



# Surround SCM

## Installation Guide

Version 2012

# Copyrights

© 2012 Seapine Software, Inc. All rights reserved.

QA Wizard Pro, Seapine CM, SoloBug, SoloSubmit, Surround SCM, and TestTrack are trademarks or registered trademarks of Seapine Software, Inc. in the United States and other countries.

Borland and StarTeam are trademarks or registered trademarks of Borland, Inc. in the United States and other countries.

Delphi and JBuilder are trademarks or registered trademarks of Embarcadero Technologies, Inc. in the United States and other countries.

Acrobat Reader is a registered trademark of Adobe, Inc. in the United States and other countries.

Sun, JVM, Java, JavaScript, and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Apple, Mac, Mac OS, Macintosh, Objective-C, and Safari are registered trademarks of Apple Computer, Inc.

Microsoft, Windows, Windows NT, Windows Server, Windows Vista, MS Windows, Active Directory, Internet Explorer, Outlook, SQL Server, Visual SourceSafe, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Linux is a trademark of Linus Torvalds.

Red Hat, Red Hat Enterprise Linux, and Fedora are the registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE is the registered trademark of Novell Inc. in the United States and other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

Ubuntu is a registered trademark of Canonical Ltd.

IBM, ClearCase, and all other IBM brand and product names are service marks, trademarks or registered trademarks of IBM Corporation or its subsidiaries in the United States and other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

PVCS, Serena PVCS Professional Suite, and Serena PVCS Version Manager are registered trademarks of Serena Software, Inc.

All other product names mentioned herein are the trademarks of their respective owners. All other trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Seapine Software, Inc.

Your license agreement with Seapine Software, Inc., which is included with the product, specifies the permitted and prohibited uses of the product. Any unauthorized duplication or use of this software, in whole or in part, in print, or in any other storage and retrieval system is forbidden.

Information in this document is subject to change without notice and does not represent a commitment on the part of Seapine Software, Inc. Unless otherwise noted, all companies, products, street addresses, and persons contained herein are purely fictitious. Mention of third-party companies and products is for informational purposes only and does not constitute an endorsement.

Seapine Software, Inc.  
5412 Courseview Drive, Suite 200  
Mason, OH 45040  
(513) 754-1655

[documentation@seapine.com](mailto:documentation@seapine.com)

# Contents

<b>Surround SCM Installation Overview</b> .....	<b>1</b>
About Surround SCM databases.....	1
About upgrade installations.....	1
About the 64-bit Surround SCM Server.....	2
<b>Before You Install</b> .....	<b>3</b>
System requirements.....	3
RDBMS database information.....	3
Installation types.....	4
Installers.....	5
<b>Installing Surround SCM</b> .....	<b>7</b>
Running the installer.....	7
Selecting Surround SCM integration options.....	7
Setting Surround SCM configuration options.....	7
Setting the WebDAV CGI configuration options.....	8
Setting Seapine License Server options.....	9
Setting CMIS Server configuration options.....	10
Selecting RDBMS configuration options.....	10
<b>After Installing</b> .....	<b>13</b>
Starting the Seapine License Server.....	13
Starting the Seapine License Server Admin Utility.....	13
Configuring a Seapine License Server connection.....	14
Adding licenses.....	14
Adding users.....	14
Starting the Surround SCM Server.....	15
Starting Surround SCM.....	15
Configuring a Surround SCM Server connection.....	15
Configuring the proxy server.....	16
Starting the proxy server.....	16
Starting the Surround SCM CMIS Server.....	16
Starting the Surround SCM CMIS Admin Utility.....	17
Configuring the Surround SCM CMIS Server.....	17
Configuring web servers for WebDAV.....	18
Configuring WebDAV.....	21
Configuring web servers for the Seapine License Server Web Admin Utility.....	23

---

<b>Troubleshooting Server Issues</b> .....	<b>27</b>
<b>Setting Up RDBMS Databases</b> .....	<b>29</b>
Setting up PostgreSQL databases.....	29
Setting up Oracle databases.....	30
Setting up SQL Server databases.....	31
Troubleshooting RDBMS connections.....	32
<b>Appendix A: Third-Party Software Licenses</b> .....	<b>37</b>
<b>Index</b> .....	<b>41</b>

# Surround SCM Installation Overview

In general, there are three stages to installing Surround SCM.

1. Preparation tasks to complete before running the installer, such as checking system requirements and determining what RDBMS information you will need.
2. Installation tasks to perform while running the installer, such as selecting which components to install and setting configuration options.
3. Configuration tasks to complete after running the installer, such as configuring server connections or upgrading existing mainline branches.

## About Surround SCM databases

Surround SCM data is stored in RDBMS-based databases. Microsoft SQL Server, Oracle, and PostgreSQL are supported. When you install Surround SCM, you can install PostgreSQL or add connections to existing SQL Server, Oracle, or PostgreSQL databases. See [RDBMS database information, page 3](#).

The following Surround SCM data is stored in an RDBMS database:

- Each Surround SCM Server has a server database, which is a set of tables that store user, security group, workflow, custom field, and TestTrack integration connection information.
- Each mainline branch has a mainline database, which is a set of tables that store all file information.

By default, the server and mainline databases are stored in the same RDBMS database. After installation, you can change the configuration if you decide to use a different RDBMS type or move databases between servers. You can also move mainline databases to a separate RDBMS database from the server database or store mainlines in multiple RDBMS databases and point a single Surround SCM Server to them. Mainlines can only be associated with one Surround SCM Server.

You can leverage your existing database administration process and use standard database tools for tasks such as analysis, manipulation, and backups. All Surround SCM data is stored in the RDBMS database except the server database connection information.

**Note:** All file data is stored in the RDBMS database as binary large objects (BLOBs). The RDBMS may allow you to control where BLOB data is stored and indexed. If you want more granular control over BLOBs, consult your DBA and RDBMS documentation.

## About upgrade installations

You should always create backup copies of the Surround SCM Server database, mainline databases, and the Seapine License Server database before installation.

- Run the Surround SCM Analyze Utility before installation to analyze and repair any data integrity issues in the Surround SCM Server database.
- If you are upgrading the Seapine License Server, back up the license server directory and all subdirectories and files in it before installation. Following are the default license server installation directories.
  - **Windows**—C:\Program Files\Seapine\License Server

- **Mac**—/Applications/Seapine License Server
- **Linux**—/var/lib/splicsvr
- If you upgrade from Surround SCM 5.x or later, the server database is automatically upgraded to Surround SCM 2008 format before it is upgraded to RDBMS format. You cannot revert back to the flat file database format after upgrading, which makes it important to back up the database before installation. Your Surround SCM backup strategy will no longer work after the upgrade because the database format and location are different. Make sure you develop a new backup strategy before upgrading.
- Surround SCM 2009 and later stores the server database and mainline branches in RDBMS-based databases. The Surround SCM Server database is automatically upgraded when the server starts. After installation, you must manually upgrade mainline branches to RDBMS format before users can access them. See the [Surround SCM Upgrade Guide](http://downloads.seapine.com/pub/docs/SurroundScmUpgradeGuide.pdf) (<http://downloads.seapine.com/pub/docs/SurroundScmUpgradeGuide.pdf>).
- Some fields with unlimited sizes in Surround SCM 2008 and earlier now have size restrictions due to the change to RDBMS database format. File names have a 255 character limit. Repository names have a 1024 character limit. Other name fields, such as ones for triggers, filters, security groups, and TestTrack projects, have a 128 character limit. Security group descriptions have a 1020 character limit, and comment fields have a 4096 character limit. If field values exceed the database size limit, they are truncated during the upgrade.

## About the 64-bit Surround SCM Server

The 64-bit version of the Surround SCM Server application lets the server computer access more RAM, which increases the number of branches that can be cached when the server starts.

- Only the Surround SCM Server is supported on 64-bit systems. A 64-bit Surround SCM Client is not available. The 32-bit clients can communicate with the 64-bit Surround SCM Server and vice versa.
- The 64-bit Surround SCM Server is packed in a separate installer for Windows, Mac OS X, and Linux (Perl and Java). See [Installers, page 5](#).
- The 64-bit Surround SCM Server has different system requirements than the 32-bit Surround SCM Server. Make sure the server computer meets the recommended system requirements. See the [Surround SCM Server System Requirements](#) knowledgebase article ([www.seapine.com/kb/questions/1173](http://www.seapine.com/kb/questions/1173)).
- Database conversion is not necessary when upgrading from the 32-bit Surround SCM Server to the 64-bit Surround SCM Server or downgrading from 64-bit to 32-bit. The only exception is if you upgrade from Surround SCM 5.x and later.

# Before You Install

Before installing Surround SCM, take some time to determine what options you will need to select during the installation. Keep the following in mind:

- You must be logged in as a user with full administrative privileges.
- If you use TestTrack, the Seapine License Server and Seapine License Server Admin Utility may already be installed on your network. Check with the TestTrack administrator.
- If you are installing the Surround SCM Proxy Server, we recommend configuring a proxy server definition on the master Surround SCM Server before the proxy server is installed. See 'Using Proxy Servers' in the Surround SCM User Guide for information.
- If you use Surround SCM Linux and will be using PostgreSQL, make sure your Linux server's locale LC\_CTYPE setting is either UTF8, C, or POSIX. See the [Surround SCM PostgreSQL Installation Fails on Linux](http://www.seapine.com/kb/questions/1534) knowledgebase article ([www.seapine.com/kb/questions/1534](http://www.seapine.com/kb/questions/1534)).

## System requirements

Review the following knowledgebase articles to check system requirements for the Surround SCM Client and the Surround SCM Server:

- [Surround SCM Client System Requirements](http://www.seapine.com/kb/questions/1204) ([www.seapine.com/kb/questions/1204](http://www.seapine.com/kb/questions/1204))
- [Surround SCM Server System Requirements](http://www.seapine.com/kb/questions/1173) ([www.seapine.com/kb/questions/1173](http://www.seapine.com/kb/questions/1173))

## RDBMS database information

Determining which RDBMS you will use before installing Surround SCM can help streamline the installation process. Keep the following in mind:

- The server database tables are installed in a single RDBMS database. PostgreSQL is the default database type. Surround SCM can install PostgreSQL and create the database tables during the installation, or you can manually install it. You can also host Surround SCM databases in Oracle or SQL Server (Windows only). Your DBA must manually install Oracle or SQL Server before installation. See [Setting Up RDBMS Databases, page 29](#).
- If you choose to use PostgreSQL, decide if you want to install the PostgreSQL files and databases on the Surround SCM Server computer or a different computer. You can point the Surround SCM Server to access RDBMS servers on other computers.
- The database configuration you use depends on your installation and environment. At any time, you can convert the RDBMS type or location for the server or mainline database or distribute mainline databases across multiple RDBMS database instances. If you do not know how you want to configure the databases, use the default PostgreSQL installation and make configuration changes later.
- Review the operating system and database firewall settings on the RDBMS server to make sure the Surround SCM databases are secure. Some RDBMS servers must be configured to allow remote computers to access databases.

## Installation types

Installation type	Description	Notes
Surround SCM Client	Installs the GUI client, the CLI, and the SCCI DLL.	Most users only need to install the client.
Surround SCM API	Installs the API.	Allows third-party client applications to communicate with the Surround SCM Server.
Surround SCM Server	Installs the server and optionally installs PostgreSQL to host data.	The server application is generally installed on a networked computer.
Surround SCM Proxy Server	Installs the proxy server.	We recommend configuring a proxy server definition on the master Surround SCM Server before the proxy server is installed. See <a href="#">Configuring the proxy server, page 16</a> .
Surround SCM CMIS Server	Installs the CMIS Server and CMIS Admin Utility.	Allows Surround SCM integration with Content Management Interoperability Services (CMIS) clients. See <a href="#">Configuring the Surround SCM CMIS Server, page 17</a> .
Surround SCM WebDAV CGI	Installs the WebDAV CGI, including the sscmdav.cgi script and sscmdav.xml config file.	When the WebDAV CGI is installed and configured, users can access source files using a web browser, a Windows network place, the Mac OS X Finder, a Linux filesystem path, and WebDAV-specific applications. You can work with files in applications that support WebDAV functionality such as Microsoft Office, Adobe Photoshop, or Adobe Dreamweaver. See <a href="#">Configuring web servers for WebDAV, page 18</a> .
Seapine License Server Web Admin Utility	Installs the web-based Seapine License Server Admin Utility.	A web server must be installed on the computer before installation. See <a href="#">Configuring web servers for the Seapine License Server Web Admin Utility, page 23</a>

Installation type	Description	Notes
Seapine License Server Admin Utility	Installs the Seapine License Server Admin Utility.	The Seapine License Server and Seapine License Server Admin Utility are generally installed on one networked computer.
Seapine License Server	Installs the Seapine License Server.	The Seapine License Server and Seapine License Server Admin Utility are generally installed on one networked computer.

## Installers

Platform	Installation Program	Name
Windows	Complete	sscmwininstall.exe
	64-bit Surround SCM Server (includes 64-bit Seapine License Server)	sscmwininstall64bit.exe
	Client-only	sscmwininstallclient.exe
Mac	Complete (includes the 64-bit Surround SCM Server and 64-bit Seapine License Server)	sscmmacosxinstall.dmg.gz
	Client-only	sscmmacosxclientinstall.dmg.gz
Linux	Complete	sscmlinuxjavainstall.tar.gz
	64-bit Surround SCM Server (includes 64-bit Seapine License Server)	sscmlinux64javainstall.tar.gz
	Client-only	sscmlinuxjavaclientinstall.tar.gz
	Command line	sscmlinuxinstall.tar.gz
	Command line 64-bit Surround SCM Server (includes 64-bit Seapine License Server)	sscmlinux64bitinstall.tar.gz



# Installing Surround SCM

You must select settings for the Surround SCM components you decide to install during the installation. Depending on the type of installation you are performing, you may be prompted for different information.

## Running the installer

- **Windows**—Double-click the installation file.
- **Mac**—Gunzip the installation file to extract the installer, then double-click **sscmmacosxinstall.dmg** to mount the image on the desktop. Double-click the Surround SCM disk image, then double-click the **Install Surround SCM** icon.
- **Linux graphical installer**—Untar and gunzip the installation file, then log in as root and double-click the installer file in the Window Manager.
- **Linux command line installer**—Enter `./install.pl` to run the install script.

## Selecting Surround SCM integration options

Surround SCM can be integrated into various third-party IDEs, build tools, and applications. These integrations allow users to access source code and files stored in Surround SCM from other programs without using the Surround SCM Client. See the [Surround SCM Third-Party Integrations](#) knowledgebase article ([www.seapine.com/kb/questions/1504](http://www.seapine.com/kb/questions/1504)) for a list of supported integrations.

Surround SCM conforms to the Microsoft Source Code Control Interface (SCCI) standard and can be integrated with many Windows IDEs and applications. To use Surround SCM as the default source control provider for applications that support the SCCI interface, select the **Make Surround SCM my default SCCI provider** option.

Other integration options and plug-ins are also available during Surround SCM installation for Windows and other supported platforms. Some integration plug-ins for Unix applications must be manually installed. See the [Integrations](#) knowledgebase category ([www.seapine.com/kb/categories/Surround+SCM/Integrations](http://www.seapine.com/kb/categories/Surround+SCM/Integrations)) for setup, usage, and troubleshooting information.

## Setting Surround SCM configuration options

You must select a Surround SCM application directory. The Mac and Linux installers also require you to select a directory for creating the `SCMStartup.log` and `SCMProxyStartup.log` files. You can use the default directory or select a different directory.

Additional configuration options include setting the server port number and choosing a server execution mode (Windows only).

## Default installation directories

Installer	Files	Default directory
Windows	All files	C:\Program Files\Seapine\Surround SCM
Mac	Application	/Applications/Surround SCM
	SCMStartup.log and SCMPProxyStartup.log files	/var/log
	Unix commands	/usr/bin
Linux	Application	/var/lib/SurroundSCM
	SCMStartup.log and SCMPProxyStartup.log files	/var/log
	Unix commands	/usr/bin

## Server execution mode (Windows only)

You can choose to run the Surround SCM Server as a service if you want the server to automatically start when the computer starts. If you run the server as an application, you must manually start the Surround SCM Server application.

## Server port

The server communicates with Surround SCM clients on this port. Use the default port number (4900) or enter another number.

## Setting the WebDAV CGI configuration options

If you are installing the WebDAV CGI, you must set a location to install the CGI scripts and a server IP address and port number.

Platform	Default CGI directory	Default port number
Windows	C:\InetPub\scripts	4900
Mac	/Library/WebServer/CGI-Executables	4900
Linux	/var/www/cgi-bin	4900

## Setting Seapine License Server options

You must select a Seapine License Server application directory. The Mac and Linux installers also require you to select a directory for creating the LSStartup.log file. You can use the default directory for these options or select a different directory.

Additional configuration options include setting the server port number, choosing a server execution mode (Windows only), and setting the web server admin utility CGI and HTML file locations.

### Default installation directories

Platform	Files	Default directory
Windows	All files	C:\Program Files\Seapine\License Server
Mac	Application	/Applications/Seapine License Server
	LSStartup.log file	/var/log
	Unix commands	/usr/bin
Linux	Application	/var/lib/splicsvr
	LSStartup.log file	/var/log
	Unix commands	/usr/bin

### Web server admin utility CGI and HTML file installation directories

If you are installing the Seapine License Server Web Admin Utility, you must set a location to install the CGI scripts and HTML files.

Microsoft IIS and Apache web servers are supported. See [Seapine License Server Supported Web Servers](http://www.seapine.com/kb/questions/1658) (www.seapine.com/kb/questions/1658) for supported versions.

Web server	Platform	Default CGI directory	Default HTML files directory
IIS	Windows	C:\inetpub\scripts	C:\inetpub\wwwroot
Apache	Windows	C:\Program Files\Apache Software Foundation\Apache <version>\cgi-bin	C:\Program Files\Apache Software Foundation\Apache <version>\htdocs
	Mac	/Library/WebServer/CGI-Executables	/Library/WebServer/Documents
	Linux	/var/www/cgi-bin	/var/www/html

## Server execution mode (Windows only)

You can choose to run the Seapine License Server as a service if you want the server to automatically start when the computer starts. If you run the server as an application, you must manually start the Seapine License Server application.

**Note:** The Seapine License Server supports single sign-on, which allows LDAP users to automatically log in to Seapine products using the same credentials used to log in to their computer. See the [Seapine License Server Admin Guide](http://downloads.seapine.com/pub/docs/licenseserveradmin.pdf) (<http://downloads.seapine.com/pub/docs/licenseserveradmin.pdf>) for more information.

## Server port

The Seapine License Server communicates with Surround SCM clients on this port. Use the default port number (5100) or enter another number.

## Setting CMIS Server configuration options

The Surround SCM CMIS Server is installed in the CMIS directory in the Surround SCM application directory by default. If you are only installing the CMIS Server, and installing it for the first time, you can specify the installation location and server port number during installation.

## Default installation directories

Installer	Files	Default directory
Windows	All files	C:\Program Files\Seapine\Surround SCM\CMIS
Mac	Application	/Applications/Surround SCM/CMIS
	Unix commands	/usr/bin
Linux	Application	/var/lib/Surround SCM/CMIS
	Unix commands	/usr/bin

## Server port

The Surround SCM CMIS Server communicates with CMIS clients on this port. Use the default port number (8080) or enter another number.

## Selecting RDBMS configuration options

Surround SCM data must be stored in an RDBMS database. If you do not have an existing RDBMS installation, you can install PostgreSQL during the Surround SCM installation. PostgreSQL is the default RDBMS type, but Oracle or SQL Server can also be used.

If you are using an existing RDBMS installation, create an empty database before running the Surround SCM installer so that you have the RDBMS connection information available.

## Installing PostgreSQL with Surround SCM

Following are the default PostgreSQL directories used by each installer.

Platform	Files	Default directory
Windows	Application and documentation files Databases, tables, and configuration files	C:\Program Files\PostgreSQL\ <version> C:\Program Files\PostgreSQL\<version>\data</version></version>
Mac	All files	/usr/local/pgsql
Linux	All files	/usr/local/pgsql

## Configuring PostgreSQL options

You must use the default host name and port number for PostgreSQL to install properly. The default host name is **localhost** and the default port number is **5432**.

**Note:** You can change the port number at a later time if other applications use port 5432. See the [Changing the PostgreSQL Port Number](http://www.seapine.com/kb/questions/1535) knowledgebase article (www.seapine.com/kb/questions/1535).

The default PostgreSQL database username is **seapine** and the database password is **s34p1n3**. We strongly recommend changing the database username and password during installation, but you can use PostgreSQL commands to change the credentials at a later time. Refer to the PostgreSQL documentation for information.

**Note:** The Surround SCM Server will automatically create tables in the empty database at startup.

The PostgreSQL service starts automatically the first time you start the Surround SCM Server. The service is also configured to start automatically when the server computer is restarted. During PostgreSQL installation, a new user is automatically created to start and stop the PostgreSQL service and manage the PostgreSQL data directory. The default username for the PostgreSQL service is **postgres** and the password is **P0stgreSQL**.

## Using Oracle, SQL Server, or existing PostgreSQL installations

If you choose to use an existing RDBMS service, you must manually install the database server and enter connection information for an empty UTF-8 encoded database before starting the Surround SCM Server. See [Setting Up RDBMS Databases](#), page 29.



# After Installing

After Surround SCM is installed, an administrator or another high-level user needs to perform the following tasks:

- Configure a Seapine License Server connection
- Add licenses and users to the Seapine License Server
- Configure a Surround SCM Server connection
- Configure a proxy server connection (optional)
- Configure the CMIS Server (optional)
- Configure WebDAV (optional)

**Note:** During installation, an administrative user with full admin security rights is created. To log in as this user, enter **Administrator** as the username and leave the password field empty. You can also delete this user and add a new admin user. If you do not want to delete this user, you should add a password to prevent unauthorized users from logging into the admin account.

## Starting the Seapine License Server

The Seapine License Server must be running before the Surround SCM Server is started.

- **Windows**—If you chose to run the license server as a service, it starts automatically. If you chose to run the license server as an application, you have to start it yourself. Choose **Programs > Seapine Software > Seapine License Server > Seapine License Server** from the Start menu.
- **Mac**—Click **Seapine License Server** in the System Preferences. If you want to set the server to start automatically, click the lock button and select **Start Seapine License Server when this computer starts up**.
- **Linux**—Enter `/usr/bin/spls start`

## Starting the Seapine License Server Admin Utility

The Seapine License Server Admin Utility provides a convenient way to manage global users and customers. Managing users and customers from one central location reduces the time spent on administrative tasks and allows you to quickly assign licenses.

- **Windows**—Choose **Programs > Seapine Software > Seapine License Server > Seapine License Server Admin** on the Start menu.
- **Mac**—Double-click the **Seapine License Server Admin Utility** icon in the Applications/Seapine License Server folder.
- **Linux**—Enter `/usr/bin/ladmin`
- **Web**—In a web browser, enter the server admin utility URL. The URL uses the static or IP address of the web server hosting the admin utility and the path to the admin utility files. For example, `http://www.yourserver.com/lweb/admin`.

## Configuring a Seapine License Server connection

Before you can access a server, you need to add the server connection information.

**Note:** Steps 1-6 may not be necessary if you installed the Surround SCM Server and the Seapine License Server on the same computer using the default port configurations.

1. Start the Seapine License Server and the Seapine License Server Admin Utility.
2. Click **Setup** on the Seapine License Server Login dialog box to add a server connection.
3. Click **Add** on the Setup Server Connections dialog box.
4. Enter a **Server Name**, **Server Address**, and **Port**.
5. Click **OK** to add the server connection.
6. Click **Close** in the Setup Server Connections dialog box to return to the Seapine License Server Login dialog box.
7. Log in as the default administrative user and click **Connect**. The username is **Administrator** and there is no password.

By default, the Administrator user has full admin security rights and uses a Surround SCM floating license. We strongly recommend setting a password for this user to prevent unauthorized user access.

## Adding licenses

1. Click **Licenses** on the License Server Admin Utility dialog box.
2. Click **Add** and enter the license serial number or click **Browse** to select a license file.  
This field is case sensitive. Licenses can be entered with or without dashes.
3. Click **OK** to add the license.

## Adding users

1. Click **Global Users** on the License Server Admin Utility dialog box and then click **Add**.
2. Enter the user's contact information, username and password, security rights, and licenses.
3. Click **Add** to add the user to the Global Users list.

**Note:** Global users can be shared by Surround SCM and TestTrack.

4. Close the Seapine License Server Admin Utility.

You are prompted to change the communications and Administrator passwords. We strongly recommend changing these passwords to prevent unauthorized user access.

## Starting the Surround SCM Server

- **Windows**—If you chose to run the Surround SCM Server as a service, it starts automatically. If you chose to run the server as an application, you have to start it yourself. Choose **Programs > Seapine Software > Surround SCM > Surround SCM Server** from the Start menu.
- **Mac**—Click **Surround SCM** in the System Preferences. If you want to set the server to start automatically, click the lock button and select **Start Surround SCM Server when this computer starts up**.
- **Linux**—Enter `/usr/bin/surroundscm start`

## Starting Surround SCM

- **Windows**—Choose **Programs > Seapine Software > Surround SCM > Surround SCM Client** on the Start menu.
- **Mac**—Double-click the **Surround SCM Client** icon in the Applications/Surround SCM folder.
- **Linux**—Enter `/usr/bin/scmgui start`

When Surround SCM starts, select the **Server** you want to connect to, enter a **Username** and **Password**, and click **Connect**.

## Configuring a Surround SCM Server connection

Make sure the Seapine License Server is running before you start the Surround SCM Server.

1. Start the Surround SCM Server and then start the Surround SCM Client.  
If the server does not start, see [Troubleshooting Server Issues, page 27](#).
2. Click **Setup** on the Surround SCM Login dialog box and click **Add** to configure a new server connection.
3. Enter a **Server Name**, **Server Address**, and **Server Port**.  
Enter a unique name, such as a product or department name, to help users identify the server. Surround SCM clients connect to the server on this port via TCP/IP. Valid values are 1-65535.
4. Click **OK**.
5. Log in as the administrative user and click **Connect**. The default username is **Administrator** and there is no password.  
By default, the Administrator user has full admin security rights and uses a Surround SCM floating license. We strongly recommend that you set a password for this user.

**Note:** If you are prompted to create a mainline branch, refer to the [Surround SCM User Guide](http://downloads.seapine.com/pub/docs/SurroundSCMUserguide.pdf) (<http://downloads.seapine.com/pub/docs/SurroundSCMUserguide.pdf>) for information.

## Configuring the proxy server

For security reasons, you must configure a master Surround SCM Server to accept connections from known Surround SCM proxy servers before attempting to use the proxy server. The installation and configuration of the proxy server requires information about both computers, and you must set the configuration options on both computers.

1. Start the Seapine License Server and the Surround SCM Server.
2. Start Surround SCM and log in using your existing admin username and password.
3. Choose **Tools > Administration > Proxy Maintenance** and click **Add**.
4. Enter the **Proxy name**, **Password**, **Proxy address**, and **Proxy port** for the proxy server.

Keep the following in mind:

- Use a unique server name such as the geographical location of the proxy server computer.
  - The password must match the password set on the proxy server.
  - The proxy address is the IP address or host address of the computer where the Surround SCM proxy server application is installed.
  - Surround SCM clients connect to the proxy server on this port via TCP/IP. The default port number is 4901. Valid values are 1-65535. The proxy server port must be different from the master server port if the servers are hosted on the same computer.
5. Optionally enter or select any additional proxy server options.
  6. Select the **Default proxy server users** and click **OK**.

If a user is added as a default proxy server user, they will automatically use the proxy server to retrieve files.

**Note:** You must restart the proxy server for the changes to take effect.

## Starting the proxy server

- **Windows**—If you chose to run the proxy server as a service, it starts automatically. If you chose to run the proxy server as an application, you have to start it yourself. Choose **Programs > Seapine Software > Surround SCM > Surround SCM Proxy Server** from the Start menu.
- **Mac**—Click **Surround SCM Proxy** in the System Preferences. If you want to set the server to start automatically, click the lock button and select **Start Surround SCM Proxy Server when this computer starts up**.
- **Linux**—Enter `/usr/bin/surroundscmproxy start`

## Starting the Surround SCM CMIS Server

- **Windows**—The Surround SCM CMIS Server is installed as a Windows service and starts automatically. If it is not running or you need to restart the server, refer to the Windows documentation for information about starting a service.

- **Mac**—Click **Surround SCM CMIS Server** in the System Preferences.
- **Linux**—Enter `/usr/bin/surroundscmcmis start`

## Starting the Surround SCM CMIS Admin Utility

- **Windows**—Choose **Programs > Seapine Software > Surround SCM > Surround SCM CMIS Admin Utility** on the Start menu.
- **Mac**—Double-click the **Surround SCM CMIS Admin Utility** icon in the Applications/Surround SCM/CMIS folder.
- **Linux**—Enter `/usr/bin/surroundscmcmisadmin`

## Configuring the Surround SCM CMIS Server

The Surround SCM Content Management Interoperability Services (CMIS) Server provides access to Surround SCM files and actions through CMIS clients, such as Adobe Drive and CMIS Workbench. CMIS repositories, which map to Surround SCM branches and repositories, must be configured on the Surround SCM CMIS Server before users can access Surround SCM from CMIS clients. You can manage CMIS repositories and change the server port number using the Surround SCM CMIS Admin Utility.

**Note:** Refer to the Surround SCM User Guide for additional information about managing and troubleshooting the CMIS Server.

1. Start the Surround SCM CMIS Server and Surround SCM Server if they are not running.
2. Start the Surround SCM CMIS Admin Utility.
3. Click **Add** to add a CMIS repository.
4. Enter the **Name**, Surround SCM Server **Address** and **Port** number, and **Surround SCM Repository** options for the CMIS repository and click **OK**.

Keep the following in mind:

- Adobe Drive only displays one CMIS repository when connected to the CMIS Server, even if the server contains multiple CMIS repositories. The repository that Adobe Drive users can browse is typically the repository listed first alphabetically on the server.
  - You can add CMIS repositories that map to a Surround SCM repository in a specific branch or to a Surround SCM repository in all branches.
  - The name you enter for the CMIS repository is displayed in CMIS clients. If the CMIS repository maps to a Surround SCM repository in all branches, the name and an underscore are prepended to the Surround SCM branch name to help users distinguish between different branches.
  - If you browse to a Surround SCM repository, you must log in to Surround SCM before selecting the repository to map the CMIS repository to.
5. Optionally add additional CMIS repositories.
  6. Optionally change the **Server port** number for CMIS clients to communicate to the CMIS Server on. The default number is 8080.
  7. Click **Save** to save the changes.

If you changed the server port number, you must restart the Surround SCM CMIS Server for the change to take effect. If you changed CMIS repository information, the server automatically refreshes Surround SCM data every 30 minutes, but you can restart the CMIS Server for the changes to take effect immediately.

**Note:** After the Surround SCM CMIS Server is configured, you must provide users with the server address before they can connect to it from CMIS clients. The default CMIS Server address is `ServerName:PortNumber/atom`. For example, `localhost:8080/atom`.

## Configuring web servers for WebDAV

Before you can use WebDAV with Surround SCM, you need to change the web server configuration to make sure that script execution is enabled for the directory that contains the WebDAV CGI and that users can log in. Configuration information is provided for the Apache and Microsoft Internet Information Services (IIS) web servers. See the web server documentation for more information about enabling CGI execution and authentication.

### Configuring Apache for WebDAV

1. Open the Apache configuration file. The file name is usually `httpd.conf`.
2. Find the `<Directory>` directive for the directory that contains the WebDAV CGI. For example, `C:/Program Files/Apache Group/Apache/cgi-bin`.
3. Add the following line to the directive to enable CGI execution for the directory:

```
Options +ExecCGI
```

4. Add the following lines to the directive to allow Windows to recognize the WebDAV CGI as a DAV provider:

```
Header set DAV "1, 2"
```

```
Header set MS-Author-Via DAV
```

**Note:** These settings require the Apache `mod_headers` module. Make sure you enable the following line in the configuration file:

```
LoadModule headers_module modules/mod_headers.so
```

5. Add the following lines to the directive to enable authentication:

```
RewriteEngine on
```

```
RewriteRule .* - [E=REMOTE_USER:%{HTTP:Authorization},L]
```

**Tip:** If you copy and paste the Rewrite Rule line into the directive, the spaces in the line may not be correct. We recommend typing the line to ensure the spacing is correct.

6. Save and close the configuration file.

**Note:** These settings require the Apache `mod_rewrite` module. Make sure you enable the following lines in the configuration file:

```
LoadModule rewrite_module modules/mod_rewrite.so
```

```
AddModule mod_rewrite.c
```

## Configuring Microsoft IIS 7 for WebDAV

Following are the steps required to configure IIS 7 on Windows Vista and Windows Server 2008 to host the Surround SCM WebDAV CGI.

### Enable support for CGI executables

#### Windows Vista

1. Choose **Start > Control Panel > Programs and Features**.
2. Click **Turn Windows features on or off** in the Tasks Pane.
3. Expand the **Internet Information Services, World Wide Web Services, and Application Development Features** nodes.
4. Select **CGI** and click **OK**.

#### Windows Server 2008

1. Choose **Start > Control Panel > Programs and Features**.
2. Click **Turn Windows features on or off** in the Tasks Pane.
3. Click **Roles** in the left pane and click **Add Role Services** in the right pane.
4. Expand the **Web Server and Application Development Features** nodes.
5. Select **CGI** and click **OK**.

### Add an application for the web site

1. Choose **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Connections pane, expand the **Web Sites** node.
3. Right-click the web site used for Surround SCM WebDAV and choose **Add Application**.
4. Enter 'Scripts' as the **Alias**, enter C:\inetpub\scripts as the **Physical Path**, and click **OK**.

### Enable the sscmdav CGI

1. In the Connections pane, select the server computer.
2. Double-click **ISAPI and CGI Restrictions**.
3. Click **Add** in the Actions pane and enter the path to the sscmdav.cgi file as the **ISAPI or CGI path**.  
This is the path entered for the sscmdav.cgi program during the Surround SCM installation. The default path is C:\inetpub\scripts.
4. Enter 'sscmdav' as the Description.
5. Select **Allow extension path to execute** and click **OK**.

## Add a module mapping between the CgiModule and sscmdav.cgi file

1. Open the IIS 7 configuration file in a text editor. Following is the configuration file location:  
C:\windows\System32\inetsrv\config\applicationHost.config
2. Add the following above the </configuration> tag, which is near the end of the file. Replace Default Web Site/Scripts/sscmdav.cgi with the actual path to the sscmdav.cgi file.

```
<location path="Default Web Site/Scripts/sscmdav.cgi">  
<system.webServer> <handlers> <clear /> <add name="sscmdav"  
path="sscmdav.cgi" verb="*" modules="CgiModule" resourceType="File"  
requireAccess="Execute" allowPathInfo="true" /> </handlers>  
</system.webServer> </location>
```

3. Save the file.

## Disable Windows authentication for sscmdav.cgi

### Disabling authentication for sscmdav.cgi at the server, web page, or application level

1. In the IIS Manager, select the server, web page, or application that includes sscmdav.cgi.
2. In the Features View, double-click **Authentication**.
3. Click **Windows Authentication**.
4. In the Actions pane, click **Disable**.

### Disabling Windows authentication for sscmdav.cgi at the URL level

1. Open the IIS 7 configuration file in a text editor.
2. Add the following immediately before the <handlers> tag:  

```
<security> <authentication> <windowsAuthentication enabled="false" />  
</authentication> </security>
```
3. Enter any additional security settings immediately after the <authentication> tag.
4. Save the file.

## Configuring Microsoft IIS 5 and 6 for WebDAV

1. On the Start menu, choose **Settings > Control Panel > Administrative Tools > Internet Information Services**.
2. Select the virtual directory that contains the WebDAV CGI and choose **Action > Properties**.
3. Select **Scripts and Executables** from the Execute Permissions list.
4. On the **Directory Security** tab, click Edit in the Anonymous access and authentication control area and clear the **Integrated Windows authentication** check box in the Authentication Control dialog box.
5. On the **Custom Errors** tab, select all of the errors and click **Set to Default**.
6. Click **OK** to close the Properties dialog box.

**Note:** The following steps are only required for IIS 6.

7. Expand the server node and select the **Web service extensions** node.
8. Click **Add a new Web service extension** in the Tasks section of the right pane.
9. Enter an **Extension name** and click **Add**.
10. Select **Set extension status to Allowed**.
11. Change the Files of Type field to **All Files**, browse to the location of the sscmdav.cgi file, and click **OK**.
12. Click **OK** again.

The sscmdav.cgi file is displayed in the Required Files section of the New Web Service Extension dialog box.

## Configuring WebDAV

You need to configure WebDAV to locate the Surround SCM Server, point to the branches and repositories, and optionally allow anonymous user access. Keep the following security options in mind when configuring WebDAV with Surround SCM:

- WebDAV access to Surround SCM repositories is controlled using Surround SCM security groups. Users can perform the same functions and access the same files using WebDAV as they can using Surround SCM. Unless anonymous user access is enabled, users must log in using their Surround SCM username and password to access a repository.
- The Login Via WebDAV server security command must be enabled to allow a security group to access repositories using WebDAV.
- You can allow anonymous user access to Surround SCM repositories. See [Configuring anonymous user access, page 22](#).

The WebDAV configuration is named sscmdav.xml, which is installed in the default Surround SCM application directory on Windows or in /etc/ on Mac and Linux.

The configuration file contains aliases, which are virtual directories that provide access to Surround SCM repositories. Each alias contains directories for the branches and repositories that you specify in the configuration file. You may want to provide access to all branches and repositories on a server or limit access to a specific branch and repository. You can configure several aliases to provide access to repositories and branches on one or more Surround SCM Servers. You can also configure access for anonymous users who do not have to log in.

**Note:** To move the configuration file from the default installation location, you must create a SSCMDAV\_CONFIG environment variable on the Surround SCM Server that includes the full path, including the file name, to the new location. Refer to your web server documentation for information about creating environment variables.

1. Open the sscmdav.xml configuration file and edit the existing attribute values with the following information:
  - **Alias**—Name of the virtual directory that contains Surround SCM branches and repositories.
  - **SCMServerAddress**—Surround SCM Server port number and IP address or domain name.

- **Branch**—Name of the branch to include. Use \* to include all branches.
- **Repository**—Name of the repository to include. Use \* to include all repositories.

**Tip:** If you include all repositories you must also include all branches and vice versa.

2. Optionally add the following elements if you specified \* to display all branches.
  - `<HideSnapshotBranches>1</HideSnapshotBranches>`—Hide snapshot branches.
  - `<ShowHiddenBranches>1</ShowHiddenBranches>`—Display hidden branches.
3. To add another alias directory, copy the entire Alias element and paste it directly above the `</SSCMDAV>` tag. Edit the attribute values as needed.

## Configuring anonymous user access

You can configure WebDAV to provide anonymous users access to Surround SCM repositories. For example, you may have consultants who are not Surround SCM users but need remote access to view files. You can add an anonymous user in Surround SCM, create a security group with limited access, and provide the username and password information in the configuration file to log in anonymous users automatically. See the [Surround SCM User Guide](http://downloads.seapine.com/pub/docs/SurroundSCMuserguide.pdf) (<http://downloads.seapine.com/pub/docs/SurroundSCMuserguide.pdf>) for information on adding users and security groups.

1. Add a new Surround SCM user, then add a security group and add the new user to the group.  
For example, create a new security group named Anonymous Web. Enable only the Login Via WebDAV, View Repository List, and Get File server security commands to ensure that anonymous users cannot modify files.
2. Open the `sscmdav.xml` configuration file in the default Surround SCM directory or another location.
3. Add the following line after the `</Repository>` tag and enter the username and password for the new anonymous user.  

```
<Anonymous user="username" password="password"></Anonymous>
```
4. Save then close the configuration file.
5. Open the alias directory to make sure you can open it without logging in.

## Configuring text file end-of-line format

WebDAV returns text files using the application's default end-of-line termination format. To change the format, add the following element to the WebDAV configuration file:

```
<TextEOLFormat>format</TextEOLFormat>
```

Enter one of the following values to specify the format:

- **AutoDetect-Default**—Auto-detect or use the format of the computer that contains the WebDAV CGI. For example, if the CGI is on a Windows computer, Windows format is used.
- **AutoDetect-Windows**—Auto-detect or use Windows format.
- **AutoDetect-Unix**—Auto-detect or use Unix format.
- **AutoDetect-MacOS9**—Auto-detect or use Mac OS 9 format.

- Always-Windows—Always use Windows format.
- Always-Unix—Always use Unix format.
- Always-MacOS9—Always use Mac OS 9 format.

## Configuration example

The first alias is WysiCorp Products. This alias directory provides access to all branches and all repositories on the specified Surround SCM Server. Users must log in to view the repositories in the alias directory. They can only access commands and repositories enabled for their security group.

The second alias is WysiChart Documentation. This alias directory provides access to the repository with the following path in the WysiChart 1.0 branch: WysiCorp Product/WysiChart/Documentation/PDFs. Any user can access this repository without logging in because anonymous access is enabled.

```
<SSCMDAV>
<Alias name="WysiCorp Products">
<SCMServerAddress port="4900">127.0.0.1</SCMServerAddress>
<Branch>*</Branch>
<Repository>*</Repository>
</Alias>
<Alias name="WysiChart 1.0 Documentation">
<SCMServerAddress port="4900">127.0.0.1</SCMServerAddress>
<Branch>WysiChart 1.0</Branch>
<Repository>WysiCorp Products/WysiChart/Documentation/PDFs</Repository>
<Anonymous user="Anonymous" password="a12345"></Anonymous>
</Alias>
</SSCMDAV>
```

## Configuring web servers for the Seapine License Server Web Admin Utility

The Seapine License Server Web Admin Utility requires a web server to host the HTML files and execute the CGI scripts. The CGI scripts connect to the Seapine License Server using a TCP/IP connection.

The Seapine License Server web components can be installed during Surround SCM installation. After installation, you need to configure the web server before administrators can log in using the web admin utility.

See the [Seapine License Server Supported Web Servers](http://www.seapine.com/kb/questions/1658) knowledgebase article (www.seapine.com/kb/questions/1658) for a list of supported web servers.

## Configuring Apache for the license server admin utility

You must create a CGI directory alias on the Apache web server before administrators can log in to the Seapine License Server Web Server Admin Utility.

1. Open the httpd.conf file.
2. Search the file for `ScriptAlias/cgi-bin`.

If the directory does not exist, add the following to the file:

```
ScriptAlias/cgi-bin/"C:\Program Files\Apache Group/cgi-bin/"
```

## Configuring Microsoft IIS 7 for the license server admin utility

After you install the Seapine License Server Web Admin Utility files, you need to configure the web server before administrators can log in to the admin utility.

Refer to the IIS documentation for information about enabling CGI execution and authentication.

## Enabling support for CGI executables

### Windows Vista and Windows 7

1. Choose **Start > Control Panel > Programs and Features**.
2. Click **Turn Windows features on or off** in the Tasks pane.
3. Expand the **Internet Information Services, World Wide Web Services, and Application Development Features** nodes.
4. Select **CGI**.
5. Click **OK**.

### Windows Server 2008

1. Choose **Start > Control Panel > Programs and Features**.
2. Click **Turn Windows features on or off** in the Tasks pane.
3. Click **Roles** in the left pane.
4. Click **Add Role Services** in the right pane.
5. Expand the **Web Server** and **Application Development Features** nodes.
6. Select **CGI**.
7. Click **OK**.

## Creating a CGI directory alias

1. Open IIS Manager.
2. In the Connections pane, expand the **Web Sites** node.
3. Right-click the default web site or the site used for the Seapine License Server Web Admin Utility and choose **Add Virtual Directory**.

4. Enter 'scripts' as the **Alias**.
5. Enter the path to the Iscgi.exe as the **Physical Path**. This is the path entered during the admin utility installation. The default path is C:\inetpub\scripts.
6. Click **OK**.

## Enabling the .exe CGI extension

1. Click the scripts virtual directory in the Connections pane.
2. Double-click **Handler Mappings**.
3. Click **Add Module Mapping** in the Actions pane.
4. Enter '\*.exe' as the **Request path**.
5. Select CgiModule as the **Module**.
6. Enter 'Iscgi' as the **Name**.
7. Click **OK**.
8. Select the server computer in the Connections pane.
9. Double-click **ISAPI and CGI Restrictions**.
10. Click **Add** in the Actions pane.
11. Enter the path to the Iscgi.exe program as the **ISAPI or CGI path**. This is the path entered for the Iscgi.exe program during the admin utility installation. The default path is C:\inetpub\scripts\Iscgi.exe.
12. Enter 'Iscgi' as the **Description**.
13. Select **Allow extension path to execute**.
14. Click **OK**.

## Configuring Microsoft IIS 5 and 6 for the license server admin utility

After you install the Seapine License Server Web Admin Utility files, you need to configure the web server before administrators can log in to the admin utility.

Refer to the IIS documentation for information about enabling CGI execution and authentication.

## Creating a CGI directory alias

1. Open IIS Manager.
2. Right-click the default web site or the site used for the Seapine License Server Web Server Admin Utility and choose **New > Virtual Directory**.
3. Follow the on-screen instructions. Enter the following information when prompted:
  - Enter 'scripts' as the **Alias**.

- Set the **Directory** to the path that was entered during the admin utility installation for the Iscgi.exe program. The default path is C:\inetpub\scripts.
- Select the following **Access Permissions**: Read, Run scripts, Execute.

## Enabling the .exe CGI extension

The following steps are only required for IIS 6.

1. In IIS Manager, expand **Web Sites** and click **Web Service Extensions**.
2. Click **Add a new Web service extension** in the Web Service Extensions pane.
3. Enter 'LSAdmin' as the **Extension name**.
4. Click **Add**.
5. Enter the path to the Iscgi.exe program and click **OK**. The default location is C:\inetpub\scripts\Iscgi.exe.
6. Select **Set extension status to Allowed**.
7. Click **OK**.
8. Click **OK** to save the changes.

# Troubleshooting Server Issues

If there is a problem connecting to the Surround SCM Server or the Seapine License Server, first check the following and try reconnecting:

- Make sure the server computer is running
- Check the IP address and port number
- Make sure you are connected to the network, intranet, or Internet

## The Seapine License Server and Surround SCM Server are not communicating

If the servers are not communicating, make sure the connections are configured correctly.

1. Start the Seapine License Server and the Surround SCM Server.
2. Start Surround SCM and log in using your existing admin username and password.  
Use the local SCM admin password to log in if your username and password are not recognized. Leave the username blank and enter **admin** as the password. This password only provides access to the Seapine License Server configuration.
3. Choose **Tools > Administration > Server Options** and select the **License Server** category.
4. Make sure the server address and port number are both correct and click **Test Connection**.
5. If the connection is successful, stop and restart the Surround SCM Server for the changes to take effect.
6. If the connection is not successful, check the following:
  - If the Surround SCM Server and the Seapine License Server are installed on different computers, check your network and firewall configurations to open the necessary ports.
  - Check the Surround SCM Server and Seapine License Server address and port number.
  - Check the communications password on the Seapine License Server and the Surround SCM Server. You can set a communications password that requires the Surround SCM Server and the Seapine License Server to use the same password to communicate with each other.

To check the password in Surround SCM, choose **Tools > Administration > Server Options**, then select the **License Server** category. To check the password in the Seapine License Server Admin Utility, click **Server Options**, then select the **Server** category.

## The proxy server does not start

If the proxy server does not start, check the SCMPProxyStartup.log file for error messages (the log is located in the Surround SCM application directory on Windows or \var\log on Linux and Mac OS X).

Following are some common reasons why the proxy server may not start:

- The proxy server does not have read/write permissions for the proxy cache directory and its files. Check the permissions and make sure they are set to read/write.

- The master Surround SCM Server rejects the connection because the Proxy Name and Password are incorrect. See 'Configuring proxy servers' in the Surround SCM User Guide for additional information.

## The Surround SCM Server cannot find the server database

If the Surround SCM Server cannot find the server database, make sure the connection to the RDBMS server is configured correctly.

1. Start the Surround SCM Server and RDBMS server hosting the server database.
2. Log in to the Surround SCM Client and click **Yes** when you are prompted to configure the server database location.
3. Make sure the connection information is correct and click **Test**.
4. If the connection is successful, stop and restart the Surround SCM Server for the changes to take effect.
5. If the connection is not successful, check the following:
  - If the Surround SCM Server and database are installed on different computers, check the network and firewall configurations to open the necessary ports.
  - Make sure the connection information is correct. See [Troubleshooting RDBMS connections, page 1](#).

# Setting Up RDBMS Databases

The Surround SCM Server database and mainline databases are stored in a Relational Database Management System (RDBMS). The default RDBMS is PostgreSQL, but you can also use ODBC (Microsoft SQL Server) or Oracle .

PostgreSQL is supported out of the box. If you use Oracle or SQL Server, review the following information for help setting up databases. Information about supported platforms and databases is provided in the [Surround SCM RDBMS Support](http://www.seapine.com/kb/questions/1497) knowledgebase article ([www.seapine.com/kb/questions/1497](http://www.seapine.com/kb/questions/1497)).

**Note:** You can also use an RDBMS for the Seapine License Server database. See the [Seapine License Server Admin Guide](http://downloads.seapine.com/pub/docs/licenseserveradmin.pdf) (<http://downloads.seapine.com/pub/docs/licenseserveradmin.pdf>) for information about setting up license server databases.

## Setting up PostgreSQL databases

The Surround SCM installer allows you to easily install the PostgreSQL database services and create a supported RDBMS server database. Seapine does not provide support for configuring or maintaining PostgreSQL. If you do not install PostgreSQL during the Surround SCM installation, a qualified PostgreSQL database administrator should configure the PostgreSQL database.

Keep the following in mind:

- Do not add, delete, or modify any fields in the Surround SCM tables.
- Do not directly add, edit, or delete any data in the tables.
- Do not create different primary keys. This will adversely affect application performance.
- Do not create complex triggers on any of the tables. Triggers may cause severe database issues and correcting these issues is not covered by Seapine Software.
- Create a process to back up database tables on a regular schedule.
- Running PostgreSQL and the Surround SCM Server on the same computer can result in slow performance if not configured properly. Make sure PostgreSQL is properly configured to avoid using all the system memory.

## Connecting to PostgreSQL

The Surround SCM Server uses the server connection information provided during installation to connect to the PostgreSQL database. You can also enter the server connection information after installation. When you first start the Surround SCM Server and Client, you are prompted to configure the database location. You must restart the Surround SCM Server and Client after configuring the server database connection.

**Note:** If no tables are found in the database you specify, you are also prompted to allow the Surround SCM Server to create them. Decline this prompt if you are using a Surround SCM 2008 or earlier server database. When you restart the Surround SCM Server, it automatically upgrades the old server database.

## Creating and upgrading server databases

During Surround SCM installation, you are prompted to enter database connection information. All the required information is automatically created and entered if you install PostgreSQL with Surround SCM. If PostgreSQL is already installed, create an empty UTF-8 encoded database, username, and password so you can enter the connection information during installation.

The Surround SCM Server connects to the server database at startup and checks for the required PostgreSQL tables. If no tables are found, the Surround SCM Server automatically creates them. The SCMServerDB.sql script file, which is located in the PostgreSQL directory in the Surround SCM application directory, is used to create the tables.

If you are upgrading to Surround SCM 2009 or later, the Surround SCM Server upgrades native Surround SCM databases to RDBMS format when it is started after installation.

## Setting up Oracle databases

Seapine does not provide support for installing, configuring, or maintaining Oracle. A qualified Oracle database administrator should install and configure the database and create the necessary schemas and tablespaces.

Keep the following in mind:

- Do not add, delete, or modify any fields in the Surround SCM tables.
- Do not directly add, edit, or delete any data in the tables.
- Do not create different primary keys. This will adversely affect application performance.
- Do not create complex triggers on any of the tables. Triggers may cause severe database issues and correcting these issues is not covered by Seapine Software.
- Create a process to back up database tables on a regular schedule.
- Running Oracle and the Surround SCM Server on the same computer can result in slow performance if not configured properly. Make sure Oracle is properly configured to avoid using all the system memory.

## Connecting to Oracle

The recommended method for using Oracle is via Oracle Call Interface (OCI). A separate installer that includes the required Oracle Instant Client libraries can be downloaded from Seapine's web site.

- Windows—<http://downloads.seapine.com/pub/software/OracleInstantClientInstaller.exe>
- Mac OS X—<http://downloads.seapine.com/pub/software/oraclemacosjavainstall.zip>
- Linux—<http://downloads.seapine.com/pub/software/oraclelinuxjavainstall.tar.gz>

## Creating database tables

The Surround SCM Server automatically creates tables when you start the server or convert the server database. The SCMServer.sql script file, which is located in the Oracle directory in the Surround SCM application directory, is used to create the tables.

## Creating Oracle users

You must create an Oracle user for the Surround SCM Server. The user only requires default connection privileges and should not have any Oracle DBA privileges. Use your preferred tablespace management for the users. An easy method is to set up the user to share the USERS tablespace and to enable an unlimited quota.

## Database character set

Oracle only converts characters when the Oracle client's character set, specified by `NLS_LANG`, does not match the character set stored in the database. If the character set is not UTF-8, VARCHAR2 fields may not be able to correctly store data. If this happens, the following misnomer of an error is returned: 'ORA-01461: can bind a LONG value only for insert into a LONG column'. The Oracle database character set should be AL32UTF8 or UTF8.

## Sizing, memory, and tuning

Oracle sizing and tuning settings should be consistent with your corporate standards. Review the SQL scripts for schema creation installed with Surround SCM Server to determine the appropriate settings.

## Setting up SQL Server databases

Seapine does not provide support for installing, configuring, or maintaining SQL Server. A qualified SQL Server database administrator should install and configure the database.

Keep the following in mind:

- Do not add, delete, or modify any fields in the Surround SCM tables.
- Do not directly add, edit, or delete any data in the tables.
- Do not create different primary keys. This will adversely affect application performance.
- Do not create complex triggers on any of the tables. Triggers may cause severe database issues and correcting these issues is not covered by Seapine Software.
- Create a process to back up database tables on a regular schedule.
- Running SQL Server and the Surround SCM Server on the same computer can result in slow performance if not configured properly. Make sure SQL Server is properly configured to avoid using all the system memory.

**Note:** You must be a member of the `db_ddladmin` role and have the `CREATE TABLE`, `CREATE PROCEDURE`, and `CREATE VIEW` permissions to create the Surround SCM tables.

## Connecting to SQL Server

The only supported method for using SQL Server is via an ODBC connection. Use the ODBC Data Source Administrator to add a SQL Server data source name (DSN) on the Surround SCM computer.

- SQL Server must contain a Surround SCM database before you create the DSN.
- You must use a system DSN.

- Make sure you change the default database to the Surround SCM database. Do not use the master database.
- Make sure the **Use ANSI quoted identifiers, ANSI nulls, padding, and warnings, and Perform translation for character data** options are selected.

## Creating server database tables

The Surround SCM Server automatically creates tables when you start the server or convert the server database. The SCMServer.sql script file, which is located in the SQLServer directory in the Surround SCM application directory, is used to create the tables.

## Troubleshooting RDBMS connections

The following information can help you troubleshoot common RDBMS issues. Refer to the database vendor documentation for additional help.

**Note:** If the Surround SCM Server cannot connect to the server database, errors are added to the SCMSStartup.log file in the Surround SCM application directory.

### Server database cannot be shared

The Seapine License Server, Surround SCM Server, and TestTrack Server store server configuration information in a server database. The server databases cannot be located in the same RDBMS database.

### Dropped tables or change database configuration

You must stop and restart the Surround SCM Server if you drop server or tables from an RDBMS and need to re-create them. You must also stop and restart the server if you reconfigure the destination database in the ODBC Data Source Administrator.

The Surround SCM Server caches data from the database. If the underlying database is modified, the cached data no longer matches the data in the database. The connection fails if the server identifies that the backend database is different and the following error is logged: 'The server failed to initialize a connection for XYZ. The destination RDBMS database was changed'.

### Mismatched UUID affects server database lock

This error occurs when the database is in use by a different Surround SCM Server. You are prompted to reconfigure the database. Do not reconfigure the database if it is used on a different computer. You must manually modify the Surround SCM Server connection information to point to a different database and restart the server. If the database is no longer in use by a different server, reconfigure the database connection information to allow the current Surround SCM Server access to the database.

### ODBC connection issues

Try the following if you are experiencing ODBC connection problems.

1. Test the ODBC connection in the ODBC Data Source Administrator.

If you cannot connect to the RDBMS, click the Test Connection button in the ODBC Data Source Administrator to test the connection.

2. Make sure the DSN is a system DSN.

The data source you are trying to connect to must be configured as a system DSN in the ODBC Data Source Administrator. Surround SCM only displays system DSNs.

## ODBC connection errors

Error	Cause
[Microsoft][ODBC Driver Manager] Data source name not found and no default driver specified QODBC3: Unable to connect	An ODBC data source with the specified DSN was not set up in the ODBC Data Source Administrator. The DSN must be a system DSN.

## SQL Server connection errors

Error	Cause
[Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user '(null)'. Reason: Not associated with a trusted SQL Server connection. QODBC3: Unable to connect	Occurs on Windows. A username is not specified for the RDBMS connection and the ODBC data source was not configured to run 'With Windows NT authentication using the network login ID' in the ODBC Data Source Administrator.
[Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'xxxx'. QODBC3: Unable to connect	The username or password entered in the RDBMS connection information is not valid.

## Oracle connection errors

Error	Cause
ORA-06401: NETCMN: invalid driver designator QOCI: Unable to logon	The Oracle Instant client drivers are not installed. See <a href="#">Setting up Oracle databases, page 30</a> for information about downloading the installers.

Error	Cause
<p>ORA-12705: invalid or unknown NLS parameter value specified QOCI: Unable to logon</p>	<p>The full Oracle client is installed on the same computer with a language setting other than UTF8. To resolve this issue, set the following environment variable:</p> <ul style="list-style-type: none"> <li>■ Windows—NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252</li> <li>■ Linux and Mac OS X—NLS_LANG=American_America.UTF8</li> </ul> <p>You can also remove the following registry entry to help resolve the issue: HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\NLS_LANG</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Refer to Oracle Metalink article 179133.1, “The Correct NLS_LANG in a Windows Environment,” for information about the correct setting, which varies based on the Windows version.</p> </div>
<p>ORA-12514: TNS:listener does not currently know of service requested in connect descriptor QOCI: Unable to logon</p>	<p>The service name specified in the RDBMS connection information does not exist. Make sure that an Oracle listener was created with the specified service name on the host computer.</p> <p>This error can also occur if a version of the full Oracle client older than 10g is installed. If the full client appears in the PATH environment variable, the older oci.dll may be loaded. To resolve this issue, search for all instances of the oci.dll file. If multiple copies are found, remove the other copies or remove their directory reference from the PATH environment variable.</p>
<p>ORA-12154: TNS:could not resolve the connect identifier specified QOCI: Unable to logon</p>	<p>The computer specified in the RDBMS connection host name cannot be found. Make sure the host name is correct and the host computer is running.</p>
<p>ORA-12541: TNS:no listener QOCI: Unable to logon</p>	<p>The port number specified in the RDBMS connection information is not a valid TNS listener port on the specified host computer. Check the host port number.</p>
<p>ORA-01017: invalid username/password; logon denied QOCI: Unable to logon</p>	<p>The username or password specified in the RDBMS connection information is not valid. Check the username and password.</p>

## PostgreSQL connection errors

Error	Cause
Opening the database connection failed because the Surround SCM Server could not connect to the server or translate the host name	<p>The Surround SCM Server cannot connect to the PostgreSQL service. Check the following and then restart the server:</p> <ul style="list-style-type: none"><li>■ The PostgreSQL service is running.</li><li>■ The host name and port number are correct.</li><li>■ A firewall is not blocking the port.</li><li>■ If connecting to a remote PostgreSQL server, the server is configured to accept remote connections.</li></ul>



# Appendix A: Third-Party Software Licenses

## OpenSSL license

The following license information pertains specifically to the OpenSSL toolkit.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

## OpenSSL license

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

## Original SSLeay license

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

## Qt LGPL License

Surround SCM uses the Qt library covered by version 2.1 of the GNU Lesser General Public License (LGPL). A copy of the Qt LGPL license is available in the Qt License.txt file in the Surround SCM application directory. Source code for the Qt libraries is available in the [Qt LGPL Source Code Archives](#) knowledgebase article ([www.seapine.com/kb/questions/1550](http://www.seapine.com/kb/questions/1550)).



# Index

<b>A</b>			
After installing	13		
<b>B</b>			
Backing up databases	1		
<b>C</b>			
CMIS Admin Utility			
starting	17		
CMIS Server			
changing port number	17		
configuration options	10		
configuring	17		
server address	18		
starting	16		
<b>D</b>			
Databases	1		
backing up	1		
Oracle	30		
PostgreSQL	29		
RDBMS information	3		
SQL Server	31		
<b>I</b>			
Installation directories			
CMIS Server default	10		
PostgreSQL default	11		
Seapine License Server CGI and HTML files	9		
Seapine License Server default	9		
Surround SCM default	8		
Installation types	4		
Installing Surround SCM			
before you install	3		
downloading installers	5		
running installers	7		
upgrade installations	1		
Integration options	7		
<b>L</b>			
Licenses			
adding	14		
Login			
PostgreSQL default	11		
Seapine License Server default	14		
Surround SCM default	15		
<b>M</b>			
Mainline branches			
databases	1		
<b>N</b>			
New installation			
adding licenses	14		
adding users	14		
configuring license server connection	14		
configuring Surround SCM Server connection	15		
<b>O</b>			
ODBC			
connection errors	33		
connection issues	32		
Oracle			
connecting to	30		
connection errors	33		
creating server database tables	30		
creating users	31		
database character set	31		
instant client libraries (OCI)	30		
setting up	30		
sizing, memory, and tuning	31		
<b>P</b>			
PostgreSQL			
connection errors	35		
default connection information	11		
default installation directories	11		

server database tables	30	Server port number	
setting up	29	CMIS Server	10
Proxy server		Seapine License Server	10
starting	16	Surround SCM Server	8
<b>R</b>		SQL Server	
RDBMS configuration options	10	connecting to	31
existing PostgreSQL installation	11	connection errors	33
Oracle	11	creating server database tables	32
PostgreSQL	11	setting up	31
SQL Server	11	Starting	
RDBMS connections		CMIS Admin Utility	17
changed database configuration	32	CMIS Server	16
dropped tables	32	proxy server	16
exclusive lock	32	Seapine License Server	13
mismatched UUID	32	Seapine License Server Admin Utility	13
server database cannot be shared	32	Surround SCM	15
troubleshooting	32	Surround SCM Server	15
Running the installer	7	Surround SCM	
<b>S</b>		configuration options	7
Seapine License Server		default login	15
configuration options	9	starting	15
configuring connection	14	Surround SCM Server	
default login	14	64-bit server	2
starting	13	RDBMS database information	3
Seapine License Server Admin Utility		server database	1
configuring web servers		starting	15
Apache	24	System requirements	3
IIS 5 and 6	25	<b>T</b>	
IIS 7	24	Troubleshooting	
starting	13	proxy server does not start	27
URL	13	RDBMS connections	32
Server database tables		server database not found	28
Oracle	30	servers not communicating	27
SQL Server	32	<b>U</b>	
Server execution mode		Upgrading	
Seapine License Server	10	Surround SCM	1
Surround SCM server	8	URL for license server admin utility	13

Users	
adding	14
<b>W</b>	
WebDAV	
anonymous user access	22
CGI configuration options	8
configuring	21
configuring web servers	18
Apache	18
Microsoft IIS 5 and 6	20
Microsoft IIS 7	19
end-of-line format	22