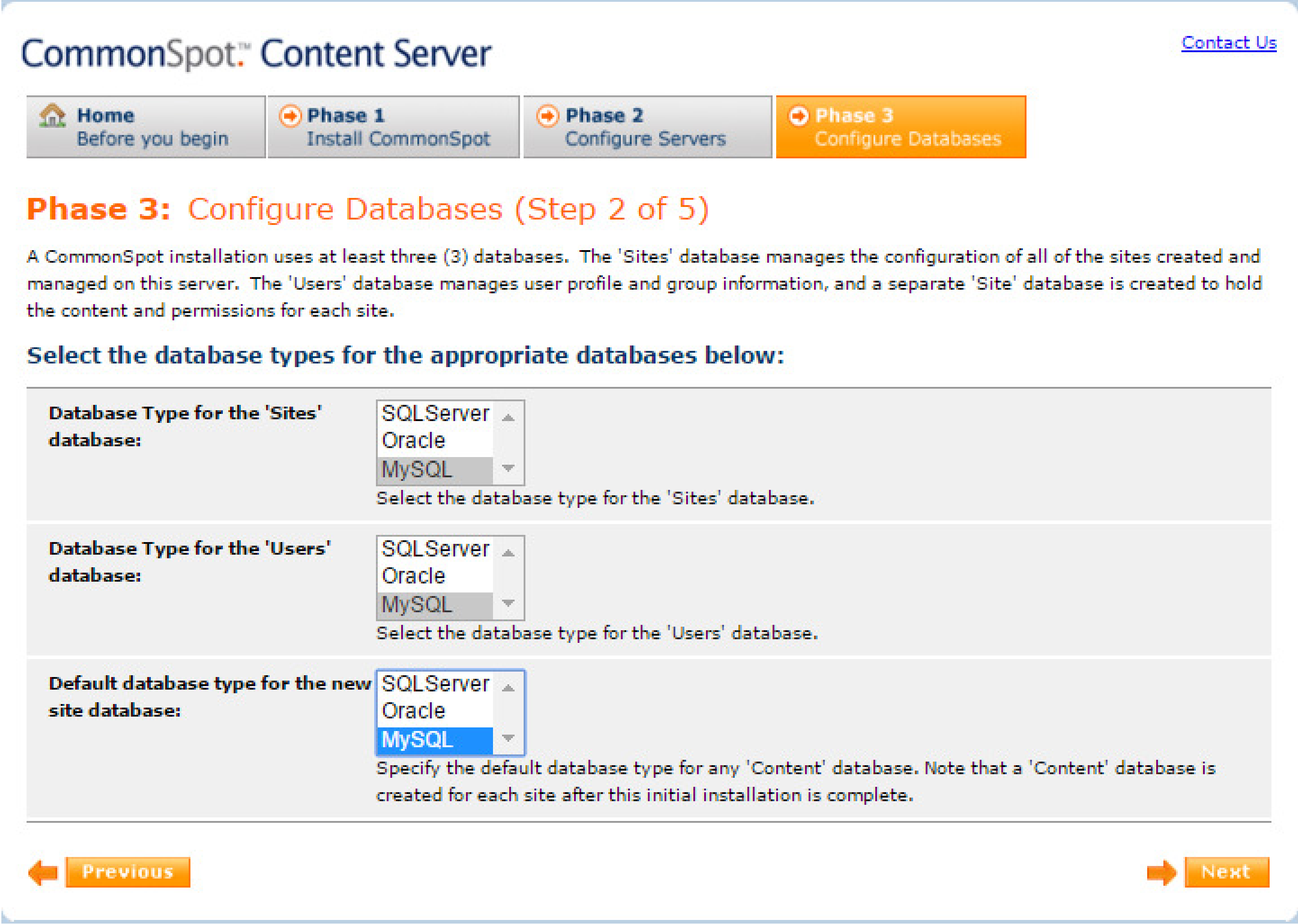
If you are not going to use one or more of the database types listed, you can ignore any warnings that display about them.

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 the CommonSpot server and all sites. The environment information for this CommonSpot instance.
- **Users**. This is the database used to store user and group information. Customers with multiple sites may choose to have all sites use the same users database (the norm) or have individual users database for each site. If choosing the later additional customer key is required. One users database per customer key.
- **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: SQLServer / Oracle / MySQL
Select the database type for the 'Sites' database.

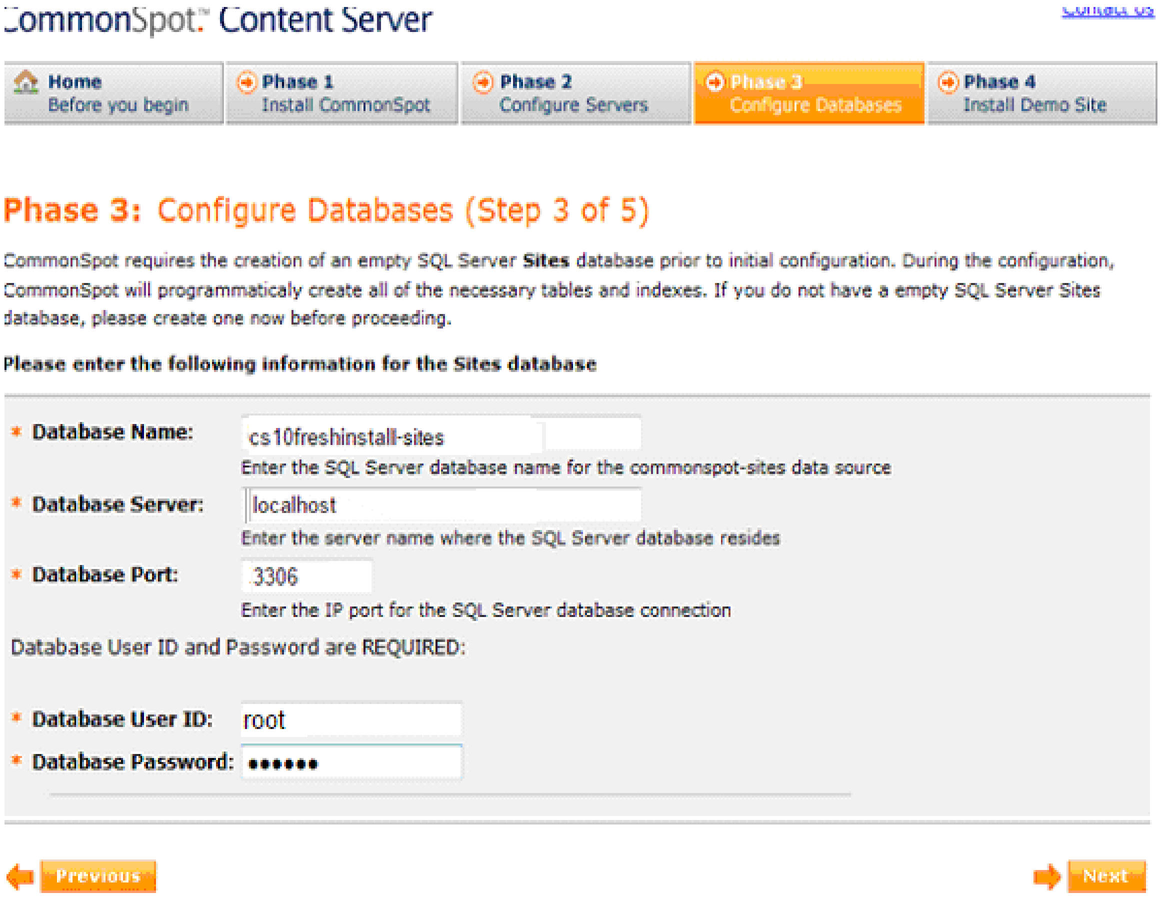
Database Type for the 'Users' database: SQLServer / Oracle / MySQL
Select the database type for the 'Users' database.

Default database type for the new site database: SQLServer / Oracle / 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 datasource:

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. *port may be left blank for SQL Server Instances.



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 programmaticaly 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:** cs10freshinstall-sites
Enter the SQL Server database name for the commonspot-sites data source

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

* **Database Port:** 3306
Enter the IP port for the SQL Server database connection

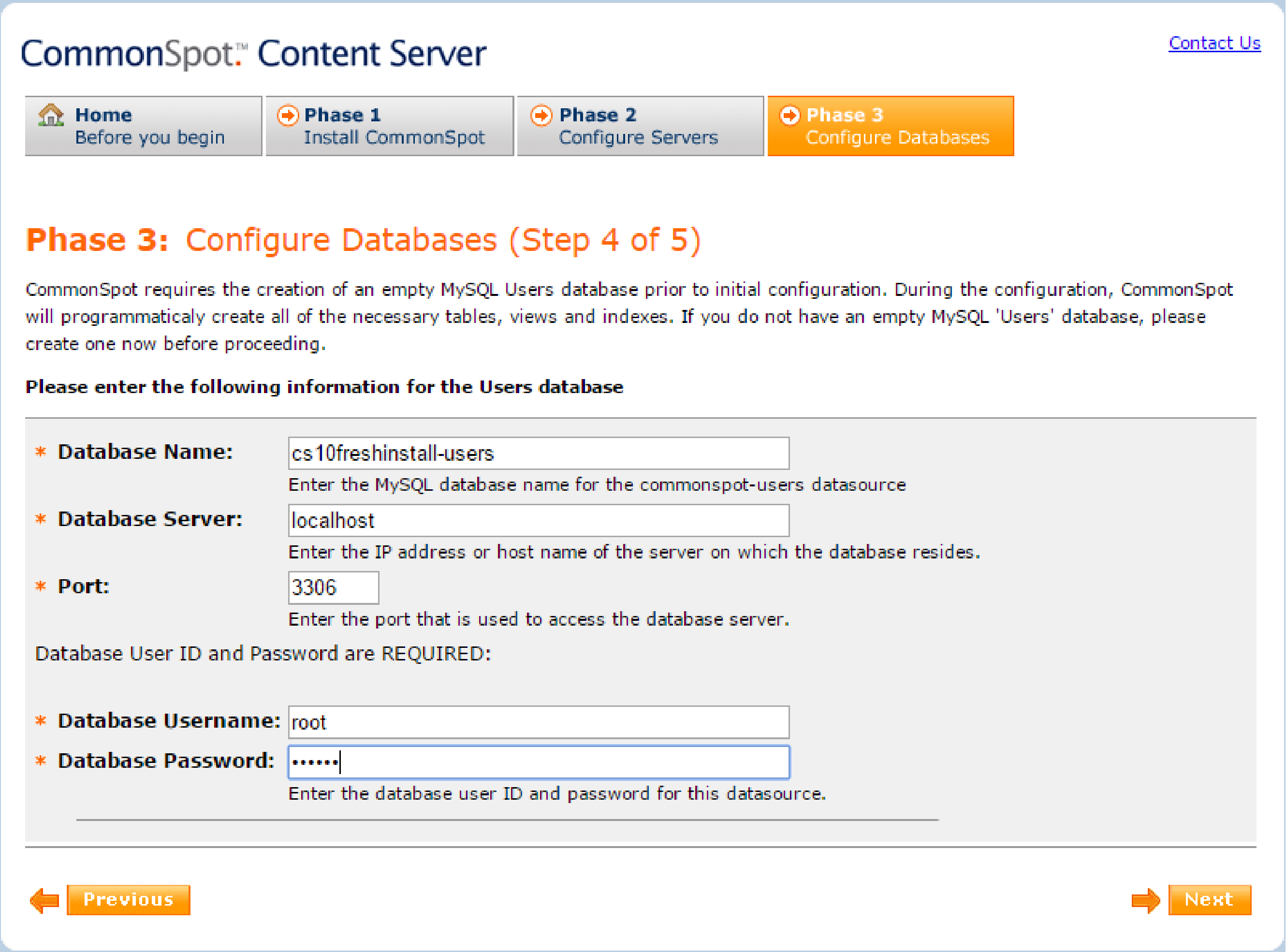
Database User ID and Password are REQUIRED:

* **Database User ID:** root
* **Database Password:** ••••••

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.



Phase 3: Configure Databases (Step 4 of 5)

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

Please enter the following information for the Users database

* **Database Name:** cs10freshinstall-users
Enter the MySQL database name for the commonspot-users datasource

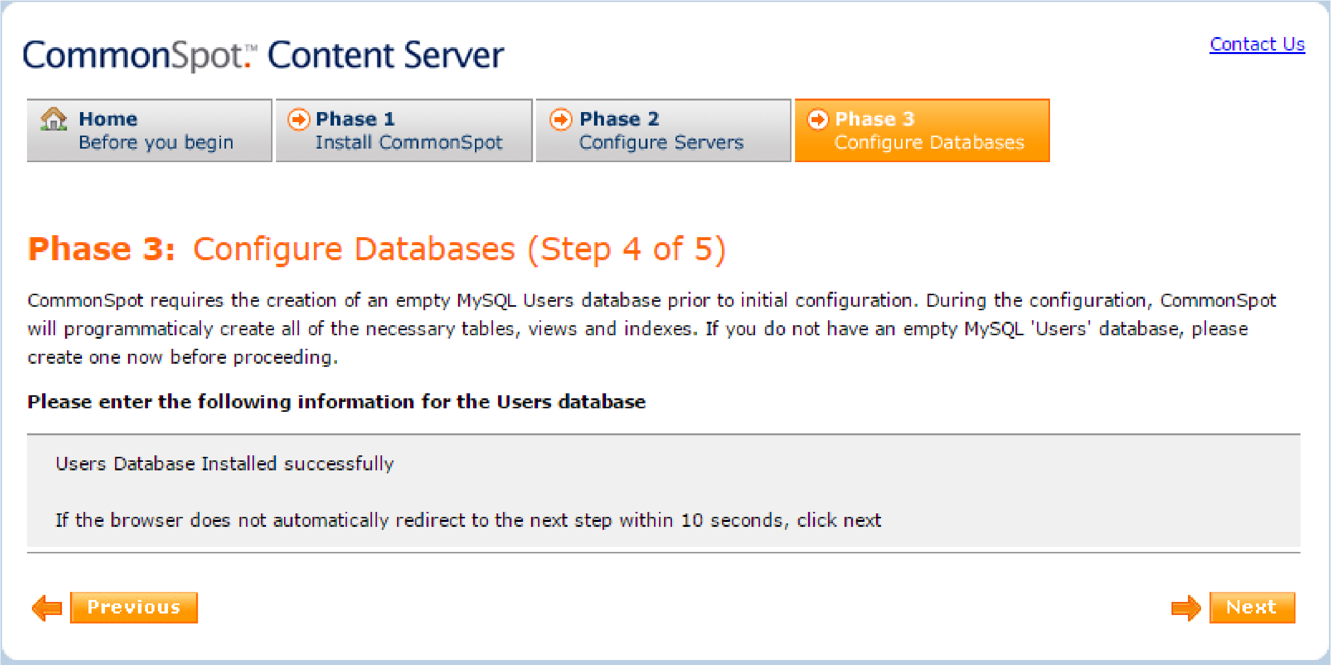
* **Database Server:** localhost
Enter the IP address or host name of the server on which the database resides.

* **Port:** 3306
Enter the port that is used to access the database server.

Database User ID and Password are REQUIRED:

* **Database Username:** root

* **Database Password:** ••••••
Enter the database user ID and password for this datasource.


CommonSpot™ Content Server
Contact Us
Home Before you begin
Phase 1 Install CommonSpot
Phase 2 Configure Servers
Phase 3 Configure Databases
Previous
Next

Phase 3: Configure Databases (Step 4 of 5)

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

Please enter the following information for the Users database

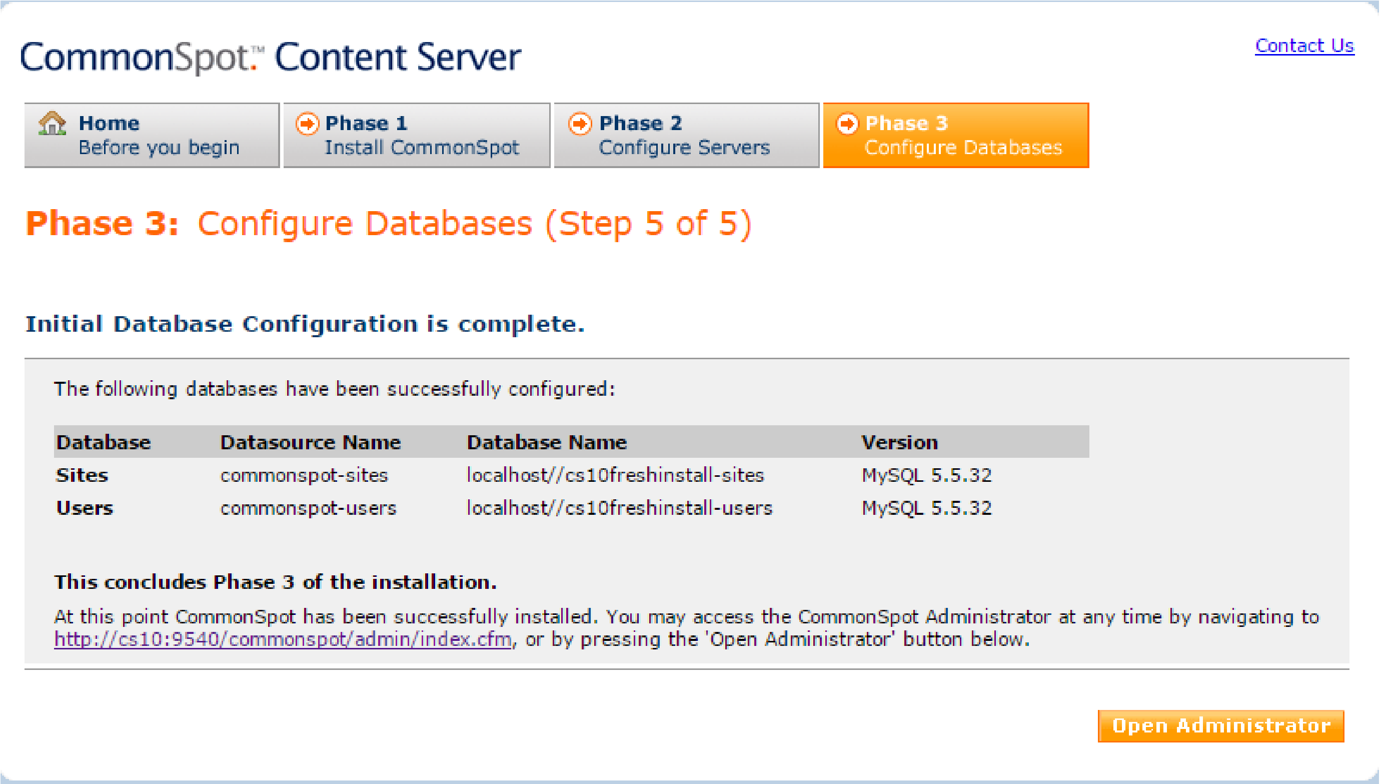
Users Database Installed successfully

If the browser does not automatically redirect to the next step within 10 seconds, click next

The following Step 5 of 5 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:

Database	Datasource Name	Database Name	Version
Sites	commonspot-sites	localhost//cs10freshinstall-sites	MySQL 5.5.32
Users	commonspot-users	localhost//cs10freshinstall-users	MySQL 5.5.32

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://cs10:9540/commonspot/admin/index.cfm, or by pressing the 'Open Administrator' button below.

Chapter 4 Post-Installation Considerations

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

4.1. 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 can recover CommonSpot Web sites only with a backup of the required databases. Make sure you maintain a regular backup schedule for CommonSpot databases and site file system(s).

4.2. Create Scheduled Jobs

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 the details of inserting jobs and managing changes in the ColdFusion or Lucee Administrator.

You must explicitly enable and schedule jobs in order to run them. CommonSpot does not automate job creation or insertion.

Access this 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**.

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

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.

4.3. 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.

4.4. For MySQL Environments, Check Field Size

By default, MySQL limits field size to 1MB, even though it can handle fields as large as 1GB. In CommonSpot, this limitation is easily exceeded, resulting in errors like the following:

Packet for query is too large (2138999 > 1048576).

You can change this value on the server by setting the max_allowed_packet variable through the MySQL Workbench or by adding the following line to the '[mysqld]' section of the '.ini' file:

```
max_allowed_packet = 1G
```

By default, this is 'my.ini' and lives in the root directory of the MySQL installation. You can find the name of the .ini file on the command line for the service. For example, in Windows, open Services and check Properties from the right-click menu for the MySQL service.

4.5. 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/

4.6. 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 ESR and later and Internet Explorer 11, as well as Chrome and Safari on the Mac. For details, review the Release Notes and visit:

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

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

Chapter 5 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)

For the most up-to-date information on security issues affecting CommonSpot, search for “security” or “alert” in:

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

In addition, the Support team sends notices to all customer DSRs for issues of immediate concern.

5.1. 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. Exceptions for * installation ** upgrades *** demo site and **** CommonSpot tools are noted below.

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, 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 that are meant 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

5.2. 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.

5.2.1. 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`).

5.2.2. 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 or Lucee service is restarted on each server where encryption was applied..

5.3. 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. An internal security review was conducted on CommonSpot code and pages with potential issues were modified with strict input validation.

In addition, security has been added to the core of CommonSpot to prevent SQL injection.

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.

5.4. Controlling Access to CommonSpot Modules (URL Tampering)

If you do not adhere to proper security guidelines, it becomes possible for intruders 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). By default 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.

These modules are used for CommonSpot Content Creation API purposes and access to them are not required to use CommonSpot. See the CommonSpot Developers Guide for additional information.

5.4.1. 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.

5.4.2. 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.

5.4.3. 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 or Lucee 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.

5.4.4. 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):
```

To preserve log files and make it easier to locate valuable information, this and other CommonSpot log files are created new each calendar day if needed.