



Seapine License Server

Admin 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 registered trademarks of Red Hat, Inc. in the United States and other countries.

SUSE is a 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

Contents

Getting Started	1
Installing the license server and server admin utility.....	1
About the 64-bit license server.....	1
Starting the Seapine License Server.....	2
Starting the Seapine License Server Admin Utility.....	2
Adding server connections.....	3
Editing server connections.....	3
Finding servers.....	4
Connecting to a different server.....	4
Deleting server connections.....	4
Generating support diagnostic reports.....	5
Configuring Server Options	7
Setting server log options.....	7
Setting server options.....	8
Configuring the server database.....	9
Automatically creating Seapine License Server tables.....	13
Setting password options.....	13
Setting LDAP options.....	15
Managing Licenses	23
Adding licenses.....	23
Configuring license pools.....	24
Assigning licenses.....	27
Associating users with named licenses.....	28
Viewing used licenses.....	28
Viewing license counts.....	29
Viewing license details.....	30
Deleting licenses.....	30
Managing Global Users	31
Customizing the Global Users list.....	31
Adding users.....	32
Adding LDAP users.....	34
Viewing users.....	35
Editing users.....	35
Changing usernames.....	36

Re-syncing LDAP users.....	36
Inactivating users.....	36
Activating users.....	37
Unlocking users.....	37
Exporting user information.....	38
Importing user information.....	39
Deleting users.....	39
Undeleting users.....	39
Printing the global users list.....	40
Changing bulk user fields.....	40
Using Single Sign-On.....	45
Single sign-on requirements.....	45
Configuring single sign-on for LDAP servers.....	45
Enabling single sign-on for users.....	46
Disabling single sign-on for users.....	46
Managing the Server Log.....	47
Viewing the server log.....	47
Exporting the server log.....	48
Deleting all log entries.....	48
Deleting log entries by date.....	48
Setting Up RDBMS Databases.....	49
Setting up PostgreSQL databases.....	49
Setting up Oracle databases.....	49
Setting up SQL Server databases.....	50
Troubleshooting RDBMS connections.....	51
Using the Seapine License Server API.....	55
Appendix A: LDAP Authentication.....	57
Appendix B: Third-Party Software Licenses.....	59
Index.....	65

Getting Started

The client/server Seapine License Server stores license, user, and customer information on one networked computer. You must have a Seapine License Server running on your network that other Seapine products can access.

The Seapine License Server Admin Utility is used to perform the following tasks:

- Manage licenses
- Manage global users and customers
- Configure LDAP or Active Directory server support
- Manage license server options
- View and manage the server log
- Manage license server admin security

Installing the license server and server admin utility

The Seapine License Server and Seapine License Server Admin Utility are installed when you install Seapine products. If you did not install the license server components, rerun the installer and select an installation type that includes the license server and admin utility.

Note: A web-based license server admin utility is also available. After installing the web admin utility, you must perform additional configuration on the web server that hosts the admin utility. See the Surround SCM or TestTrack Installation Guide for information.

If you are upgrading Seapine products, always install the license server and admin utility. The license server is backward compatible. It supports the Seapine product versions it is installed with and earlier versions, but not later versions. To view the supported versions for the installed license server, choose **Help > About License Server** in the admin utility.

Note: Licenses, users, and customers cannot be shared between license servers. Do not install and use multiple license servers unless you are sure the licenses, users, and customers will not be shared. For example, your company may have stringent security requirements. Each department functions separately and cannot share information because of legal or auditing reasons. In this case, each department runs and maintains a separate license server with its own set of licenses, users, and customers.

About the 64-bit license server

The 64-bit version of the Seapine License Server is packaged in the 64-bit TestTrack Server and 64-bit Surround SCM Server installers.

- 32-bit TestTrack and Surround SCM clients and the 32-bit Seapine License Server Admin Utility can communicate with the 64-bit Seapine License Server and vice versa.

- The 64-bit license server has different system requirements than the 32-bit server. Make sure the server computer meets the recommended system requirements. See the [Seapine License Server System Requirements](http://www.seapine.com/kb/questions/1613) (www.seapine.com/kb/questions/1613).

New installations

If you are performing a new 64-bit license server installation, a SQLite server database is created automatically the first time you start the license server. You can configure the server database to use a different RDBMS. See [Setting Up RDBMS Databases, page 49](#) and [Configuring the server database, page 9](#).

Upgrade installations

If you are upgrading from the 32-bit Seapine License Server, you must perform the steps in the [Migrating from the 32-bit Seapine License Server to the 64-bit Seapine License Server on the Same Computer](http://www.seapine.com/kb/questions/1612) knowledgebase article (www.seapine.com/kb/questions/1612).

Starting the Seapine License Server

The Seapine License Server must be started before the Seapine server applications. If users cannot connect to the server, make sure the server computer is online, the Seapine License Server application is running, and the IP address and port number are correct.

- **Windows**—If the Seapine License Server is installed as an application, choose **Programs > Seapine Software > Seapine License Server > Seapine License Server** on the Start menu.

Note: If the license server is installed as a service, it starts automatically. If it does not start, refer to the Windows documentation for help.

- **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

You need to add licenses and users the first time you start the Seapine License Server and admin utility. See [Adding licenses, page 23](#) and [Adding users, page 32](#).

Note: An administrative user is created during installation. Log in as this user the first time you start the admin utility. The username is **Administrator** and there is no password. To prevent unauthorized access, create a password for this user after you log in.

1. **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`

The Seapine License Server Login dialog box opens.

2. Select the **Server** you want to connect to. See [Adding server connections, page 3](#) if you need to add a server.
3. Enter a **Username** and **Password** or select **Use single sign-on** to log in using the workstation credentials.

Note: Single sign-on must be enabled. Single-sign on is only available for Windows and Mac.

4. Select **Always login with this username and password** to automatically log in with the credentials you entered when the admin utility starts.
5. Click **Connect**.

The admin utility starts.

Adding server connections

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

1. Choose **File > Connect to Server** to open the login dialog box.
2. Click **Setup**.

The Setup Server Connections dialog box opens.

3. Click **Add**.

The Add License Server dialog box opens.

4. Enter a **Server Name**.

Use a name that uniquely identifies the server. For example, Satellite Office.

5. Enter the **Server Address** of the computer where the license server is installed.
6. Enter server computer **Port** number.

Clients connect to the license server via TCP/IP on this port. The default value is 5100. Valid values are 1-65535.

7. Click **OK**.

The server is added.

Note: You may want to move the servers you log in to most frequently to the top of the list. To reorder the servers, select a server and click Top, Move Up, Move Down, or Bottom.

Editing server connections

1. Choose **File > Connect to Server** to open the login dialog box.
2. Click **Setup**.

The Setup Server Connections dialog box opens.

3. Select the server you want to edit and click **Edit**.

The Edit License Server dialog box opens.

4. Make any changes.

5. Click **OK** to save the changes.

Finding servers

You can quickly find all Seapine License Servers on the network.

1. Choose **File > Connect to Server** to open the login dialog box.
2. Click **Setup**.

The Setup Server Connections dialog box opens.

3. Click **Find**.

The Available License Servers dialog box opens when the search is complete. All available license servers are displayed.

Note: Select **Include IPv6 in scan** to find servers hosted on IPv6 computers.

4. Select a server and click **Add**.

The Add License Server dialog box opens.

5. Enter a unique **Server Name**.

Note: The Server Address and Port fields are read-only and cannot be changed.

6. Click **OK**.

The server is added.

Connecting to a different server

You can connect to a different license server without closing the admin utility.

1. Choose **File > Connect to Server**.

The login dialog box opens.

2. Select the server you want to connect to and click **Connect**.

Deleting server connections

1. Choose **File > Connect to Server** to open the login dialog box.

2. Click **Setup**.

The Setup Server Connections dialog box opens.

3. Select the server you want to delete and click **Delete**.

You are prompted to confirm the deletion.

4. Click **Yes** to delete the server.

Generating support diagnostic reports

If you are experiencing license server issues and need help from Seapine support, you can generate a report that includes detailed information about the license server configuration. You can then email the report to Seapine support to provide information for troubleshooting the issue.

1. Choose **Help > Generate Support File**.

The Generate Support File dialog box opens.

2. Click **Save As** to save the file.

The Save As dialog box opens.

3. Select a **Save in** location and enter a **File name**.

The default file name is SeapineSupportDiagnostics.txt.

4. Click **Save**.
5. Click **Close**.

Configuring Server Options

You can configure various Seapine License Server options including log levels, password options, the database type, and LDAP options.

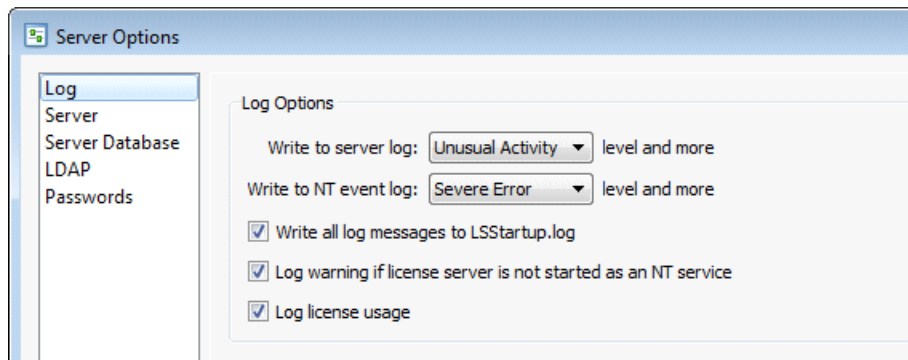
Setting server log options

The license server creates log files that record events, such as severe errors or unusual activity, and help you monitor the server's operation. See [Viewing the server log, page 47](#).

1. Choose **View > Server Options**.

The Server Options dialog box opens.

2. Select the **Log** category.



3. Select a **Write to server log** level to specify the types of events written to the log. See [Server log levels, page 8](#).

4. Select a **Write to NT event log** or **Write to Unix system log** level.

This option, which is named based on the operating system the license server is running on, specifies the types of events written to the event or system log.

5. Select **Write all log messages to LSStartup.log** to write all messages to the log file.

Select this option if you are experiencing server problems and want to log messages that occur after startup. The LSStartup.log file is generally stored in the same directory as the Seapine License Server executable on Windows and in `/var/log` on Unix. You can email the log file to Seapine support for help resolving the problem.

Note: Startup errors are always logged to the LSStartup.log file.

6. Select **Log warning if license server is not started as a service** to log a warning if the license server is started as an application. (Windows only)

Most companies run the license server application as a service. If it runs as an application, the license server is shut down by the operating system when a user logs out, which can negatively affect other users.

7. Select **Log license usage** to keep track of when licenses are used.

You can use this data to determine the appropriate time to perform system maintenance and to see if additional licenses are needed.

Note: The Seapine License Server can only provide usage reports for TestTrack 2009 and later licenses, Surround SCM 2009 and later floating licenses, and Surround SCM 2010 and later named licenses.

- Click **OK** to save the changes.

Server log levels

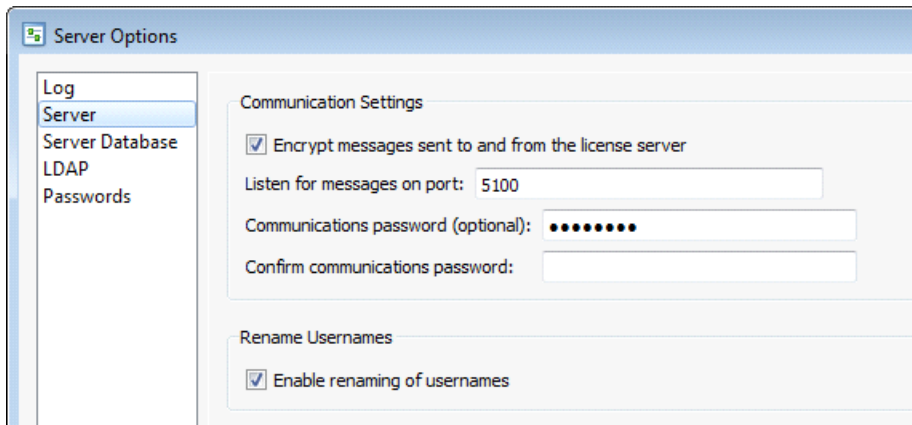
The level of logging defines how detailed the server log is. A lower level, such as Unusual Activity, provides more detail because multiple types of events are logged.

Level	Writes an event to the log when:
Severe Error (1)	A severe problem or critical condition occurs, such as a server failure.
Error (2)	An error condition occurs, such as a failed connection attempt.
Warning (3)	A warning condition occurs, such as the server not starting as an NT service.
Unusual Activity (4)	Unusual activity occurs, such as a user trying to log in with an incorrect username.
Information (5)	Any significant action occurs, such as a user action timing out.

Note: Events for the selected level and all higher levels are logged. If you select Unusual Activity, the server logs all severe error, error, warning, and unusual activity events.

Setting server options

- Choose **View > Server Options**.
The Server Options dialog box opens.
- Select the **Server** category.



3. Select **Encrypt messages sent to and from the license server** to encrypt messages between the license server, admin utility, and Seapine product servers.

Encryption increases security but may impact performance.

4. Enter the **Listen for messages on port** number.
5. Optionally enter and confirm a **Communications password**.

Using a communications password provides additional security by requiring the Seapine product servers to use a password to communicate with the license server.

If you change the communications password, you must also change the password in Seapine products or users cannot log in.

- To enter the password in TestTrack, log in to the TestTrack Server Admin Utility. Click **Server Options**, and then select the **License Server** category. Enter the password in the Password Settings area and click **OK**.
- To enter the password in Surround SCM, choose **Tools > Administration > Server Options**. Click the **License Server** category. Enter the password in the Communication Settings area and click **OK**.

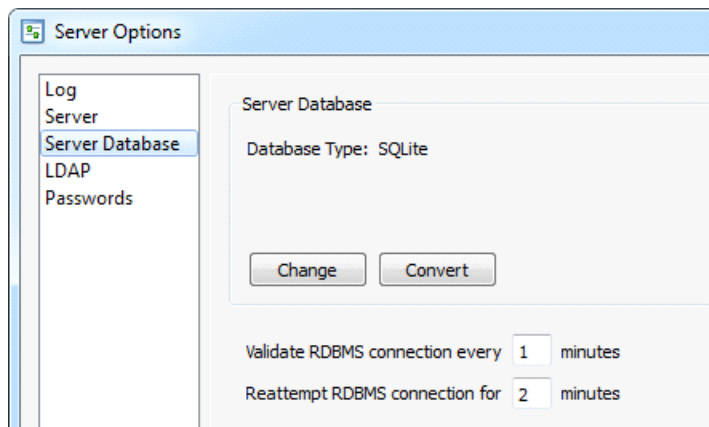
Note: If users cannot log in because the communications password was not changed, the administrator can use the default local admin credentials to correct the problem. Enter **Administrator** as the username and leave the password field empty.

6. Select **Enable renaming of usernames** to allow administrators to change usernames.
Only select this option if you have a specific reason to change usernames, such as a corporate security restrictions that require a standard username format.
7. Click **OK** to save the changes.

Configuring the server database

The Seapine License Server uses SQLite, a Relational Database Management System (RDBMS), for the backend database by default. You can change the database location or convert the database to a use a different RDBMS.

1. Choose **View > Server Options**.
The Server Options dialog box opens.
2. Select the **Server Database** category.
The current license server type and location is displayed.



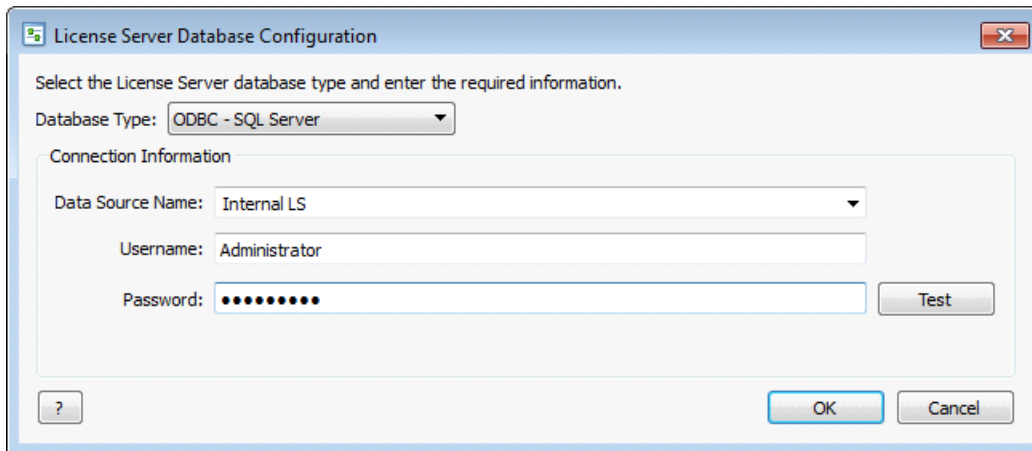
3. Click **Change** to change the database location. See [Changing the server database, page 10](#).
4. Click **Convert** to convert the database to another type. See [Converting the server database, page 11](#).
5. Make any changes to the RDBMS connection options.
 - **Validate RDBMS connection**—Enter how frequently you want to validate the RDBMS connection.
 - **Reattempt RDBMS connection**—Enter how long the license server should attempt connecting to an RDBMS server before initializing the server database. The license server attempts to connect to RDBMS servers for one minute by default. You can set the value between 0 and 10 minutes. There is a 20 second delay between each attempt. If you stop the license server while it is connecting to an RDBMS server, it stops after the 20 delay ends. You cannot log in to the license server while it is connecting to an RDBMS server.
6. Click **OK** to save the changes.

Changing the server database

You can configure the Seapine License Server to use a different server database location. For example, you move the database to another computer or experience problems and want to use a backup copy of the database. You should not need to frequently change the server database location.

1. Make sure you are logged into the license server that uses the database you want to change. Choose **File > Connect to Server** to connect to a different server.
2. Choose **View > Server Options**.
3. Select the **Server Database** category.
4. Click **Change**.

The License Server Database Configuration dialog box opens.



5. Select a **Database Type**.
6. Enter the **Connection Information**.
The available fields change based on the selected database type.
7. Click **Test** to test the connection.
The Test Connection dialog box opens and displays the results.

Tip: If the test connection fails, contact your DBA or internal support department for help.

8. Click **Close** to close the Test Connection dialog box.
9. Click **OK** to change the database location.
The following information is verified if you selected ODBC - SQL Server or Oracle Native:
 - The specified information connects to a valid database.
 - The database is not used by another Seapine License Server.
 - The required database tables exist and are accessible. If the database does not contain any license server tables, you are prompted to create them. See [Automatically creating Seapine License Server tables](#), page 13.
10. You return to the Server Database category. Click **OK** to save the changes.
Stop and restart the license server to complete the process.

Converting the server database

You can convert the Seapine License Server database to a different RDBMS type. SQLite, ODBC - SQL Server, Oracle Native, and PostgreSQL are supported.

Keep the following in mind before you start the conversion:

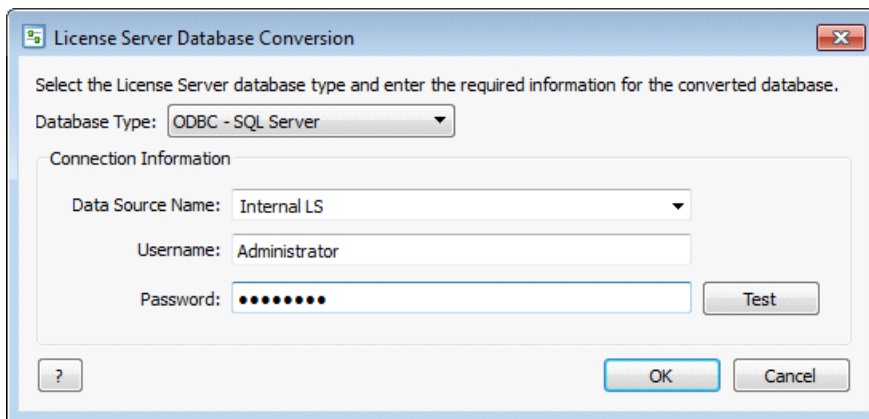
- The database you are converting to must be created before the conversion (except SQLite).
- All tables in the physical database must be empty (except SQLite).

- The database you are converting cannot be in use by another Seapine application or another license server.
- All other users must be logged out of the license server and admin utility.

Note: If you are converting to ODBC - SQL Server, we recommend that you manually create the server database tables. The license server can also create the tables during the conversion. See [Automatically creating Seapine License Server tables](#), page 13.

1. Make sure you are logged into the license server you want to convert the database for. Choose **File > Connect to Server** to connect to a different server.
2. Choose **View > Server Options**.
3. Select the **Server Database** category.
4. Click **Convert**.

The License Server Database Conversion dialog box opens.



5. Select a **Database Type**.
6. Enter the **Connection Information**.

The available fields change based on the selected database type.

Note: You are not prompted for connection information or to test the connection if you are converting to SQLite. The database is automatically converted into the C:\Program Files\Seapine\License Server\LicenseServDb directory.

7. Click **Test** to test the connection.

The Test Connection dialog box opens and displays the results.

Tip: If the test connection fails, contact your DBA or internal support department for help.

8. Click **OK** to close the Test Connection dialog box.
9. Click **OK** to convert the database.

You are prompted to start the conversion.

10. If you want to use the converted database immediately after the conversion finishes, select **Use converted database**.

If you do not select this option, you can manually change the database the license server is using after the conversion. See [Changing the server database, page 10](#).

11. Click **Yes**.

The Conversion Status dialog box opens and the conversion starts.

12. Click **Close** when the conversion finishes.
13. Stop and restart the license server to complete the conversion process.

Automatically creating Seapine License Server tables

When you upgrade or convert the Seapine License Server database, the physical database and empty tables must be created before data can be converted. If the tables do not exist, you are prompted to allow the license server to create them. See [Setting Up RDBMS Databases, page 49](#).

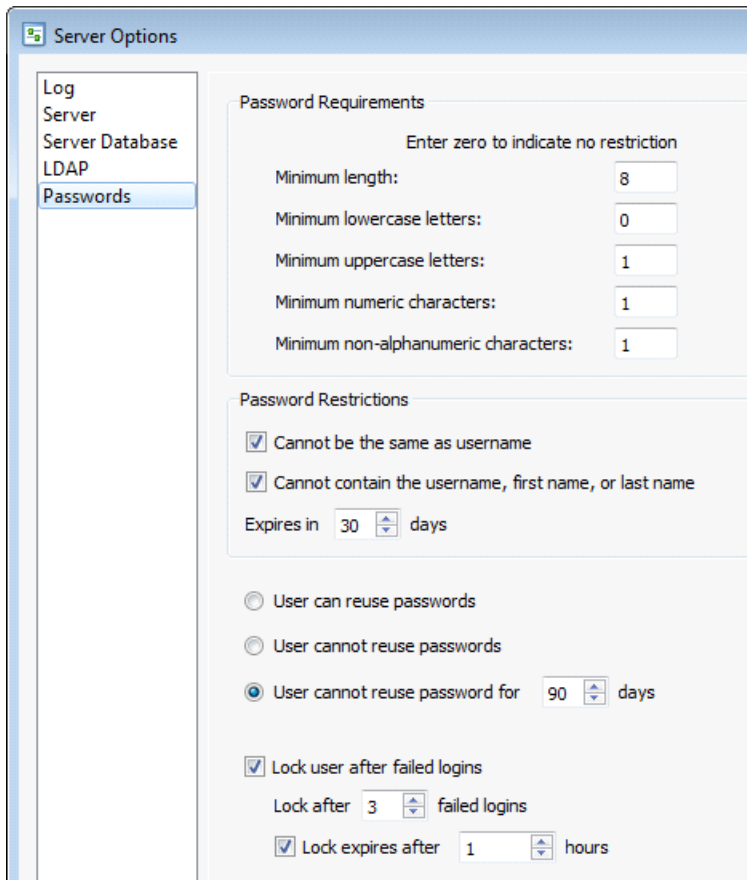
1. The Choose RDBMS Vendor dialog box opens when you are upgrading or converting the license server database.
2. Select the **RDBMS vendor** and click **OK**.
3. The server loads the corresponding table creation script and sends it to the database server.

Table creation scripts are stored in a configuration text file, which allows DBAs to use the script to help manually create tables or edit database attributes.

Setting password options

You can set options to enforce your company's password requirements and provide greater security. These password options only affect users stored on the Seapine License Server and do not apply to users associated with LDAP. Refer to your LDAP server documentation to set password restrictions on the LDAP server.

1. Choose **View > Server Options**.
The Server Options dialog box opens.
2. Select the **Passwords** category.



3. Enter any **Password Requirements** to require a minimum password length or minimum number of specific character types.

This can help you set strict password requirements that make it more difficult for unauthorized users to crack.

4. Select any **Password Restrictions**.

Requiring users to change passwords periodically adds to security and may also be required by compliance programs, such as 21 CFR Part 11.

5. Select a password reuse option.

Preventing users from reusing passwords minimizes the risk of unauthorized users finding and using passwords.

6. Select **Lock user after failed logins** to prevent users from logging in to Seapine products after the specified number of failed logins.

Select **Lock expires after** to set the number of hours before the lock is released and the user can log in to Seapine products.

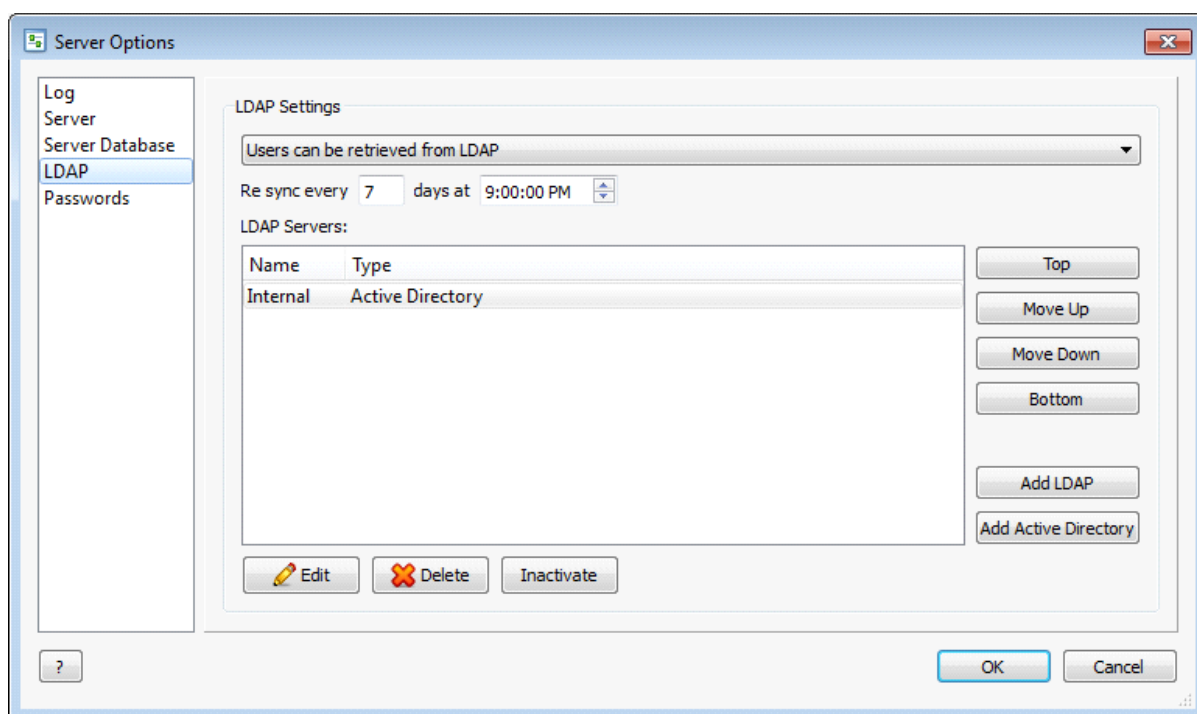
Note: If a user is locked, an administrator must unlock them on the license server before they can log in. See [Unlocking users, page 37](#). Restarting the license server does not release locks, but it resets the number of failed logins to 0.

7. Click **OK** to save the changes.

Setting LDAP options

The Seapine License Server supports LDAP, making it easy to manage and share information.

1. Choose **View > Server Options**.
The Server Options dialog box opens.
2. Select the **LDAP** category.



3. Select an LDAP retrieval option.
 - **Do not use LDAP** disables LDAP support.
 - **Users can be retrieved from LDAP** enables LDAP support, allows adding users from an LDAP server, and allows manually adding users that are not stored on an LDAP server.
 - **Users must be retrieved from LDAP** enables LDAP support and prevents administrators from adding users that are not stored on an LDAP server.
4. Select the re-sync frequency to specify how often the license server re-syncs with the LDAP server to update user information.

Note: You can also manually re-sync LDAP users. See [Re-syncing LDAP users](#), page 36.

5. Click **OK** to save the changes.

Adding LDAP servers

1. Choose **View > Server Options**.
2. Select the **LDAP** category.

3. Click **Add LDAP**.

The Add LDAP Server dialog box opens.

The screenshot shows the 'Add LDAP Server' dialog box with the following details:

- Name:** Internal LS
- Host:** server.seapine.com
- Port:** 389
- Use SSL
- Base:** o=development,dc=seapine,dc=com
- Password encryption:** Simple
- Secondary/Backup Server:** Host: , Port: 389
- Use anonymous binding for query
- Username:** Administrator
- User DN:** cn=Administrator,cn=users,dc=addoej,dc=seapine,dc=com
- Password:** [Masked]
- Attributes Table:**

User Field	LDAP Field
Work phone	telephoneNumber
Username	uid
User type	employeeType
Mobile phone	mobile
Last name	sn
Initials	initials
First name	givenName
Email	mail

4. Enter a descriptive **Name** for the LDAP server.
5. Enter the LDAP server IP address or alias as the **Host**.
For example, ldap.wysicorp.com.
6. Enter the LDAP server **Port** number.
The default port is 389.

Note: If the license server is running on Windows and you select the Use SSL option, the port number automatically changes to 636, which is the standard port for LDAP SSL on Windows. The standard LDAP SSL port on Unix is 389.

7. Enter the **Base** directory DN.

This field specifies where to start searching from in the LDAP tree. For example, your Base DN is wysicorp.com and includes development, sales, and support nodes. Entering o=sales, dc=wysicorp, dc=com instructs the license server to start searching from sales.

8. Select **Use SSL** to encrypt authentication messages sent over the network.

Selecting this option requires the license server to use the Secure Sockets Layer (SSL) protocol when sending and receiving authentication transmissions between the license server, the LDAP server, and Seapine products. We recommend selecting this option if the license server is configured to use simple password encryption.

9. Select the type of **Password encryption** to use when sending usernames and passwords over the network.
 - **Simple** sends usernames and passwords as plain text. We recommend selecting the **Use SSL** option if you use simple password encryption. The Username and Password fields are required if this option is selected.
 - **DIGEST-MD5** sends usernames and passwords as encrypted text. This option is only available if the license server is running on Unix. The Username, User DN, and Password fields are required if this option is selected.
10. Optionally enter the **Host** address and **Port** number of a backup server.

The backup server is only queried if the primary server cannot be reached.

11. Select **Use anonymous binding for query** to anonymously access the LDAP server.

You must be an authenticated, non-anonymous user if you want to perform LDAP operations, such as password checking.

12. Enter a **Username**, **User DN**, and **Password** if anonymous binding is not enabled.
 - **Username** is the name of the user you want to use to connect to the LDAP server. The license server will try to automatically connect to the LDAP server using one of the supported SASL authentication mechanisms.
 - **User DN** is the distinguished name (DN) of the user. This sequence of attributes and values specifies the location of an entry in the LDAP tree. For example: cn=Administrator, cn=users, dc=addeej, dc=wysicorp, dc=com.
 - **Password** is the password of the user you want to use to connect to the LDAP server.

13. Select an LDAP user attribute and click **Edit** to map the attribute to a license server user field. See [Mapping LDAP attributes, page 20](#).

14. Click **Test LDAP Connection** to test the LDAP server connection.

If the connection is not successful, correct any mistakes and retest it.

15. Click **OK** to save the changes.

The server is added.

Tip: Servers are queried in the order they are displayed. To reorder the servers, select a server and click Top, Move Up, Move Down, or Bottom.

Adding Active Directory servers

1. Choose **View > Server Options**.

2. Select the **LDAP** category.
3. Click **Add Active Directory**.

The Add Active Directory Server dialog box opens.

Add Active Directory Server

Name: Internal LS

Host: test.wysicorp.com Port: 389 Use SSL

Domain: WYSICORP

Username: Administrator

Password:

Auto Configure Single Sign-On: Enabled

Password encryption: Simple

Secondary/Backup Server

Host: backup.wysicorp.com Port: 389

Distinguished Names

Base DN: o=sales,dc=wysicorp,dc=com

User DN: cn=Administrator, cn=users, cd=addeoj, dc=wysicorp, dc=com

Attributes

User Field	Active Directory Field
User Field	Active Directory Field
Work phone	telephoneNumber
Username	sAMAccountName
User type	employeeType
Mobile phone	mobile
Last name	sn

Edit Preview Users...

Synchronization

Synchronize user activation

? Test Connection OK Cancel

4. Enter a descriptive **Name** to identify the Active Directory server.
5. Enter the IP address or alias for the Active Directory server as the **Host**.
6. Enter the **Port** number where the Active Directory server resides.

The default port is 389.

Note: If the Seapine License Server is running on Windows and you select the Use SSL option, the port number automatically changes to 636, which is the standard port for LDAP SSL on Windows. The standard LDAP SSL port on Unix is 389. Contact your system administrator if you do not know which port number to use.

7. Select **Use SSL** to encrypt authentication messages sent over the network.

Selecting this option requires the Seapine License Server to use the Secure Sockets Layer (SSL) protocol when sending and receiving authentication transmissions between the license server, the LDAP server, and Seapine products. We recommend selecting this option if the license server is configured to use simple password encryption.

8. Enter the Windows **Domain** name the Active Directory services.
9. Enter the **Username** and **Password** for the Active Directory user used to bind to the Active Directory.
10. Select a **Single Sign-On** option.

Single sign-on allows LDAP users to automatically log in to Seapine products using the same credentials used to log in to their computer. For example, your organization may use a non-password login method, such as a secure ID token or biometrics. Single sign-on uses the same authentication to log in to Seapine products. See [Configuring single sign-on for LDAP servers, page 45](#).

11. Click **Auto Configure** to query the Active Directory server for the configuration information. Click **Advanced** to manually enter this information.
 - Enter the **Base DN**. This field specifies where to start searching from. For example, your Base DN is wysicorp.com and includes development, sales, and support nodes. Entering o=sales, dc=wysicorp, dc=com instructs the license server to start searching from sales.
 - Enter the **User DN**. This sequence of attributes and values specifies the location of an entry. For example: cn=Administrator, cn=users, dc=addeej, dc=wysicorp, dc=com.
 - Optionally enter the **Host** address and **Port** number of a backup server. The backup server is only queried if the primary server cannot be reached.
 - Select an LDAP user attribute and click **Edit** to map the attribute to a license server user field. See [Mapping LDAP attributes, page 20](#).

Note: When you auto configure the settings, the license server queries the Active Directory server for rootDSE information and retrieves the Base DN information. Next, the license server searches for the authentication user's User DN. After this DN is found, the user's CN value is removed and the remaining data is used as the final Base DN. For example, the license server queries an Active Directory server for rootDSE information and retrieves "dc=seapine,dc=com" as the Base DN. Next, the license server queries the Active Directory server for the authentication user's User DN and retrieves "cn=Virtual User, cn=Users,dc=seapine,dc=com". Finally, the license server trims off the user's CN value and uses "cn=Users,dc=seapine,dc=com" as the Base DN.

Due to performance reasons, we recommend using a subtree Base DN (e.g., cn=Users, dc=seapine, dc=com) instead of the topmost Base DN (e.g., dc=seapine,dc=com). If the topmost Base DN is used, it may cause a large amount of unnecessary network traffic. If users are dispersed across the Active Directory tree, we also recommend that you create multiple Active Directory server entries.

12. Select the type of **Password encryption** to use when sending usernames and passwords over the network.
 - **Simple** sends usernames and passwords as plain text. We recommend selecting the **Use SSL** option if you use simple password encryption. The Username and Password fields are required if this option is selected.
 - **DIGEST-MD5** sends usernames and passwords as encrypted text. The Domain, Username, User DN, and Password fields are required if this option is selected.
 - **GSSAPI** uses advanced encryption for usernames and passwords. This option is only available if the license server is running on Windows and is recommended to ensure secure authentication.
13. Select **Synchronize user activation** to automatically sync user activation between Active Directory and the license server. If a user is disabled or enabled in Active Directory, the user is inactivated or activated on the license server.
14. Click **Test Connection** to test the Active Directory server connection.

If the test is not successful, correct any mistakes and retest the connection. Click **Reset** to clear all information.
15. Click **OK** to save the changes.

The server is added.

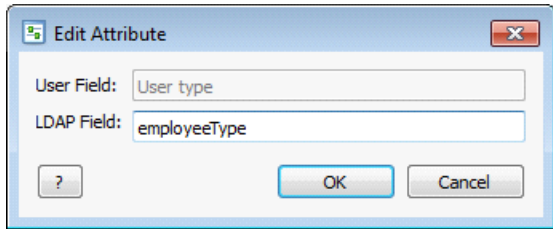
Tip: Servers are queried in the order they are displayed. To reorder the servers, select a server and click Top, Move Up, Move Down, or Bottom.

Mapping LDAP attributes

You can map license server user fields to LDAP and Active Directory fields to import all the information in a user record to the license server.

1. When adding or editing an LDAP or Active Directory Server, select a user attribute and click **Edit**.

The Edit Attribute dialog box opens.



2. Enter the **LDAP Field** you want to map to the license server user field and click **OK**.

You can enter the LDAP field name to map a single attribute to the field or use an expression to map multiple attributes to the field. Append and prepend the LDAP field name with a percentage sign (%). For example, the expression %organization% %company% maps the Organization and Company LDAP attributes to a license server user field. Any empty fields are not set for all users on the LDAP server.

The license server uses the following backup field expressions if the primary field is unavailable or empty.

User field	LDAP attribute
Company	company
Address	%postOfficeBox% %streetAddress% %l%, %st% %postalCode%

3. Click **Preview Users** to preview the field mappings. See [Previewing mapped LDAP attributes, page 21](#).
4. Click **OK** to save the changes.

Previewing mapped LDAP attributes

You can preview custom LDAP attribute mappings to see how LDAP fields are displayed in license server user records.

1. Click **Preview Users** when you are adding or editing an LDAP or Active Directory server.

The Preview LDAP Users dialog box opens.

2. Select a user to preview and click **Preview**.

The Preview LDAP Users dialog box opens. LDAP data from the field mappings is displayed on the Info and Address tabs.

Note: If you selected multiple users, click the arrow buttons to preview each user.

3. Click **Close** to close the preview.

Editing LDAP servers

1. Choose **View > Server Options**.
2. Select the **LDAP** category.

3. Select the server you want to edit.
4. Click **Edit**.
The Edit Server dialog box opens.
5. Make any changes.
6. Click **OK** to save the changes.

Inactivating LDAP servers

You can inactivate LDAP and Active Directory servers to remove them from the list of queried servers.

1. Choose **View > Server Options**.
2. Select the **LDAP** category.
3. Select the server you want to inactivate.
4. Click **Inactivate**.
The server is no longer active and will not be queried.
5. Click **OK** to save the changes.

Deleting LDAP servers

When you delete an LDAP or Active Directory server, any users associated with it are inactivated and cannot access Seapine products.

1. Choose **View > Server Options**.
2. Select the **LDAP** category.
3. Select the server you want to delete.
4. Click **Delete**.
You are prompted to confirm the deletion.
5. Click **Yes** to delete the server.
Make sure you want to delete the server. This action cannot be undone.
6. Click **OK** to save the changes.

Managing Licenses

Seapine's flexible licensing model allows you to use the right mix of licenses for your company's specific needs. Product licenses are managed globally with the Seapine License Server, reducing license administration time.

Seapine products include floating and named licenses. Floating licenses are best for users who log in occasionally while named licenses are best for users who log in frequently.

- A floating license can be used by anyone on the network, up to the limit specified on the Seapine License Server. The license server tracks the number of available floating licenses. When a user logs in, the corresponding total used floating license number increases by one. If more users than allowed by the floating license try to log in, they are denied access.
- A named license is dedicated to a specific user and allows the user to run the product from any place on the network. Named licenses cannot be shared. In addition, the Seapine License Server Admin Utility tries to automatically associate existing named license users with corresponding named licenses. For example, if you edit a 5-user named license and replace it with a 3-user named license, the license server admin utility tries to reassociate the remaining users with another named license.

Note: Each TestTrack license includes a license for the SOAP-based SDK.

Adding licenses

When you purchase a new product license or receive a maintenance extender key, you need to add the key to the license server before the product can be used.

Note: You can manually enter license keys or upload the .lic file that is attached to the email you received with the license keys. We recommend uploading the .lic file, which needs to be saved to your hard drive or another accessible location.

1. Choose **View > Licenses**.
The Seapine Licenses dialog box opens.
2. Click **Add**.
The Add License dialog box opens.
3. Click **Browse** to select a license file. Licenses have a .lic file extension.
4. Select the license file and click **Open**.

Tip: If you manually enter a license, the Serial Number field is case sensitive. Licenses can be entered with or without dashes.

5. Click **OK**.
The serial number is added. If you are adding a maintenance extender key, the existing key is updated. You do not need to delete existing licenses.

Configuring license pools

You can configure license pools to assign specific floating licenses to a group of users. This helps ensure a certain number of floating licenses are available for different groups of users. For example, you can create a license pool for occasional users to share and another license pool for developers to guarantee that developers always have access to a license.

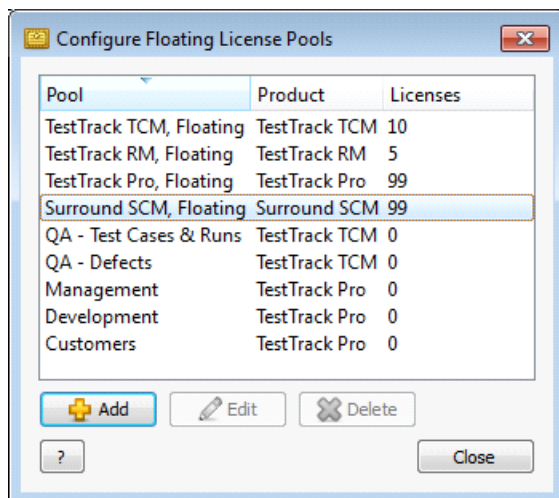
Note: All available licenses that are not dedicated to a specific pool are included in the default Floating license pool for each product. Users assigned to a license pool cannot use licenses from the default pool.

1. Choose **View > Licenses**.

The Seapine Licenses dialog box opens.

2. Click **Configure Floating Pools**.

The Configure Floating License Pools dialog box opens.



3. Click **Add** to create a new license pool. See [Adding license pools](#), page 24.
4. Select a license pool and click **Edit** to modify it. See [Editing license pools](#), page 25.
5. Select a license pool and click **Delete** to delete it. See [Deleting license pools](#), page 26.
6. Click **Close** to close the dialog box.

Adding license pools

You can create license pools to specify the number of floating licenses available to a group of users.

1. Choose **View > Licenses**.

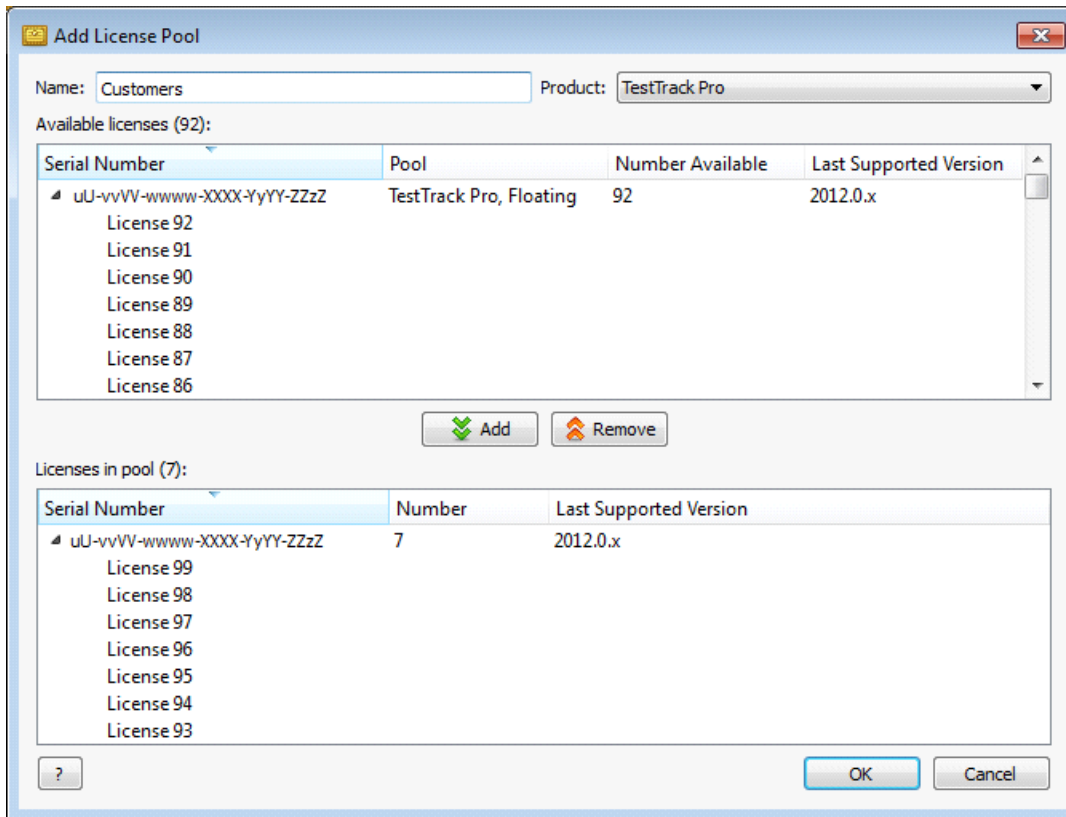
The Seapine Licenses dialog box opens.

2. Click **Configure Floating Pools**.

The Configure Floating License Pools dialog box opens. The available product licenses are listed in the default Floating pool for each product.

3. Click **Add**.

The Add License Pool dialog box opens.



4. Enter a license pool **Name**.

Note: The license pool name must be between 1 and 40 characters.

5. Select a **Product**.

The available licenses for the selected product are grouped by serial number.

6. Select a license from the **Available licenses** list.

To select multiple licenses, **Ctrl+click** the licenses. To select all the available licenses from a serial number, click the serial number.

7. Click **Add** to add the license to the pool.

To remove a license from the pool, select the license and click **Remove**.

8. Click **OK**.

The license pool is added. The licenses in the pool can only be used by the users assigned to the license pool. See [Assigning users to license pools, page 26](#).

Editing license pools

1. Choose **View > Licenses**.

The Seapine Licenses dialog box opens.

2. Click **Configure Floating Pools**.
The Configure Floating License Pools dialog box opens.
3. Select a license pool and click **Edit**.
The Edit License Pool dialog box opens.
4. Make any changes.
5. Click **OK** to save the changes.

Deleting license pools

1. Choose **View > Licenses**.
The Seapine Licenses dialog box opens.
2. Click **Configure Floating Pools**.
The Configure Floating License Pools dialog box opens.
3. Select a license pool and click **Delete**.
4. You are prompted to confirm the deletion.
5. Click **Yes**.
The license pool is removed from the list.

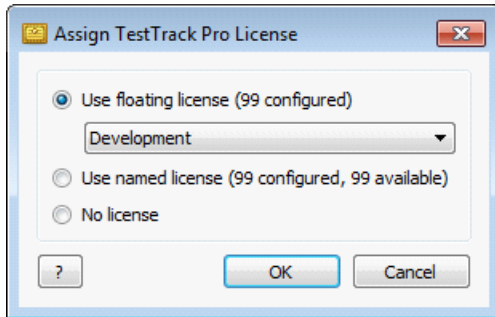
Note: License pools are not deleted from the server database. If a license pool is deleted in the admin utility, the record for the pool is marked as deleted in the database table.

Assigning users to license pools

You can assign users to license pools when assigning floating licenses.

Tip: To assign multiple users to a license pool, select the users in the Global Users list and replace the license field values for the users. See [Replacing license field values, page 42](#)

1. Choose **View > Global Users**.
The Global Users dialog box opens.
2. Click **Add** to assign a new user to a license pool or select an existing user from the Global Users list and click **Edit**.
The Add User or Edit User dialog box opens.
3. Click the **Licenses** tab.
4. Click the corresponding Seapine product license button.
The Assign License dialog box opens.



5. Select **Use floating license** and a license pool from the list. The Floating license pool is the default pool of available product licenses.
6. Click **OK** to close the Assign License dialog box.
7. Click **OK** to save the changes.
The user is assigned to the license pool.

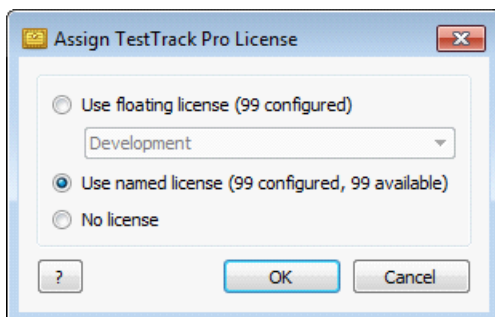
Assigning licenses

You can assign or change user licenses from the Global Users list. This is generally quicker than editing specific users to assign licenses or change their license information.

Tip: You can view the named licenses assigned to users in the Global Users list. If the product serial number column is not displayed, right-click a column heading and select the Serial Number field. Only the last four digits of the serial number are displayed for security purposes.

1. Choose **View > Global Users**.
The Global Users dialog box opens.
2. Select the users you want to assign licenses to.
To select multiple users, **Ctrl+click** each user.
3. Click the corresponding Seapine product button. Buttons are only available for products with licenses entered in the admin utility.

The Assign License dialog box opens.



4. Select a license type.

Note: You cannot assign named licenses to inactive users.

5. Click **OK**.

The licenses are assigned to the users.

Associating users with named licenses

You can quickly associate or disassociate users with named licenses. You cannot associate named licenses with inactive users.

Note: You can also assign or change user licenses from the Global Users dialog box. See [Assigning licenses, page 27](#).

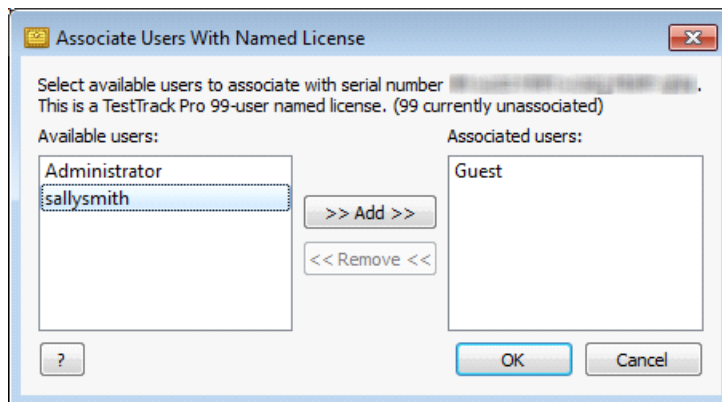
1. Choose **View > Licenses**.

The Seapine Licenses dialog box opens.

2. Select a named license.

3. Click **Associate Users**.

The Associate Users with Named License dialog box opens.



4. Select an available user and click **Add** to associate the user with the selected license.

To disassociate users, select an associated user and click **Remove**.

5. Click **OK** to save the changes.

Viewing used licenses

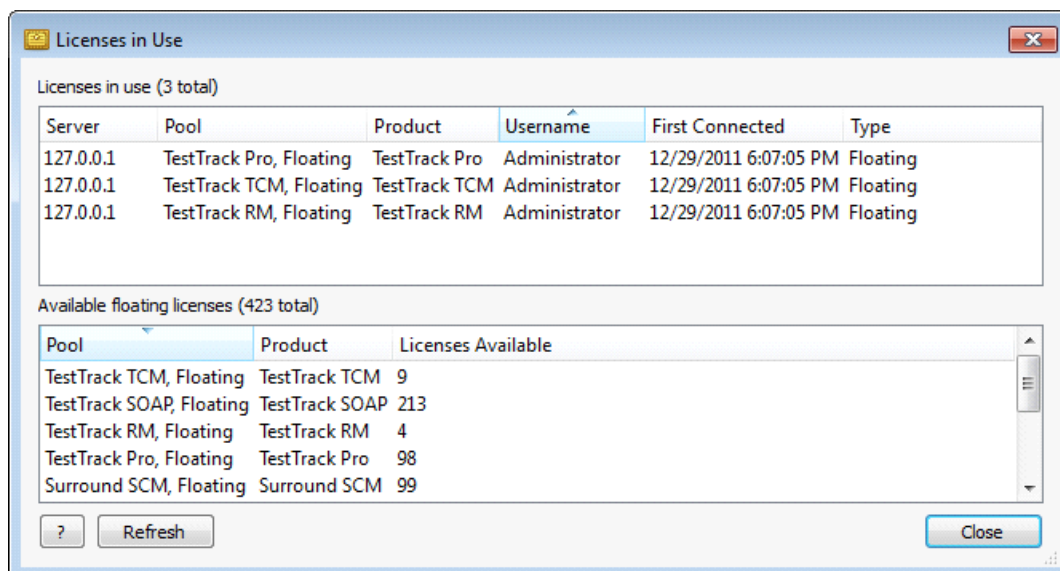
You can view the number of licenses used, which users are accessing a floating license, and the order users logged in.

1. Choose **View > Licenses**.

The Seapine Licenses dialog box opens.

2. Click **Licenses in Use**.

The Licenses in Use dialog box opens and displays the total licenses in use and the available floating licenses.

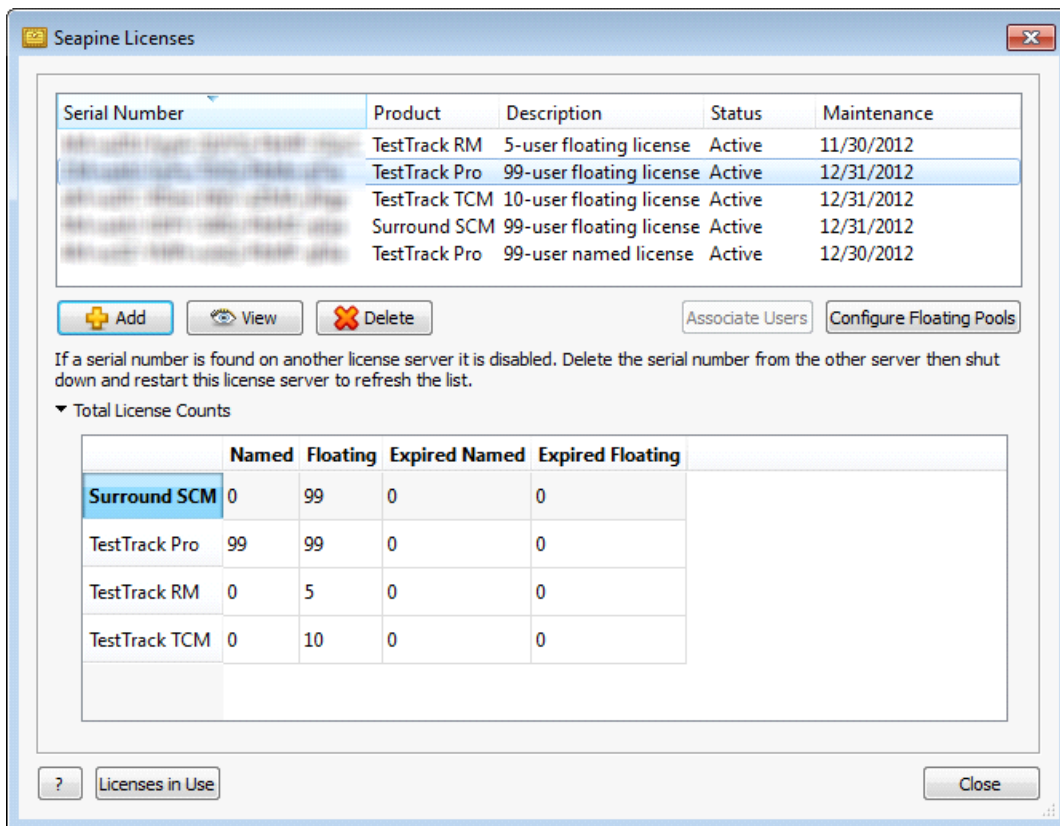


3. Click **Refresh** to update the list.
4. Click **Close** to close the dialog box.

Viewing license counts

You can view the number of current and expired licenses stored on the Seapine License Server by type and product.

1. Choose **View > Licenses**.
The Seapine Licenses dialog box opens.
2. Expand the **Total License Counts** area.
The license counts are displayed. Expanded evaluation licenses are not included.



Viewing license details

1. Choose **View > Licenses**.

The Seapine Licenses dialog box opens.

2. Select the license and click **View**.

The read-only License Details dialog box opens. The information in the dialog box changes based on the license type.

Deleting licenses

1. Choose **View > Licenses**.

The Seapine Licenses dialog box opens.

2. Select the license and click **Delete**.

You are prompted to confirm the deletion.

3. Click **Yes**.

The license is deleted.

Managing Global Users

Global users can be shared among Seapine products. Use the Seapine License Server Admin Utility to create global users.

Tip: You can also create users directly in Seapine products.

Customizing the Global Users list

You can customize the Global Users list and set up the columns to display the information you need.

To open the Global Users dialog box, click **Global Users** or choose **View > Global Users**.

Tip: You can use type ahead searching to quickly find users in the Global Users dialog box. Enter the characters you are searching for. Matching text is highlighted as you type. Press Ctrl+] to find the next match or Ctrl+[to find the previous match. Press Esc to clear the search.

Changing column contents

You can change column contents to display the information you use most frequently.

1. Right-click a column heading.

The available fields are displayed. Check marks indicate columns that are currently displayed.

2. Select a column.

The column is added and the user information is displayed. To remove a column, right-click it and select the column from the menu.

3. Click and drag the column to change its location.

Sorting columns

You can sort by any column in the Global Users list. You can also perform primary and secondary sorts.

- Click a column heading to perform a primary sort. An arrow is displayed next to the heading. Click the column heading again to toggle the sort order.
- **Shift+click** a column heading to perform a secondary sort. A double arrow is displayed next to the heading. **Shift+click** the column heading again to toggle the sort order.

Filtering columns

You can filter columns in the Global Users list to view users that match specific criteria.

- Click the funnel icon in the column heading to apply a filter. A green arrow indicates that a filter is applied to a column.

- Select **Custom** in the filter list to select multiple column values or to search for specific column text. Use the **Match Column Text** dialog box to set specific criteria to filter the Name, Username, Phone Number 1, Phone Number 2, Email Address, Address, and Notes columns. Use the **Select Column Values** dialog box to select multiple criteria to filter all remaining columns that use defined values.

Adding users

1. Choose **View > Global Users**.

The Global Users dialog box opens.

Tip: You can customize the information displayed in the Global Users list. See [Customizing the Global Users list](#), page 31.

2. Click **Add** and then select **Add User**.

The Add User dialog box opens with the Info tab selected.

- Enter the user's **First name** and **Last name**. Optionally enter the user's middle initial in the **MI** field.

- Enter a unique **Username**. Most organizations use a combination of the first and last names.

Note: First name, Last name, and Username are required. All other fields are optional.

- Enter the user's **Phone Numbers**.
- Select an email type and enter the **Email Address**.
- Enter and confirm a **Password**. Select any password options.
- Select a **User Type**. Some companies may provide customers with limited access to Seapine products. In this case, you may want to create a global customer.
- Clear **Active** to create an inactive user.

3. Click the **Security** tab to select security permissions for the user.

- **User cannot login to the license server admin utility** prevents users from accessing the admin utility. This is the default option and is recommended for most users.
- **User can retrieve global users, but cannot login to the license server admin utility** allows users to only retrieve global users in Seapine products.
- **User can only manage global users** allows users to create and maintain global users.
- **User can administer all license server functions** provides access to all admin utility commands. You should only select this option for administrative users.

4. Click the **Licenses** tab to select licenses for the user.

Click the corresponding Seapine product button and select a license. If you are assigning a floating license, you can also select a license pool to limit the number of licenses available to the user. See [Assigning users to license pools, page 26](#).

5. Click the **Address** tab to enter the address and select the company, division, and department.

If you have a large number of users, setting the Company, Division, and Department fields can help you group users. You can enter or select values in these fields. If you enter a value, it is saved and can be selected for other users and customers. You can enter up to 64 characters.

The Division field values are based on the selected Company value. The Department field values are based on the selected Division value.

The screenshot shows a user profile form with the following fields and values:

- Company:** WysiCorp
- Division:** WysiChart
- Department:** Development
- Address:** 123 Main Street, Mailstop 2, Anywhere, OH 12345

6. Click the **Notes** tab to add any notes about the user.
7. Click **OK** to add the user.

Adding LDAP users

If the Seapine License Server is configured to connect to an LDAP server, you can retrieve users from the LDAP database.

Note: The license server cannot support LDAP users with empty Name or Username fields. If you create an LDAP schema, make sure you enter the custom attributes when you add the LDAP server. See [Setting LDAP options, page 15](#).

1. Choose **View > Global Users**.
The Global Users dialog box opens.
2. Click **Add** and then select **Add LDAP User**.
The Add LDAP User dialog box opens.
3. Select any **Filter** criteria to narrow the search results.
Do not select any search criteria if you want to return a list of all LDAP users.
 - Enter a **Name** to search for LDAP users by name. This field supports wildcards.
 - Enter a **Username** to search for LDAP users by username. This field supports wildcards.
 - Select **Exclude existing license server users** if you do not want to include existing users. Users that have been deleted from the license server are included in the list if this option is selected. The username field determines if a user exists on the license server.
 - Select **Limit results to** and enter the maximum number of returned records.
4. Click **Query LDAP Servers**.
A list of matching users is displayed in the Search Results area.

5. Select the users you want to add to the license server.
 - Click **Add** to add multiple users. After the users are added, make sure you assign license types and set security permissions for each user.
 - Click **Advanced Add** to add one user to the license server and open the Add User dialog box. Most of the user information is populated from the LDAP record and cannot be edited. Make sure you assign a license to the user and set server security permissions. You can also enable single sign-on if it is enabled for the LDAP server. See [Editing users, page 35](#).
6. Click **Close** when you finish adding LDAP users.

Note: LDAP users can access Seapine products after they are added to the license server and assigned a license. If the Seapine product servers are already running, it may take a few minutes for the changes to take effect.

Viewing users

You can view read-only user information.

1. Select the users you want to change in the Global Users list.
2. Select a user and click **View**.

The View User dialog box opens.

Editing users

You can edit most user information including security and licenses. If you are an administrator, you may also be able to edit the username. See [Changing usernames, page 36](#).

Tip: You can easily enable and disable single sign-on in the Quick Edit area on the Global Users dialog box. You can also activate and inactivate users.

1. Choose **View > Global Users**.

The Global Users dialog box opens.
2. Select a user and click **Edit**.

The Edit User dialog box opens.
3. Select **Allow user to authenticate using single sign-on** to enable single sign-on.

Single sign-on allows users to log in to Seapine products using their network credentials. This option is only available for LDAP users and if single sign-on is enabled for the LDAP server. See [Setting LDAP options, page 15](#) and [Enabling single sign-on for users, page 46](#).

Note: If single sign-on is required for all users associated with the LDAP server, the **User is required to authenticate with single sign-on** option is selected by default and cannot be changed.

4. Make any LDAP user association changes.

- Click **Associate with LDAP User** to associate the selected user with an LDAP record.
 - Click **Re-associate** if you are editing an LDAP user who is experiencing problems. The license server is updated with any new or changed LDAP record data.
 - Click **Disassociate from LDAP** if you are editing an LDAP user and want to remove the LDAP association. The user is changed to a global non-LDAP user.
5. Make any other changes.
 6. Click **OK** to save the changes.

Changing usernames

You should only edit usernames if a new business process or security restriction requires it. The old username can only be used by the original user and cannot be assigned to other users.

Note: If you are using TestTrack Pro 6.x or earlier or Surround SCM 2.x or earlier, do not edit usernames. Users will not be able to log in if you change their usernames.

1. Choose **View > Global Users**.
The Global Users dialog box opens.
2. Select a user and click **Edit**.
The Edit User dialog box opens.
3. Enter a new username and click **OK**.
You are prompted to confirm the username change.
4. Click **OK** to save the changes.
The username is changed. The old username is added to the Notes tab.

Re-syncing LDAP users

You can manually re-sync LDAP users if you do not want to wait for the information to be automatically updated.

1. Choose **View > Global Users**.
The Global Users dialog box opens.
2. Select the users you want to re-sync.
All LDAP users are re-synced if you do not select specific users.
3. Click **Re-Sync LDAP Users**.
The user information is re-synced.

Note: You can also set the server to re-sync automatically. See [Setting LDAP options, page 15](#).

Inactivating users

Inactive users cannot log in to Seapine products.

1. Choose **View > Global Users**.
2. Select the user you want to inactivate.
3. Click **Quick Edit** and then select **Inactivate**.

The user is inactivated.

Note: If the user is assigned a named license, you are prompted to confirm the inactivation. Named licenses cannot be assigned to inactive users.

Activating users

Activate an inactive user to allow them to log in.

1. Choose **View > Global Users**.
2. Select the user you want to activate.
3. Click **Quick Edit** and then select **Activate**.

The user is activated. You may need to assign a license to the user. See [Assigning licenses](#), page 27.

Unlocking users

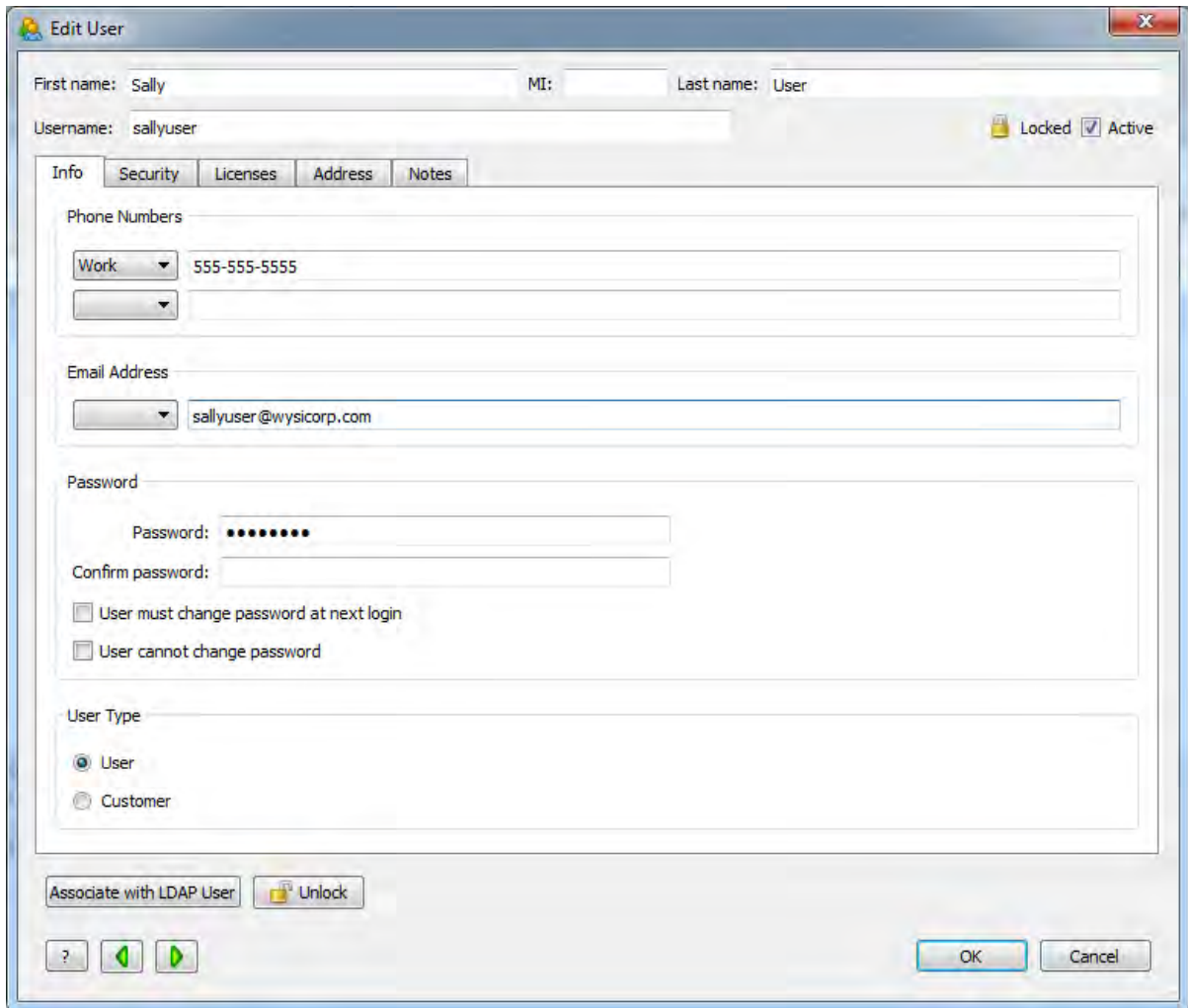
A user may be locked after failing to log in to Seapine products. You can unlock users to restore access.

Note: You can set failed login lockout options on the license server. See [Setting password options](#), page 13.

1. Choose **View > Global Users**.
2. Select a locked user.

Note: To unlock multiple users, select the users in the Global Users list, click **Quick Edit**, and then select **Unlock**. You can add the Locked column to the Global Users list to easily see which users are locked. See [Customizing the Global Users list](#), page 31.

3. Click **Edit**.
- The Edit User dialog box opens. The locked indicator is displayed.



4. Click **Unlock**. This button is only available if the user is locked.
The user is unlocked and can log in to Seapine products.

Exporting user information

User information can be exported as an XML file, which allows you to import the information into another Seapine License Server or application or use it with any XML-compatible tool.

1. Choose **File > XML Export**.
The XML Export dialog box opens.
2. Select **Encrypt Passwords** to encrypt passwords in the XML file.
3. Click **Export**.
The Export dialog box opens.
4. Select a **Save in** location and enter a **File name**.
5. Click **Save**.
The file is exported.

Importing user information

User information can be imported from an XML file. This lets you import information from another Seapine License Server or application.

If the XML file was exported from the license server, licenses are assigned based on information in the XML file. If a matching license type is not available, a license is not assigned.

1. Choose **File > XML Import**.

The XML Import dialog box opens.

2. Click **Browse** to select a file.
3. Select the file and click **Open**.

You return to the XML Import dialog box, which is populated with the file information.

4. Click **Validate XML File** to validate the file.

Tip: The XML Import Warnings and Error dialog box opens if any issues are found. You should try to correct errors before importing the file.

5. Click **Import** when you are ready to import the XML file.

The user information is imported.

Deleting users

When you delete users, their demographic information is also deleted. Inactivate users to save this information.

1. Choose **View > Global Users**.

The Global Users dialog box opens.

2. Select the user and click **Delete**.

You are prompted to confirm the deletion.

3. Click **Yes**.

The user is deleted.

Undeleting users

The Seapine License Server tracks deleted users and allows you to undelete them. For example, you may delete a user by mistake or need to reuse a specific username.

Note: Historical information can change if a username was used and you assign it to a different user. You must also maintain unique usernames to remain compliant with regulatory and other requirements. If you undelete a user, and assign the username to someone else, you may risk compliance.

1. Choose **View > Global Users**.

The Global Users dialog box opens.

2. Click **Undelete Users**.

The Undelete Users dialog box opens. A list of all deleted users is displayed.

3. Select one or more users and click **Undelete Users**.

The users are undeleted and removed from the list.

Printing the global users list

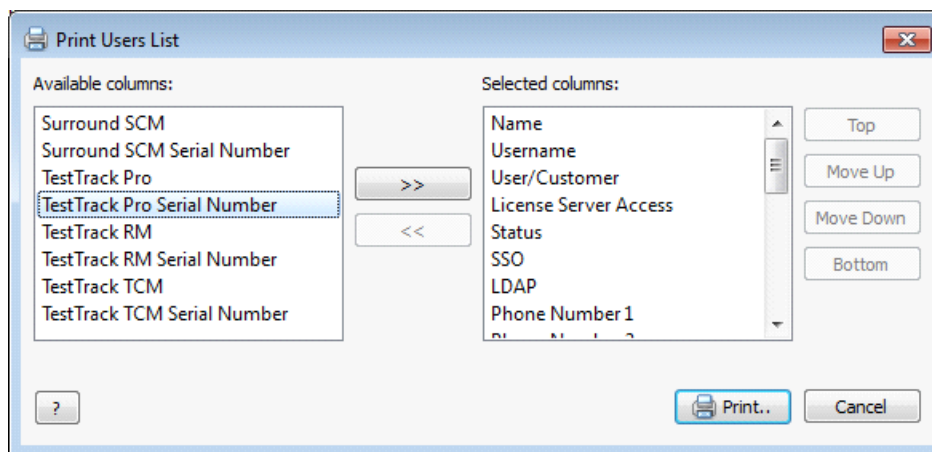
You can print the information in the Global Users dialog box.

1. Choose **View > Global Users**.

The Global Users dialog box opens.

2. Click the **Print** button.

The Print Users List dialog box opens. The Selected columns list includes the columns that are currently displayed in the Global Users window.



3. Select the column you want to add in the Available columns list and click the right arrow to move it to the Selected columns list.

To remove a column, select the column in the Selected columns list and click the left arrow to move it to the Available columns list.

4. Select a column in the Selected columns list and click Top, Move Up, Move Down, or Bottom to change the display order.

5. Click **Print**.

The Print dialog box opens.

6. Select any options and click **Print**.

Changing bulk user fields

Bulk user changes allow you to change multiple user records at once. You can change info, security, license, address, and notes fields.

Note: Users must have security permissions to administer all license server functions or manage global users to perform bulk user changes. See [Adding users](#), page 32.

Replacing info field values

LDAP user phone numbers and email addresses cannot be modified.

1. Select the users you want to change in the Global Users list.
2. Click **Quick Edit** and then select **Bulk User Changes**.

The Bulk User Changes dialog box opens with the Info tab selected.

The screenshot shows the 'Bulk User Changes' dialog box with the 'Info' tab selected. The dialog has five tabs: Info, Security, Licenses, Address, and Notes. The 'Info' tab is active and contains the following fields:

- Phone Numbers:** Two rows. The first row has a dropdown menu set to 'Set Phone 1', a dropdown menu set to 'Work', and a text input field containing '555-555-5555'. The second row has a dropdown menu set to '<Do not change>', a dropdown menu set to 'Work', and an empty text input field.
- Email Address:** A dropdown menu set to '<Do not change>', a dropdown menu set to 'Internet', and an empty text input field.
- Password:** Two rows. The first row is 'User must change password at next log in:' with a dropdown menu set to 'Set checked'. The second row is 'User cannot change password:' with a dropdown menu set to '<Do not change>'.
- User Type:** A dropdown menu set to '<Do not change>'.

At the bottom of the dialog, there is a note: 'Not all fields will be updated for LDAP users. Read-only fields will not be modified.' There are also buttons for '?', 'OK', and 'Cancel'.

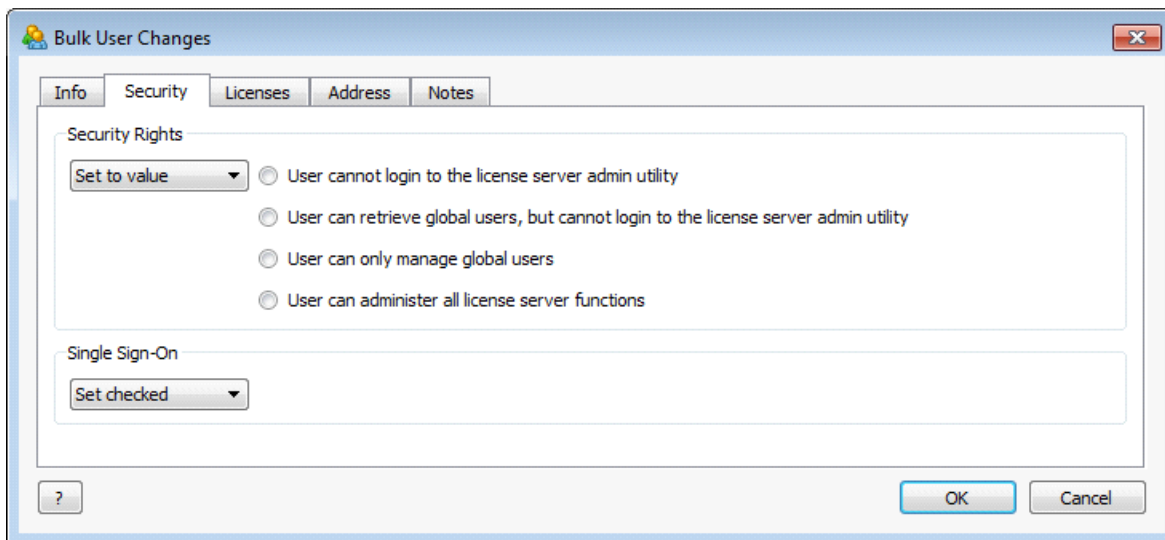
3. Make any changes. The available options depend on the field type.
To set the field to a new value, select **Set** and enter a value.
4. Click **OK** to save the changes.

Replacing security field values

1. Select the users you want to change in the Global Users list.
2. Click **Quick Edit** and then select **Bulk User Changes**.

The Bulk User Changes dialog box opens with the Info tab selected.

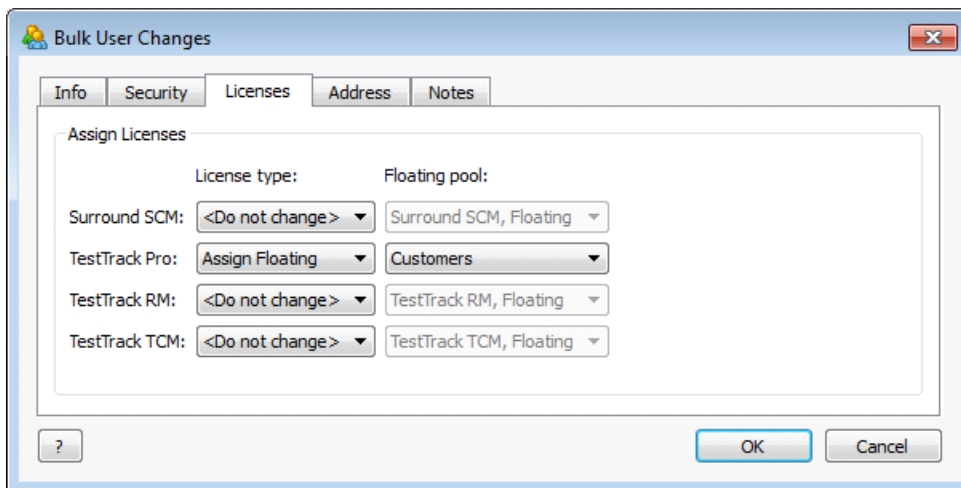
3. Click the **Security** tab.



4. Make any changes. The available options depend on the field type.
 - To change the security rights, select **Set to value** and select a value.
 - To enable single sign-on, select **Set checked**. To disable single sign-on, select **Set unchecked**.
5. Click **OK** to save the changes.

Replacing license field values

1. Select the users you want to change in the Global Users list.
2. Click **Quick Edit** and then select **Bulk User Changes**.
The Bulk User Changes dialog box opens with the Info tab selected.
3. Click the **Licenses** tab.



4. Make any changes.

- Select **Assign floating** to assign floating licenses. Optionally select a license pool to assign users to.
 - Select **Assign named** to assign named licenses. Named licenses cannot be assigned to inactive users.
 - Select **None** to remove the license assignments.
5. Click **OK** to save the changes.

Replacing address field values

Note: LDAP user address information cannot be modified.

1. Select the users you want to change in the Global Users list.
2. Click **Quick Edit** and then select **Bulk User Changes**.
The Bulk User Changes dialog box opens with the Info tab selected.
3. Click the **Address** tab.

The screenshot shows the 'Bulk User Changes' dialog box with the 'Address' tab selected. The dialog contains the following fields and values:

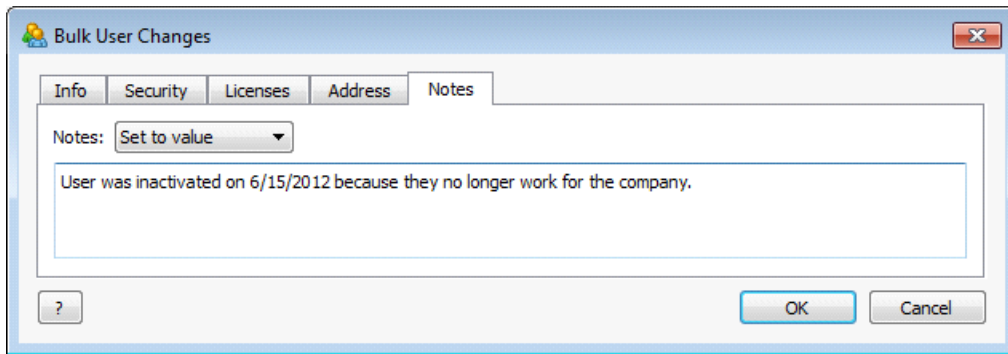
- Company: Set to value (dropdown) | WysiCorp (text field)
- Division: Set to value (dropdown) | Development (text field)
- Department: <Do not change> (dropdown) | (text field)
- Address: Set to value (dropdown) | 123 Main Street
Cincinnati, OH 44444 (text field)

At the bottom of the dialog, there is a note: "These fields will not be modified for LDAP users." and buttons for "?", "OK", and "Cancel".

4. Make any changes. The available options depend on the field type.
 - To set the field to a new value, select **Set to value** and enter or select a value.
 - To add text to the beginning of a text field value, select **Prepend** and enter the text.
 - To add text to the end of a text field value, select **Append** and enter the text.
5. Click **OK** to save the changes.

Replacing notes field values

1. Select the users you want to change in the Global Users list.
2. Click **Quick Edit** and then select **Bulk User Changes**.
The Bulk User Changes dialog box opens with the Info tab selected.
3. Click the **Notes** tab.



4. Make any changes.
 - To set the field to a new value, select **Set to value** and enter a value.
 - To add text to the beginning of the value, select **Prepend** and enter the text.
 - To add text to the end of the value, select **Append** and enter the text.
5. Click **OK** to save the changes.

Using Single Sign-On

Single sign-on allows LDAP (Active Directory) users to automatically log in to Seapine products using the same credentials used to log in to their computers, eliminating the requirement to enter a username and password. For example, if your organization uses a login method, such as secure ID tokens or biometrics, single sign-on can use this authentication to log in to Seapine products.

To use single sign-on, you must enable it when you add or edit an Active Directory server connection on the license server. You can enable single sign-on for individual users or you can require all users to use single sign-on.

Single sign-on requirements

- The Seapine License Server must be running on Windows as a service in an Active Directory domain.
- By default, the server computer Local System account is used to run the Seapine License Server application. If a different user runs the application, the user must be a trusted delegate in the Active Directory domain.
- Users can only use TestTrack 7.6 and later (Mac OS X, Web, or Windows) or Surround SCM 5.0 and later (Mac OS X or Windows). Client applications running on other platforms are not supported. Seapine server applications can run on any platform.
- Seapine client applications must run in the same Active Directory domain as the Seapine License Server or in a subdomain as part of the Windows forest (group of domain trees).
- TestTrack Web users must use Internet Explorer 6.0 or later. TestTrack must be hosted by an IIS web server with Windows Integrated Authentication enabled.

Configuring single sign-on for LDAP servers

You must enable single sign-on for the LDAP server before you can allow users to use it.

1. Choose **View > Server Options**.

The Server Options dialog box opens.

2. Select the **LDAP** category.
3. Select the Active Directory server you want to enable single sign-on for and click **Edit**.

If you need to add a new server connection, click **Add Active Directory**. See [Adding Active Directory servers, page 17](#).

The Edit Active Directory Server dialog box opens.

4. Select a **Single Sign-On** option.
 - **Disabled** disables single sign-on for all LDAP users associated with the Active Directory server. Users must manually log in to Seapine products.
 - **Enabled** enables single sign-on for all LDAP users associated with the Active Directory server.

- **Required** enables single sign-on for all LDAP users associated with the Active Directory server and restrict them from logging in using a username and password. Single sign-on is automatically enabled for all users associated with the Active Directory server.

Note: If single sign-on is required, all users associated with the Active Directory server must use the Seapine product versions and clients that support single sign-on. If the Active Directory server is not available, users cannot access Seapine products.

5. Click **OK** to save the changes.

If you enabled single sign-on, you must also enable it for users. See [Enabling single sign-on for users, page 46](#).

Enabling single sign-on for users

After you enable single sign-on for the LDAP server, you must enable it for users. Single sign-on can only be enabled for users retrieved from the LDAP database. See [Adding LDAP users, page 34](#).

Note: If single sign-on is required for the LDAP server, all users must it. You cannot enable or disable single sign-on for each user.

1. Choose **View > Global Users**.

The Global Users dialog box opens.

2. Select the user you want to enable single-sign on for.
3. Click **Quick Edit** and then select **Allow Single-Sign On**.

Single sign-on is enabled for the user. The user can select the Use single sign-on option on the Seapine product login dialog box to log in with their network credentials instead of entering a username and password.

Disabling single sign-on for users

You can disable single sign-on if it is not required for all users associated with the LDAP server.

1. Choose **View > Global Users**.

The Global Users dialog box opens.

2. Select the user you want to disable single-sign on for.
3. Click **Quick Edit** and then select **Do Not Allow Single-Sign On**.

The user must enter a username and password to log in.

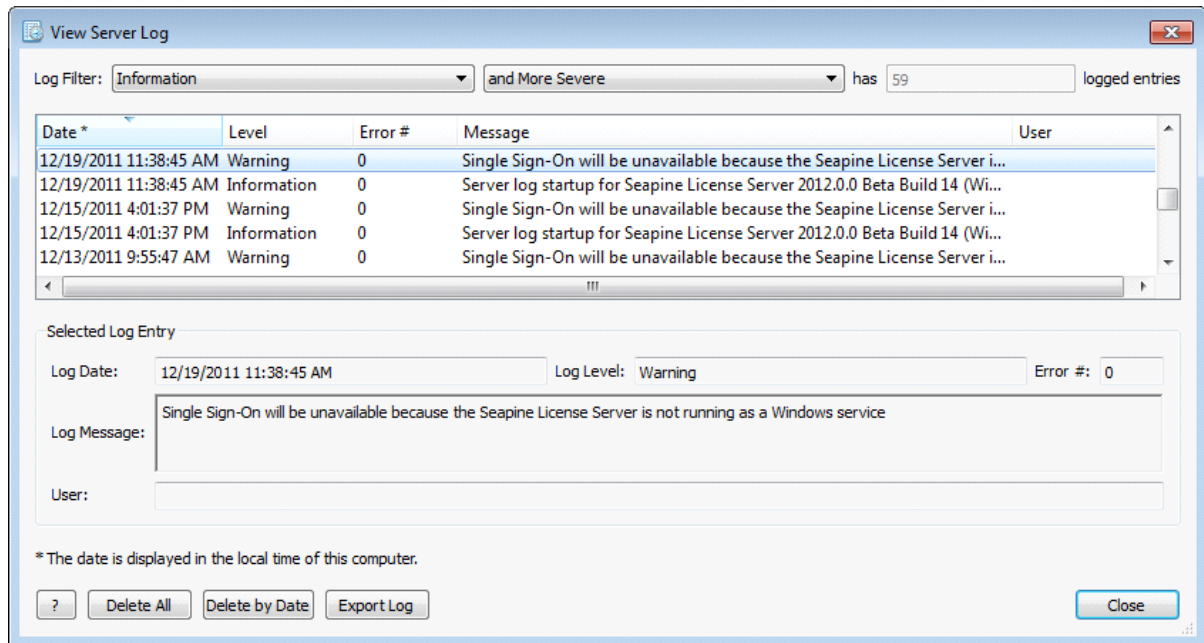
Managing the Server Log

The Seapine License Server log records server activity and any problems that may occur including errors, warnings, and timeout and user activity information. The amount of information in the log depends on the server options you set.

Viewing the server log

1. Choose **View > Server Log**.

The View Server Log dialog box opens.



2. Select a **Log Filter** to filter the log entries.
 - **Severe Error** includes errors that cause incorrect functionality that the user is not notified about.
 - **Error** includes errors handled and reported to the user.
 - **Warning** includes messages about potential problems.
 - **Unusual Activity** includes unusual activity by a user or unusual situations in the database.
 - **Information** includes any activity that may be of interest to the administrator.
3. You can filter the log list even more by choosing one of the following options:
 - **and Less Severe** includes the filtered log entries plus less severe entries.
 - **and More Severe** includes the filtered log entries plus more severe entries.
 - **Only** limits the filter to the filtered log entries.

Note: The read-only logged entries field displays how many entries match the restrictions you chose.

4. Select the entry you want to view.
The details are displayed in the Selected Log Entry area.

Exporting the server log

You can export the server log to a text file for analysis or report generation with other tools.

1. Choose **View > Server Log**.
The View Server Log dialog box opens.
2. Click **Export Log**.
The Export File dialog box opens.
3. Select a **Save in** location and enter a **File name**.
4. Click **Save**.
The log is exported.

Deleting all log entries

You can safely delete log entries if the log becomes too large and you are not experiencing problems.

1. Choose **View > Server Log**.
The View Server Log dialog box opens.
2. Click **Delete All**.
You are prompted to confirm the deletion.
3. Click **Yes**.
The entries are deleted from the log.

Deleting log entries by date

You can safely delete log entries if the log becomes too large and you are not experiencing problems.

1. Choose **View > Server Log**.
The View Server Log dialog box opens.
2. Click **Delete by Date**.
The Delete Log Entries dialog box opens.
3. Enter a date in the **Date** field.
4. Click **OK**.
All log entries, including any entries that occurred on the date you entered, are deleted.

Setting Up RDBMS Databases

The Seapine License Server database is stored in a Relational Database Management System (RDBMS). ODBC (Microsoft SQL Server), Oracle, PostgreSQL, and SQLite are supported. Information about supported platforms and databases is provided in the [Seapine License Server RDBMS Support](http://www.seapine.com/kb/questions/293) knowledgebase article (www.seapine.com/kb/questions/293).

SQLite is the default database type and does not require any setup or configuration before or after installation. PostgreSQL is also supported out of the box. If you use Oracle or SQL Server, review the following information for help setting up databases.

Setting up PostgreSQL databases

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

Keep the following in mind:

- Do not add, delete, or modify any fields in the Seapine License Server 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 Seapine License 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.

Creating server database tables

The Seapine License Server automatically creates tables in PostgreSQL when you start the server or convert the server database. The LSServerDB.sql script file, which is located in the PostgreSQL directory in the Seapine License Server application directory, is used to create the tables.

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

Creating Oracle users

You must create an Oracle user for the Seapine License 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 Seapine License 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 Seapine License Server 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 Seapine License 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 Seapine License Server 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 Seapine License Server computer.

- SQL Server must contain a Seapine License Server database before you create the DSN.
- You must use a system DSN.
- Make sure you change the default database to the Seapine License Server 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 Seapine License Server automatically creates tables when you start the server or convert the server database. The LSServerDB.sql script file, which is located in the SQLServer directory in the Seapine License Server 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 Seapine License Server cannot connect to the server database, errors are added to the LSStartup.log file in the Seapine License Server 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 Seapine License 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 Seapine License 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 Seapine License 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 Seapine License 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 Seapine License 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. The Seapine License Server Admin Utility 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 'xxx'. 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 Setting up Oracle databases, page 49 for information about downloading the installers.
ORA-12705: invalid or unknown NLS parameter value specified QOCI: Unable to logon	<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"> ▪ Windows—NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252 ▪ Linux and Mac OS X—NLS_LANG=American_America.UTF8 <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>Note: 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>
ORA-12514: TNS:listener does not currently know of service requested in connect descriptor QOCI: Unable to logon	<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>

Error	Cause
ORA-12154: TNS:could not resolve the connect identifier specified QOCI: Unable to logon	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.
ORA-12541: TNS:no listener QOCI: Unable to logon	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.
ORA-01017: invalid username/password; logon denied QOCI: Unable to logon	The username or password specified in the RDBMS connection information is not valid. Check the username and password.

PostgreSQL connection errors

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

Using the Seapine License Server API

The Seapine License Server API provides developers with a dynamic library that can be used to create custom tools that leverage the Seapine License Server. The Seapine License Server API is available as a C library, Cocoa framework (Mac OS X only), Java library, and .NET assembly (Windows only). The Seapine License Server API documentation, which includes all available packages, classes, data structures, and examples, is installed along with the API library files in your Seapine License Server application directory in the following locations:

- C API documentation—[API/docs/C/index.html](#)
- Cocoa API documentation—[API/docs/Cocoa/index.html](#)
- Java API documentation—[API/docs/Java/index.html](#)
- .NET API documentation—[API/docs/DotNet/index.html](#)

Note: The APIs are not thread safe. Limit the use of any Seapine License Server API to a single thread.

Appendix A: LDAP Authentication

Windows supported protocols

The Seapine License Server running on Windows supports the following authentication protocols:

- **Simple** - Client sends username/password as plain text data over the network. This method is not secure and should only be used over secure networks or in combination with SSL/TLS encryption. This is also covered as the SASL PLAIN mechanism, documented in RFC 2595.
- **DIGEST-MD5** - Client sends username/password as encrypted text over the network. This method is only supported for authentication to an Active Directory server.
- **GSSAPI (Kerberos)** - Client sends authentication token that is generated based on username/password over the network. This method is secure because it does not send the username/password over the network. It is only supported on Windows for authentication to an Active Directory server.

Unix supported protocols

The Seapine License Server running on Unix supports the following authentication protocols:

- **Anonymous** - Client does not provide any connection parameters, which results in an anonymous authentication if the server allows it.
- **Simple** - Client sends username/password as plain text data over the network. This method is not secure and should only be used over secure networks or in combination with SSL/TLS encryption. This is also covered as the SASL PLAIN mechanism, documented in RFC 2595.
- **DIGEST-MD5** - Client sends username/password as encrypted text over the network.

LDAP technical notes

Most LDAP-enabled application clients are designed to work with a specific, well-defined schema. Standard applications, such as TestTrack, usually work with a standard schema, such as RFC 2256, A Summary of the X.500(96) User Schema for use with LDAPv3. The Seapine License Server retrieves LDAP records based on proposed RFC standards.

- ObjectClass Person (RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3)
- ObjectClass OrganizationalPerson (RFC 2798 - Definition of the inetOrgPerson LDAP Object Class)
- UserID and Email Address (RFC 1274 - The COSINE and Internet X.500 Schema)

Microsoft Active Directory technical notes

Microsoft Active Directory is an LDAP compliant directory service that is supported through the LDAP configuration. The Seapine License Server retrieves LDAP records based on proposed RFC standards.

- ObjectClass Person (RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3)
- ObjectClass OrganizationalPerson (RFC 2798 - Definition of the inetOrgPerson LDAP Object Class)
- UserID and Email Address (RFC 1274 - The COSINE and Internet X.500 Schema)

Appendix B: Third-Party Software Licenses

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS 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 OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE 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 names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

OpenLDAP Copyright

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted. Copyright 1998-2003 The OpenLDAP Foundation All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/>.

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>.

Portions Copyright 1998-2003 Kurt D. Zeilenga.

Portions Copyright 1998-2003 Net Boolean Incorporated.

Portions Copyright 2001-2003 IBM Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

Portions Copyright 1999-2003 Howard Y.H. Chu.

Portions Copyright 1999-2003 Symas Corporation.

Portions Copyright 1998-2003 Hallvard B. Furuseth.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided as is" without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.

All rights reserved.

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.

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.
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). This product includes software written by Tim Hudson (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.]

Cyrus SASL information

CMU libsasl

Tim Martin

Rob Earhart

Rob Siemborski

Copyright (c) 1998-2003 Carnegie Mellon University. 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. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213-3890, phone: (412) 268-4387, fax: (412) 268-7395, tech-transfer@andrew.cmu.edu.
4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Index

6

64-bit server	1
new installations	2
upgrade installations	2

A

Activating users	37
Active Directory servers	
adding	17
deleting	22
editing	21
enabling single sign-on	45
inactivating	22
mapping attributes	20
previewing mapped LDAP fields	21
Adding	
Active Directory servers	17
LDAP servers	15
LDAP users	34
license pools	24
licenses	23
maintenance extender keys	23
server connections	3
users	32
API	55
Assigning licenses	27

B

Bulk change users	40
address fields	43
info fields	41
licenses	42
notes fields	43
security	41

C

Changing server databases	10
---------------------------	----

Columns

changing contents	31
filtering	31
sorting	31

Connecting to different server	4
--------------------------------	---

Converting server databases	11
-----------------------------	----

Current activity	28
------------------	----

D

Databases

automatically creating tables	13
Oracle	49
PostgreSQL	49
SQL Server	50

Deleting

Active Directory servers	22
LDAP servers	22
license pools	26
licenses	30
server connections	4
server log entries	48
server log entries by date	48
users	39

E

Editing

Active Directory servers	21
LDAP attributes	20
LDAP servers	21
license pools	25
server connections	3
usernames	36
users	35

Exporting

server log	48
user information	38

F

Failed logins	13
---------------	----

Fields		deleting	26
changing for multiple users	40	editing	25
address fields	43	Licenses	
info fields	41	adding	23
licenses	42	adding maintenance extender keys	23
notes fields	43	assigning	27
security	41	associating users	28
Filtering columns	31	deleting	30
Finding servers	4	floating	23
Floating licenses	23	named	23
G		used	28
Global users list		viewing counts	29
customizing	31	viewing details	30
printing	40	Locking users	13
I		Login failures	13
Importing users	39	N	
Inactivating		Named licenses	23
Active Directory servers	22	associating users	28
LDAP servers	22	viewing user assignments	27
users	36	O	
Installing		ODBC	
64-bit license server	2	connection errors	52
license server	1	connection issues	52
server admin utility	1	Oracle	
L		connecting to	50
LDAP servers		connection errors	53
adding	15	creating server database tables	50
adding users	34	creating users	50
deleting	22	database character set	50
editing	21	instant client libraries (OCI)	50
inactivating	22	setting up	49
mapping attributes	20	sizing, memory, and tuning	50
options	15	P	
previewing mapped LDAP fields	21	Password options	13
re-syncing users	36	PostgreSQL	
License pools	24	connection errors	54
adding	24	creating server database tables	49
assigning users to	26	setting up	49

Previewing mapped LDAP attributes	21	Server options	
Printing global users list	40	LDAP	15
R		log	7
RDBMS connections		password	13
changed database configuration	52	server	8
dropped tables	52	Servers	
exclusive lock	52	connecting to different	4
mismatched UUID	52	finding	4
server database cannot be shared	51	Single sign-on	
troubleshooting	51	disabling for users	46
RDBMS databases	49	enabling for Active Directory server	45
Re-syncing LDAP users	36	enabling for users	46
Reports		requirements	45
generating support diagnostics	5	Sorting columns	31
S		SQL Server	
Seapine License Server		connecting to	51
starting	2	connection errors	53
Seapine License Server Admin Utility		creating server database tables	51
starting	2	setting up	50
Server connections		SQLite	
adding	3	converting the server database	11
deleting	4	creating server database	2
editing	3	Starting	
Server database tables		Seapine License Server	2
Oracle	50	Seapine License Server Admin Utility	2
PostgreSQL	49	T	
SQL Server	51	Troubleshooting	
Server databases		RDBMS connections	51
changing	10	U	
configuring	9	Undeleting users	39
converting	11	Unlocking users	37
Server log		Upgrades	
deleting all entries	48	64-bit server	2
deleting entries by date	48	Username	
exporting	48	editing	36
levels	8	Users	
options	7	activating	37
viewing	47	adding	32

adding LDAP	34
associating with named licenses	28
bulk change users	40
bulk field changes	
address fields	43
info fields	41
licenses	42
notes fields	43
security	41
customizing Global Users dialog box	31
deleting	39
disabling single sign-on	46
editing	35
enabling single sign-on	46
exporting	38
importing	39
inactivating	36
locking	13
printing the global users list	40
re-syncing LDAP	36
undeleting	39
unlocking	37
viewing	35
viewing assigned named licenses	27

V

Viewing

assigned named licenses	27
license counts	29
license details	30
server log	47
users	35