



# HelixALM

---

## Server Admin Guide

Version 2017.1

PERFORCE

[www.perforce.com](http://www.perforce.com)

© Perforce Software, Inc. All rights reserved.



# Copyrights

© 1996-2017 Perforce Software, Inc. and its subsidiaries. All rights reserved.

Defect Scribe, Helix ALM, Helix ALM Suite, Helix Issue Management, Helix Requirements Management, Helix Test Case Management, QA Wizard Pro, Resource Thief, SoloBug, SoloSubmit, Surround SCM, and TestTrack are trademarks or registered trademarks of Perforce Software, Inc. and its subsidiaries in the United States and other countries.

Acrobat Reader is a registered trademark of Adobe, 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, macOS, Macintosh, Objective-C, and Safari are registered trademarks of Apple Computer, Inc.

Chrome is a registered trademark of Google Inc.

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

Firefox is a registered trademark of the Mozilla Foundation.

Linux is a trademark of Linus Torvalds.

Microsoft, Windows, 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.

openSUSE and SUSE are registered trademarks of Novell Inc. in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

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

Ubuntu is a registered trademark of Canonical Ltd.

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 Perforce Software, Inc. and its subsidiaries.

Your license agreement with Perforce Software, Inc. or any of its subsidiaries, 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 Perforce Software, Inc. or any of its subsidiaries. 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.

Perforce Software, Inc. and its subsidiaries

400 N 1st Avenue

Suite 200

Minneapolis, Minnesota 55401

USA

+1 510.864.7400

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

# Contents

<b>Getting Started</b> .....	<b>1</b>
Starting the Helix ALM License Server .....	1
Starting the Helix ALM Server .....	1
Starting the Helix ALM Server Admin Utility .....	2
Setting up server connections .....	3
Adding server connections .....	4
Editing and deleting server connections .....	4
Adding server admin utility users .....	5
Removing server admin utility users .....	5
Connecting to a different server .....	5
Generating support diagnostic reports .....	6
Setting the browser path on Linux .....	6
<b>Creating Projects</b> .....	<b>7</b>
Creating native projects .....	7
Creating RDBMS projects .....	9
Creating projects from templates .....	10
<b>Configuring Server Options</b> .....	<b>13</b>
Setting log options .....	14
Setting email sending options .....	15
Setting email tracking options .....	16
Setting server options .....	18
Configuring the server database location and type .....	19
Changing the server database location .....	19
Converting the server database type .....	20
Adding RDBMS connections .....	22
Editing and deleting RDBMS connections .....	24
Setting client settings .....	24
Setting JIRA integration options .....	26
Setting security options .....	26
Securing communication between clients and the Helix ALM Server .....	28
Configuring RSA key exchange .....	30
Setting license server options .....	31
Finding license servers .....	32
Setting software update check options .....	32
Viewing software update information .....	34

---

<b>Managing Projects</b> .....	<b>35</b>
Adding existing Helix ALM native projects .....	36
Adding existing RDBMS projects .....	37
Editing project settings .....	39
Moving project directories .....	39
Moving RDBMS projects .....	40
Inactivating and activating projects .....	41
Removing projects .....	41
Deleting Helix ALM native projects .....	41
Deleting RDBMS projects .....	42
<b>Managing Databases</b> .....	<b>43</b>
Modifying Helix ALM databases .....	43
Backing up Helix ALM databases .....	43
<b>Upgrading and Converting Projects</b> .....	<b>47</b>
Upgrading projects .....	47
Converting projects .....	47
<b>Working with the Server Log</b> .....	<b>51</b>
Server log levels .....	52
<b>Managing Email</b> .....	<b>53</b>
Resending email .....	53
Deleting email .....	54
<b>Setting Up RDBMS Databases</b> .....	<b>55</b>
Setting up Oracle databases .....	55
Setting up PostgreSQL databases .....	56
Setting up SQL Server databases .....	57
Troubleshooting RDBMS connections .....	57
<b>Appendix A: Startup Log Codes</b> .....	<b>61</b>
<b>Index</b> .....	<b>63</b>

# Getting Started

Helix ALM's scalable client/server model allows you to easily track and manage projects from a central location. Use the Helix ALM Server Admin Utility to manage the Helix ALM Server including [projects](#), [the server log](#), [server admin utility users](#), [the mail queue](#), and [server options](#).

The server admin utility is generally installed on the server computer and the server administrator's computer. If you need to install the admin utility, refer to the [installation help](#).

**Note:** A web-based server admin utility is also available. After installing the web admin utility, you must perform additional configuration on the web server that hosts it. See the [installation help](#) for information.

After the admin utility is installed:

- Start the Helix ALM License Server and Helix ALM Server. See [Starting the Helix ALM License Server, page 1](#) and [Starting the Helix ALM Server, page 1](#).
- Start the admin utility and add connections to servers you need to manage. See [Starting the Helix ALM Server Admin Utility, page 2](#) and [Adding server connections, page 4](#).
- Log in to start managing the server.

**Tip:** If you are logging in for the first time, you may want to create a new project or create a project from an existing project. See [Creating Projects, page 7](#) and [Creating projects from templates, page 10](#).

## Starting the Helix ALM License Server

An administrative user must make sure the Helix ALM License Server is running before the Helix ALM Server is started.

**Tip:** If Helix ALM cannot connect to the license server, an administrative user needs to troubleshoot. See [Helix ALM Cannot Connect to the License Server](#) for information.

## Windows

If the license server is installed as a service, it starts automatically. If the license server is installed as an application, you must start it manually. Choose **All Programs > Perforce > Helix ALM License Server > Helix ALM License Server** from the Start menu.

**Note:** If the server is installed as a service but not running or you need to restart it, see the Windows documentation for information about starting a service.

## Linux

Enter `/usr/bin/spls start`.

If you need to restart the server, enter `/usr/bin/spls stop` and then restart the server.

## Starting the Helix ALM Server

An administrative user must make sure the Helix ALM Server is running before users can access Helix ALM.

**Tip:** If users cannot connect to the Helix ALM Server when it is running, an administrative user needs to make sure the server computer is online and [the Helix ALM License Server is also running](#). Users should make sure the IP address and port number are correct in the server connection information.

## Windows

If the Helix ALM Server is installed as a service, it starts automatically. If the server is installed as an application, you must start it manually. Choose **All Programs > Perforce > Helix ALM > Helix ALM Server** from the Start menu.

**Note:** If the server is installed as a service but not running or you need to restart it, see the Windows documentation for information about starting a service.

## Linux

Enter `/usr/bin/ttstudio start`.

If you need to restart the server, enter `/usr/bin/ttstudio stop` and then restart the server.

## Starting the Helix ALM Server Admin Utility

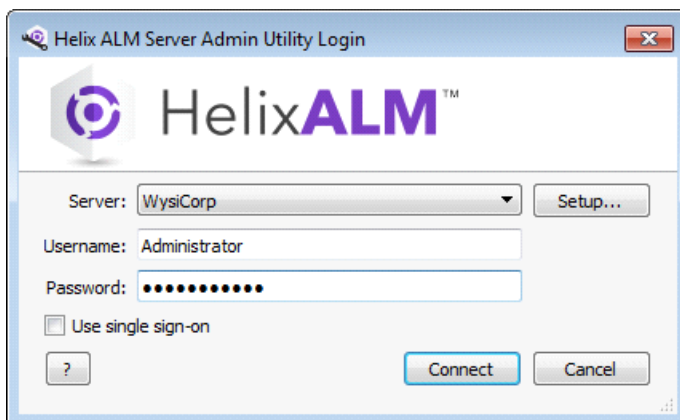
The Helix ALM License Server and Helix ALM Server must be running before starting the Helix ALM Server Admin Utility.

1. **Windows**—Choose **Programs > Perforce > Helix ALM > Helix ALM Server Admin** from the Start menu.

**Mac**—Double-click the **Helix ALM Server Admin Utility** icon in the Applications/HelixALM folder.

**Linux**—Enter `/usr/bin/ttadmin`.

The Helix ALM Server Admin Utility Login dialog box opens.



2. Select the **Server** to connect to. See [Adding server connections, page 4](#) if you need to add a server.
3. Enter your **Username** and **Password** or select **Use single sign-on** to log in with your network credentials.

Single sign-on is only available for Windows and Mac.

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

4. Click **Connect**.

The server admin utility starts.

If RSA key exchange is enabled, you may be prompted to verify the authenticity of the key fingerprint, which is used to prevent hacking. Verify that you are logging in to the correct server. If you are unsure if the fingerprint is correct, log in locally to the Helix ALM Server computer and verify that the key displayed in the Security server options matches the key displayed when you logged in from the other computer. See [Configuring RSA key exchange, page 30](#). If the fingerprint is correct, click **Yes**. If a different fingerprint is displayed in the Security server options, a hack may be in progress.

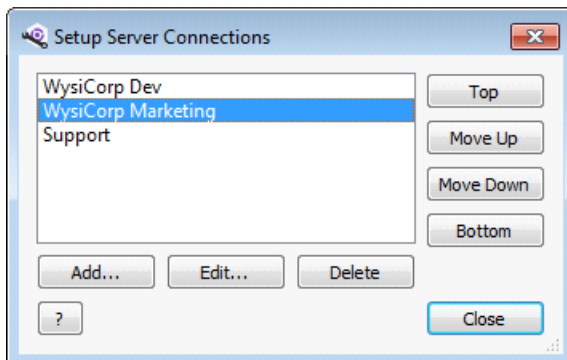
**Note:** You cannot use or upgrade TestTrack 2011.1 or earlier server databases in Helix ALM or TestTrack 2016 - 2016.1. You must upgrade these databases to TestTrack 2015.1 first or configure the server to use a different database that is upgraded to a supported version. Contact [Perforce Support](#) for help.

## Setting up server connections

The server admin utility connects to the Helix ALM Server via TCP/IP. Projects are located on a central server that is accessed by multiple remote client computers. Before you can access a 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** to add a server connection. See [Adding server connections, page 4](#).
4. Select a server and click **Edit** to change the server address or port number. See [Editing and deleting server connections, page 4](#).
5. Select a server and click **Delete** to delete the connection.
6. Select a server and click **Top**, **Move Up**, **Move Down**, or **Bottom** to reorder the list.  
You may want to move the servers you access most frequently to the top of the list.
7. Click **Close** when you finish.

## Adding server connections

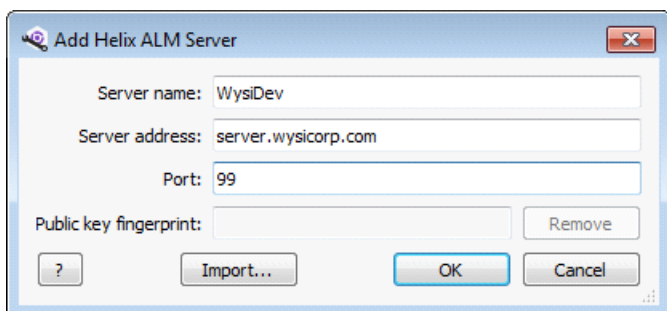
You need to add a connection to access servers that Helix ALM projects are stored on.

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 Helix ALM Server dialog box opens.



4. Enter a **Server name**.

Use a unique name to easily identify the server. For example, use your team name instead of a generic name, such as server1.

5. Enter the **Server address** for the computer the Helix ALM Server application is installed on and the **Port** number.

Helix ALM clients connect to the server on this port via TCP/IP. Valid values are 1-65535.

**Note:** If RSA key exchange is enabled for the server, click **Import** to import the server settings instead of manually entering the information. Select the XML file and click **Open**. The Server address, Port, and Public key fingerprint fields are automatically populated. The public key is required to connect to the server. See [Configuring RSA key exchange, page 30](#).

6. Click **OK**.

The server connection is added. You return to the Setup Server Connections dialog box.

7. To reorder the servers, select a server and click **Top**, **Move Up**, **Move Down**, or **Bottom**.

You may want to move the servers you access most frequently to the top of the list.

8. Click **Close** when you finish.

## Editing and deleting server connections

You can edit a server connection to change the name, address, or port number. You can also delete any server connections you no longer use.

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

The Setup Server Connections dialog box opens.



3. Edit or delete the connection.
  - To edit a connection, select it and click **Edit**. Make any changes and click **OK**.
  - To delete a connection, select it and click **Delete**. Click **Yes** to confirm the deletion.

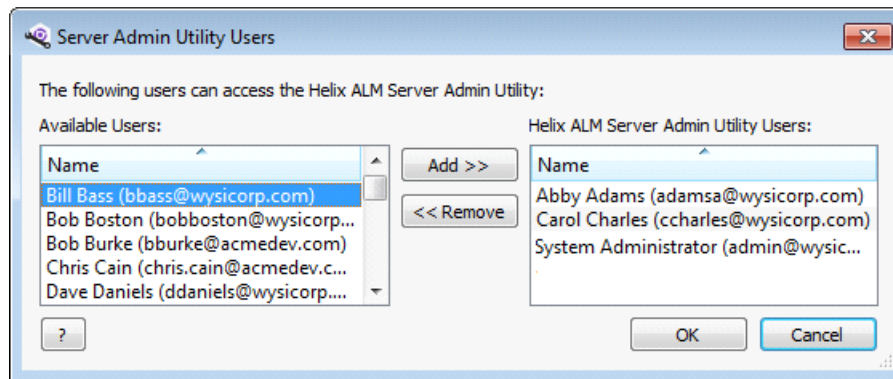
## Adding server admin utility users

Most organizations limit server admin utility access to administrators or other high-level users. Before a user can access the server admin utility, you must add them as an admin utility user. Only users that have been added to the Helix ALM License Server can be added as admin utility users.

**Note:** Server admin utility users only have access to manage the Helix ALM Server. To access project data, users must be added to a security group in projects. See the [Helix ALM help](#) for more information.

1. Click **Server Users**. You can also choose **View > Server Users**.

The Server Admin Utility Users dialog box opens.



2. Select a user in the Available Users list and click **Add**.

Server admin utility users have access to all areas in the server admin utility. Only add the user if you want to give them full access.

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

## Removing server admin utility users

You can remove server admin utility users if they no longer need access.

1. Click **Server Users**. You can also choose **View > Server Users**.

The Server Admin Utility Users dialog box opens.

2. Select a user in the Helix ALM Server Admin Utility Users list and click **Remove**.
3. Click **OK** to save the changes.

The user can no longer access the server admin utility.

## Connecting to a different server

You can connect to a different server without closing the admin utility. This is useful if the Helix ALM Server is installed on multiple computers.

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

You are prompted to confirm that you want to disconnect from the current server.

2. Click **Yes**.

The login dialog box opens.

3. Select the **Server** to connect to.
4. Enter your **Username** and **Password**.
5. Click **OK**.

You are logged in to the selected server.

## Generating support diagnostic reports

If you are experiencing Helix ALM problems and need help from Perforce Support, you can generate a report that includes detailed information about the server configuration. You can then [email the report to Perforce Support](#) to provide information for troubleshooting the issues.

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

The Save Support Information File As dialog box opens.

2. Choose a location to save the file in and enter a **File name**.

The default filename is supportinfo.zip.

3. Click **Save**.

The file is saved.

## Setting the browser path on Linux

If you use the server admin utility on Linux, you must set the browser path before you can view online help.

**Note:** If you do not set the browser path, you are prompted to set it the first time you view help.

1. Choose **Help > Browser Settings**.

The Browser Settings dialog box opens.

2. Enter the **Browser path** or click **Browse** to select it.

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

# Creating Projects

Helix ALM projects contain all information your team tracks, including issues, test cases, test runs, requirements, requirement documents, security groups, users, customers, filters, test configurations, and workbook tasks. Projects are created on the Helix ALM Server and managed using the Helix ALM Server Admin Utility. The server maintains the data for each project in a separate cache in memory on the server.

Your use of projects depends on your organization's processes. If you are using Helix ALM to track software issues, you may want to create a project for each release, for feature requests, or for specific customers. You can also customize Helix ALM for other types of tracking. For example, you can customize fields, terminology, and the workflow to help your human resources personnel track employees.

## Choosing a project database format

Projects can be stored in Helix ALM native (SQLite) and other RDBMS formats. See [Choosing a Database Format](#) for information about each database type.

When you are ready to create a project, see [Creating native projects, page 7](#) or [Creating RDBMS projects, page 9](#).

**Note:** You can also create projects based on existing projects. See [Creating projects from templates, page 10](#).

## Creating native projects

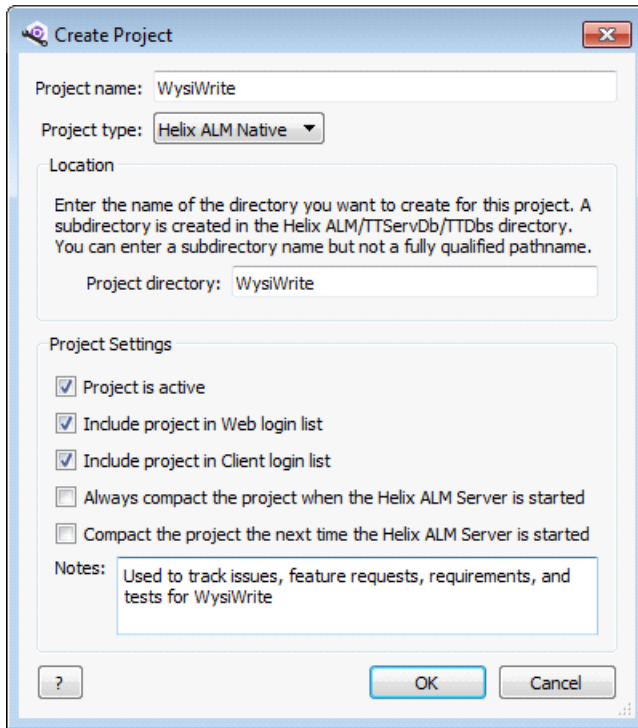
Helix ALM projects are stored in databases. Helix ALM uses SQLite as the native database type by default. All native project files, including the SQLite database file, are stored in a directory on the local hard drive of the Helix ALM Server computer or a mapped network drive. Only one project is stored in each project database.

1. Click **Projects**. You can also choose **View > Projects**.

The Projects dialog box opens.

2. Click **Create**.

The Create Project dialog box opens.



3. Enter a **Project name**. The name is displayed when users log in to Helix ALM.
4. Select **Helix ALM Native** from the Project type list.
5. Enter the **Project directory**.

A project directory with this name is created in the TTServDb/TTDBs directory in the Helix ALM application directory by default. This directory contains subdirectories for attachments, SoloBug files, and report stylesheets. The Helix ALM Server may be configured to use a different default path, which is displayed in the Location area. You may be able to enter a full path depending on the server settings. The path cannot exceed 247 characters, including the drive specifier (e.g., C:\) and names of subdirectories that Helix ALM creates in the specified directory.

**Note:** The default directory path for projects and the ability to enter fully qualified pathnames is controlled using the Helix ALM Registry Utility. See the [Registry Utility help](#) for information.

6. Select the **Project Settings**.
  - **Project is active** creates an active project. Users cannot access inactive projects.
  - **Include project in Web login list** includes the project in the list for Helix ALM Web users.
  - **Include project in Client login list** includes the project in the list for Helix ALM Client users.
  - **Always compact the project when the Helix ALM Server is started** compacts the project every time the server starts. Compacting removes space and rebuilds the index files, but may increase initialization time.
  - **Compact the project the next time the Helix ALM Server is started** compacts the project only the next time the server starts.
7. Enter any project **Notes**. For example, you can explain what the project is used for or why it was created.
8. Click **OK**.

The project is created.

**Note:** You are the only user added to the new project. You must add other users to security groups in the project from the Helix ALM Client before they can access it. See the [Helix ALM help](#) for information.

## Creating RDBMS projects

You can store Helix ALM projects in a Relational Database Management System (RDBMS). Using an RDBMS allows you to distribute projects between multiple databases if you have a large Helix ALM installation, leverage your existing database administration processes, and use standard database tools.

1. Click **Projects**. You can also choose **View > Projects**.

The Projects dialog box opens.

2. Click **Create**.

The Create Project dialog box opens.

The screenshot shows the 'Create Project' dialog box with the following fields and options:

- Project name:** WysiWrite
- Project type:** RDBMS
- Location:** Connection: WysiDev - admin
- Connection Information:** Data source/Service name: WysiDev, Username: admin
- Database project name:** WysiWrite
- Project directory:** WysiWrite
- Project Settings:**
  - Project is active
  - Include project in Web login list
  - Include project in Client login list
- Notes:** Used to track issues, feature requests, requirements, and tests for WysiWrite

3. Enter a **Project name**. The name is displayed when users log in to Helix ALM.
4. Select **RDBMS** from the Project type list.
5. Select the **Connection** for the RDBMS database to add the project to.

The list includes RDBMS connections configured for the Helix ALM Server. See [Adding RDBMS connections](#), page 22 if you need to add a connection.

6. Enter a unique **Database project name**. This name is stored in the database that hosts the project and cannot be changed after the project is created.

If the project is removed and then added to a Helix ALM Server later, this name is displayed in the project database name list in the Add Existing Project dialog box.

7. Enter the **Project directory**.

A project directory with this name is created in the TTServDb/TTDBs directory in the Helix ALM application directory by default. This directory contains subdirectories for attachments, SoloBug files, and report stylesheets. The Helix ALM Server may be configured to use a different default path, which is displayed in the Location area. You may be able to enter a full path depending on the server settings. The path cannot exceed 247 characters, including the drive specifier (e.g., C:\) and names of subdirectories that Helix ALM creates in the specified directory.

**Note:** The default directory path for projects and the ability to enter fully qualified pathnames is controlled using the Helix ALM Registry Utility. See the [Registry Utility help](#) for information.

8. Select the **Project Settings**.

- **Project is active** creates an active project. Users cannot access inactive projects.
- **Include project in Web login list** includes the project in the list for Helix ALM Web users.
- **Include project in Client login list** includes the project in the list for Helix ALM Client users.

9. Enter any project **Notes**. For example, you can enter notes about what the project is used for or why it was created.

10. Click **OK**.

A progress dialog box opens and displays actions as the project is created. You return to the Projects dialog box after the project is created.

**Note:** You are the only user added to the new project. You must add other users to security groups in the project from the Helix ALM Client before they can access it. See the [Helix ALM help](#) for information.

11. If the connection does not contain any Helix ALM tables, you are prompted to manually or automatically create them.

- Click **OK** if you want Helix ALM to automatically create the tables.
- Click **Cancel** to manually create the tables.

**Tip:** We recommend automatically creating the tables, which is faster and more reliable. Database errors are more likely when tables are manually created. See [Setting Up RDBMS Databases, page 55](#).

## Creating projects from templates

You can use an existing project as a template to create a new project. Settings from the existing project are copied to the new project. This is helpful if you need to create similar projects using the same configuration, but want to manage items separately.

Issues, requirements, requirement documents, test cases, test runs, workbook tasks, and item-related data are not copied to the new project. See [Data not copied to new projects, page 11](#).

**Note:** Legacy TestTrack 2011.1 or earlier native projects must be upgraded before they can be used as templates for new projects. See [Upgrading projects, page 47](#).

1. Click **Projects**. You can also choose **View > Projects**.  
The Projects dialog box opens.
2. Select the project to use as a template.
3. Click **Create from Template**.  
The Create Project from Template dialog box opens.
4. Enter a **Project name**. The name is displayed when users log in to Helix ALM.
5. Select a **Project type**.
6. Specify additional project information.
  - If you are creating a Helix ALM native project, see [Creating native projects, page 7](#).
  - If you are creating an RDBMS project, see [Creating RDBMS projects, page 9](#).
7. Click **OK** to create the project.

### Data not copied to new projects

Issues, requirements, requirement documents, test cases, test runs, and workbook tasks are not copied to new projects created from templates. The following item-related data is also not copied.

- Audit log
- Custom field values set in items
- Emails and recipients
- File attachments
- Historical change information for items and folders
- Hyperlinks
- Issue reported by records
- Items in folders
- Links between items and link history
- Parent-to-child item associations in task boards
- Source control file attachments
- Surround SCM changelist information
- Workflow events added to items





# Configuring Server Options

Helix ALM's client/server design centralizes email, logging, and other options and shares them across all Helix ALM projects. You can configure the following server options.

Options	Use to:	More information
Logging	Select the type of information to add to the server log and set options to send email when events occur.	<a href="#">Setting log options, page 14</a>
Email sending	Specify email server connection information to allow users to send email from Helix ALM.	<a href="#">Setting email sending options, page 15</a>
Email tracking	Enable email tracking to save emails sent about specific Helix ALM items with the items and configure an email account for it.	<a href="#">Setting email tracking options, page 16</a>
Server	Change the server port used to communication with Helix ALM clients and set the local admin password.	<a href="#">Setting server options, page 18</a>
Server database	Change the Helix ALM Server database location or convert the database to a different type.	<a href="#">Configuring the server database location and type, page 19</a>
RDBMS connections	Create and modify connections to RDBMS databases to host the Helix ALM Server database and projects instead of using the native SQLite database format.	<a href="#">Adding RDBMS connections, page 22</a>
Client settings	Select options based on the different Helix ALM client types, such as the time to wait before disconnecting inactive clients from the server and automatic upgrades.	<a href="#">Setting client settings, page 24</a>
Security	Enable encryption for communication between Helix ALM clients and the server, manage RSA key exchange, and choose how to enforce security over backward compatibility.	<a href="#">Setting security options, page 26</a>
License server	Configure Helix ALM License Server connection information, the communication password, and global user cache refresh rate.	<a href="#">Setting license server options, page 31</a>
Auto update check	Select options to automatically check for Helix ALM upgrades.	<a href="#">Setting software update check options, page 32</a>

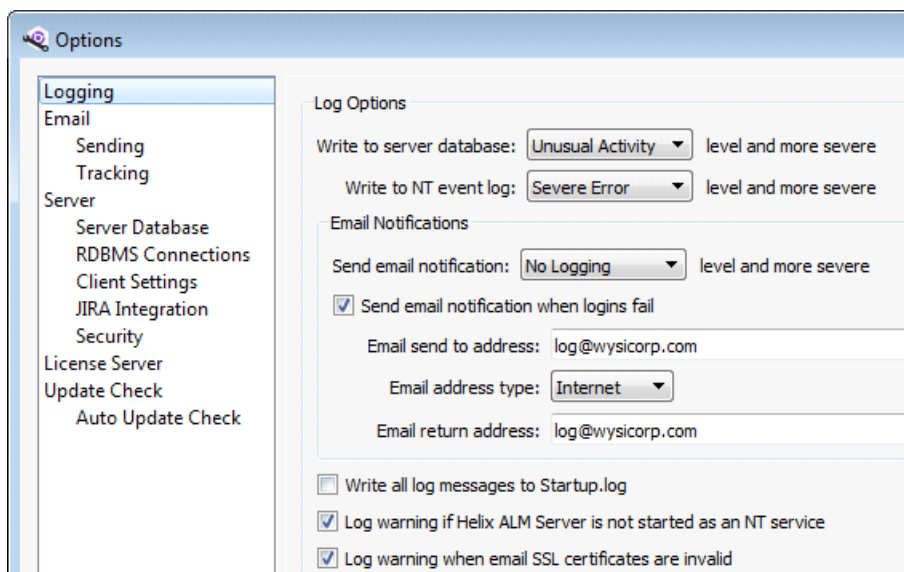
## Setting log options

The Helix ALM Server creates log files that record events, such as severe errors or unusual activity, to help you monitor server operations. The server can also send email based on these events.

See [Working with the Server Log, page 51](#) for information about viewing the server log.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.



2. In the Logging category, select any **Log Options**.
  - **Write to server database** level specifies the events to write to the server database log.
  - **Write to NT event log** or **Write to Unix system log** levels specify the events to write to the NT/2000 event log or the Unix system log.
3. Select **Email Notifications** options to send email when specific events occur.
  - **Send email notification** level specifies the types of events to email about. Select **No Logging** if you do not want to receive emails.
  - **Send email notification when logins fail** sends email when user logins fail.
  - Enter the **Email send to address**. All notifications are sent to this address.
  - Select the **Email address type**.
  - Enter the **Email return address**. Returned notifications are forwarded to this address.
4. Select **Write all log messages to Startup.log** to write errors to the log file.

Select this option if you are experiencing problems and want to log messages that occur after the Helix ALM Server starts. The log file is stored in the same directory as the server application.

**Note:** The startup log includes a list of active projects and the number of items in each project, which can be used to troubleshoot performance or caching issues. See [Startup Log Codes, page 61](#) for information about codes used to indicate item types.

5. Select **Log warning if Helix ALM Server is not started as an NT service** to add a warning to the server log if the server is started as an application. (Windows only)

Most organizations run the server application as a service. If it is started as an application, the Helix ALM Server is shut down by the operating system when a user logs out, which can negatively affect other users.

6. Select **Log warning when email SSL certificates are invalid** to add a warning to the server log if certificates used to verify the email server connection are invalid.

The warning is logged once every 24 hours when email is imported to or sent from Helix ALM and the certificates are invalid. A warning is always logged when testing the email connection in the email sending and tracking options in the admin utility.

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

## Setting email sending options

You must enable email and configure email server settings before users or the Helix ALM Server can send email.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select **Sending** from the Email category.

The screenshot shows the 'Options' dialog box with the 'Sending' tab selected. The 'Email' category is expanded, and 'Sending' is highlighted. The main area contains the following settings:

- Enable sending mail via Simple Mail Transport Protocol (SMTP)
- Authenticated login with the SMTP host will be attempted if a username is entered. Leave the username empty if authentication is not required.
- Host: mail.wysicorp.com
- SSL: SSL 3.0
- Port: 465
- Username: Administrator
- Password: [masked]
- Test Connection button
- Pause sending via SMTP
- Only send one message per SMTP connection

3. Select **Enable sending mail via Simple Mail Transport Protocol** to send email via SMTP.
4. Enter the SMTP information.
  - Enter the **Host** used to send outgoing mail. Enter an IP address (e.g., 123.34.5.26) or your mail server's fully qualified domain name (e.g., mail.yourcompany.com).
  - Select the **SSL** protocol to use to encrypt communication between the mail server and Helix ALM Server. You can use the Negotiate, SSL 3.0, STARTTLS 1.0, or TLS 1.0, 1.1, or 1.2 protocols. Select **<not set>** if you do not want to use a secure protocol.
  - Enter the **Port** number. The default port is 465 if you select an SSL protocol and 25 if you do not.
  - Enter a **Username** and **Password** if the SMTP host requires an authenticated login. Leave these fields empty if the host does not require authenticated login.

5. Click **Test Connection** to validate the connection to the email server.

The Connection Test Results dialog box opens. If the test connection fails, you can copy and paste the text into an email or text file and send it to your system administrator for help.

6. If you are experiencing SMTP problems, select the following options to help with troubleshooting.
  - **Only send one message per SMTP connection** sends one message per connection. Enable this option if the Helix ALM error log contains entries stating 'The SMTP host's reply code to the MAIL command was 503' or an entry stating 'only one MAIL per message'.
  - **Pause sending via SMTP** stops sending email via SMTP. Make sure you clear this option as soon as the problem is resolved because outgoing mail will back up in the queue.
7. Click **OK** to save the changes.

**Note:** Most mail servers have strong security, which may affect sending email from Helix ALM. Many servers require advanced authentication to execute a send mail command. Some servers may restrict some send mail types, such as multiple recipient sends and multiple send requests per SMTP connection. In some cases, virus scanners may add wrappers to an email, which can change the email to a point where the send mail commands it initiates are no longer recognizable by SMTP standards.

If you experience problems sending email, check the Helix ALM Server log. See [Working with the Server Log, page 51](#). If you know the specific SMTP error code, [search the knowledgebase](#) using the code for troubleshooting information.

## Setting email tracking options

Email tracking saves emails sent about specific issues, requirements, requirement documents, test cases, and test runs with the item. Users can view tracked emails on the item Overview or Email tab in the Helix ALM Client or Email tab in Helix ALM Web.

When a tracked email is sent, it includes a tracking cookie that identifies the project, the email, and the item it was sent from. The SMTP headers use either the user's email address or the project email notification account email address (if the email is sent by an automation rule) as the From user. The Helix ALM email tracking account name is used as the Reply To email address in the SMTP header of the tracked email.

If a reply to a tracked email is sent, the email is sent to the email tracking account specified in the Reply To SMTP header. The Helix ALM Server retrieves the email from the tracking account and uses the tracking cookie to identify the project and the email the reply was sent about. The reply email is then attached as a reply to the original email and forwarded to the email account of the user who sent the original email.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.
2. Select **Tracking** from the Email category.

The screenshot shows the 'Options' dialog box with the 'Tracking' tab selected. The 'Enable tracking mail' checkbox is checked. Below it, a note states: 'Helix ALM requires a dedicated email account. Do not use a personal account because all email is imported into the project then deleted from the account.' The configuration fields are: Protocol: POP, Host: mail.wysicorp.com, SSL: SSL 3.0, Port: 995, Username: trackedmail@wysicorp.pom, Password: masked with dots, Return email address: returnedmail@wysicorp.com. There is a 'Test Connection' button. At the bottom, there are two time-to-wait fields: 'Time to wait for initial connection response (seconds): 1' and 'Time to wait for other connection responses (seconds): 20'. A checkbox at the bottom is labeled 'Automatically remove emails without tracking cookies from the mail server'.

3. Select **Enable tracking mail** to track emails.

**Note:** Use a dedicated account for email tracking purposes. All email received by the account is imported to Helix ALM and then deleted from the account. Helix ALM cannot differentiate between personal and business email.

4. Enter information about the email account used to send tracked email.
  - Select the email **Protocol**. You can use POP or IMAP.
  - Enter the **Host** IP address or domain name.
  - Select the **SSL protocol** to encrypt communication between the mail server and Helix ALM Server. You can use the Negotiate, SSL 3.0, STARTTLS 1.0, or TLS 1.0, 1.1, or 1.2 protocols. Select **<not set>** if you do not want to use a secure protocol.
  - Enter the **Port** number. The default POP port is 995 if you select an SSL protocol and 110 if you do not. The default IMAP port is 993 if you select an SSL protocol and 143 if you do not.
  - Enter the **Username** and **Password** if the host requires an authenticated login. The Helix ALM Server uses this information to log in to the email server to retrieve tracked email. Leave these fields empty if the host does not require authenticated login.
  - Enter the **Return Email Address** used by the Helix ALM Server to send tracked email. When a user replies to tracked email, the email is returned to the Helix ALM Server and then attached to the corresponding item before it is forwarded to the user who sent the original message.
5. Click **Test Connection** to validate the connection to the mail server.  
The Connection Test Results dialog box opens. If the test connection fails, you can copy and paste the text into an email or text file and send it to your system administrator for help.
6. Enter the **Time to wait for initial connection response**.  
This is the time the Helix ALM Server waits for an initial response from the email server. The valid range is 1-32767 seconds.
7. Enter the **Time to wait for other connection responses**.

This is the time the Helix ALM Server waits for connection responses from the email server. The valid range is 1-32767 seconds.

8. Select **Automatically remove emails without tracking cookies from the mail server** to delete emails that do not include a tracking cookie.

You may want to select this option if the email tracking account receives spam or other email you do not want to import into Helix ALM.

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

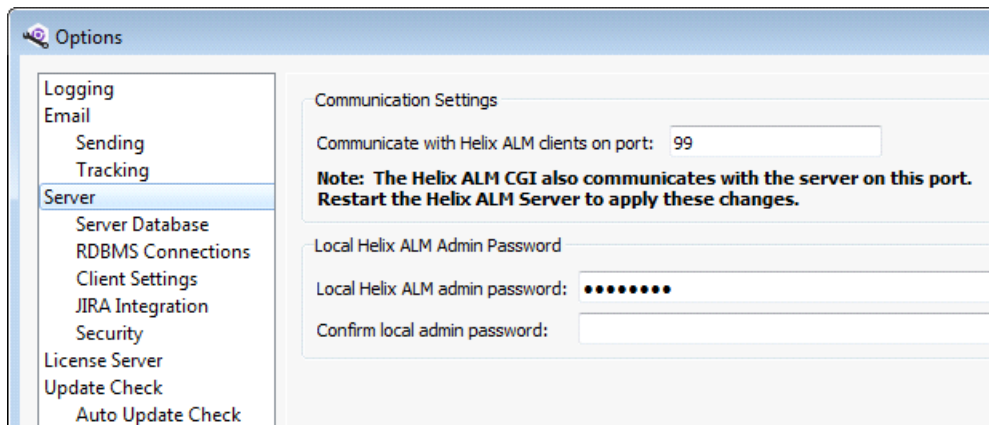
## Setting server options

You can change the local Helix ALM admin password and port number the Helix ALM Server uses to communicate with clients.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **Server** category.



3. Enter the port number the Helix ALM Server uses to communicate with Helix ALM clients. The default port is 99.

If you change the port, make sure users update their server connections. The valid range is 1-65535.

4. Enter and confirm a new password to change the **Local Helix ALM admin password**.

If your existing administrative username and password are not recognized, you can log in using the local Helix ALM admin password. This password only provides access to server options and server admin utility users.

We strongly recommend that you change this password. The default password, **admin**, is not secure and allows any user to log in and access server options and server admin utility users.

**Note:** You can also use this password to correct license server communication settings if the Helix ALM Server cannot connect to the Helix ALM License Server.

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

## Configuring the server database location and type

Helix ALM Server settings are stored in the server database. Each server has its own database. You can change the location of the server database or convert the database to a different type.

By default, native server databases are stored in the following locations on the server computer:

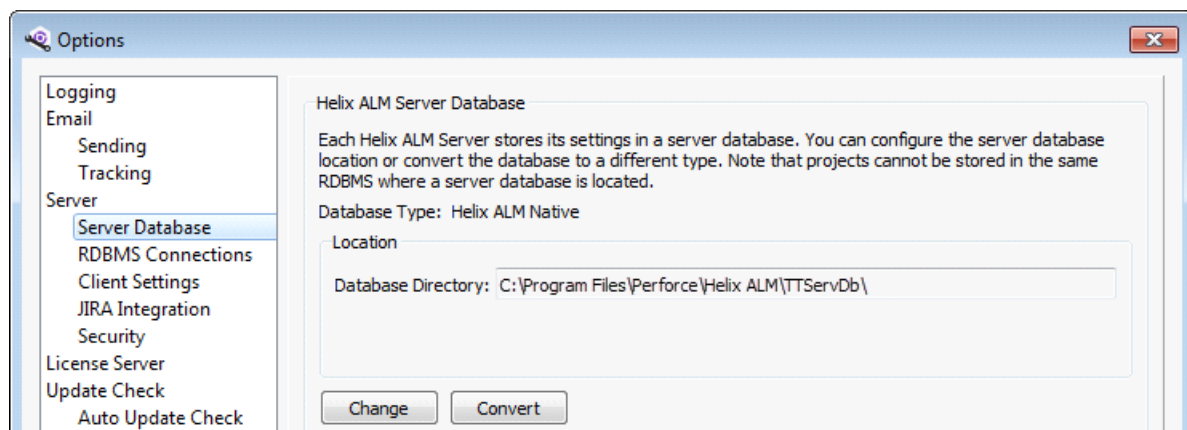
- Windows—C:\Program Files\Perforce\Helix ALM\TTServDb
- Linux—/var/lib/HelixALM/TTServDb

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **Server Database** category.

The current server database type and location are displayed.



3. Click **Change** to change the database location. See [Changing the server database location, page 19](#).
4. Click **Convert** to convert the database to a different type. See [Converting the server database type, page 20](#).

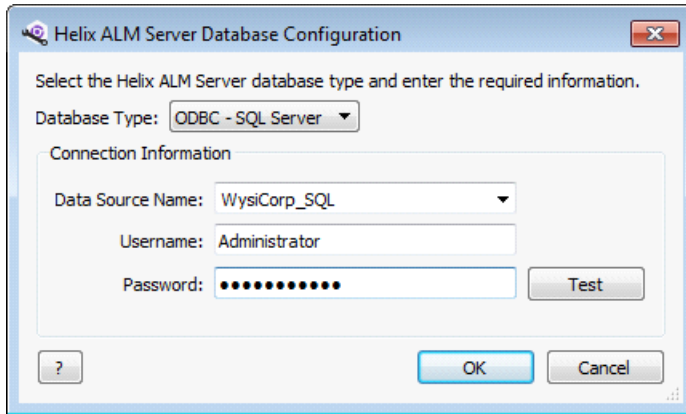
## Changing the server database location

You can configure the Helix ALM Server to use a different database. For example, you can change the database if you move it 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.

**Note:** When you start the 64-bit Helix ALM Server for the first time, a native SQLite server database (ttserv.db) is automatically created if one does not exist.

1. Make sure you are logged in to the server to change. Choose **File > Connect to Server** to connect to a different server.
2. Click **Server Options**. You can also choose **View > Server Options**.  
The Options dialog box opens.
3. Select the **Server Database** category.
4. Click **Change**.

The Helix ALM Server Database Configuration dialog box opens.



5. Select a **Database Type**. The available fields change depending on the selected type.
6. Enter the **Connection Information**.

You are not prompted for connection information or to test the connection if you are changing to Helix ALM native format. The server automatically points to the database in the Helix ALM database directory on the server computer.

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

The Test Connection dialog box opens and displays the results. If the test connection fails, you can copy and paste the text into an email or text file and send it to your DBA for help.

8. Click **Close** to close the Test Connection dialog box.

You return to the Helix ALM Server Database Configuration dialog box.

9. Click **OK** to change the database location.

The following information is verified if you selected an RDBMS database:

- The specified connection information leads to a valid RDBMS.
- A Helix ALM Server application is not configured for the selected server database.
- All of the required database tables exist and are accessible.

**Note:** If the selected server database is in use by another Helix ALM Server, you can 'steal' it. This allows you to associate a server database with a new Helix ALM installation in situations where the existing server becomes unusable.

10. You return to the Options dialog box. Click **OK** to apply the changes.

You must stop and restart the Helix ALM Server to complete the process.

## Converting the server database type

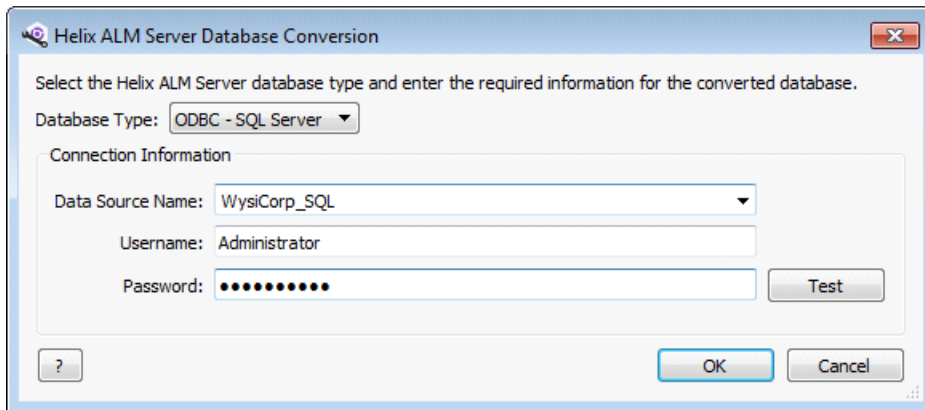
You can convert the server database to Helix ALM native, SQL Server, Oracle Native, or PostgreSQL format. Keep the following in mind before you start the conversion:

- All other users must be logged out of the Helix ALM Server.
- The destination database cannot be in use by another server.



- All of the tables in the destination database must be empty except for the serverid, ownerlck, and RDBMSOptions tables.
  - Legacy TestTrack 2011.1 or earlier native server databases must be upgraded or converted to RDBMS format before upgrading to the 64-bit server. See [Upgrading projects, page 47](#) and [Converting projects, page 47](#).
  - If you are converting to a SQL Server database, you must add a unique data source name (DSN) on the Helix ALM Server computer to connect to the database. See [Creating DSNs for SQL Server Databases](#).
1. Make sure you are logged in to the server to change. Choose **File > Connect to Server** to connect to a different server.
  2. Click **Server Options**. You can also choose **View > Server Options**.  
The Options dialog box opens.
  3. Select the **Server Database** category.
  4. Click **Convert**.

The Helix ALM Server Database Conversion dialog box opens.



5. Select a **Database Type**. The available fields depend on the selected type.
6. Enter the **Connection Information**.  
You are not prompted for connection information or to test the connection if you are converting to Helix ALM native format. The existing server database is moved to the old subdirectory in the Helix ALM database directory when the conversion finishes.
7. Click **Test** to test the connection.  
The Test Connection dialog box opens and displays the results. If the test connection fails, you can copy and paste the text into an email or text file and send it to your DBA for help.
8. Click **Close** to close the Test Connection dialog box.  
You return to the Helix ALM Server Database Conversion dialog box.
9. Click **OK** to convert the database.  
The server database conversion information is sent to the Helix ALM Server for validation.
  - If the validation succeeds, you are prompted to start the conversion. Remember that users cannot log in during the conversion process.

- If the validation fails, make sure the Helix ALM tables exist and are empty, except for the serverid, ownerlck, and RDBMSOptions tables. You should also make sure that all other users are logged out of the server and that another server is not using the database.

10. Click **Yes**.

The Conversion Status dialog box opens and the conversion starts.

11. Click **Close** when the conversion finishes.

You are prompted to use the converted server database.

12. Click **Yes**.

You must stop and restart the Helix ALM Server to complete the conversion.

**Note:** You can also manually change the database the Helix ALM Server is using. See [Changing the server database location, page 19](#).

## Adding RDBMS connections

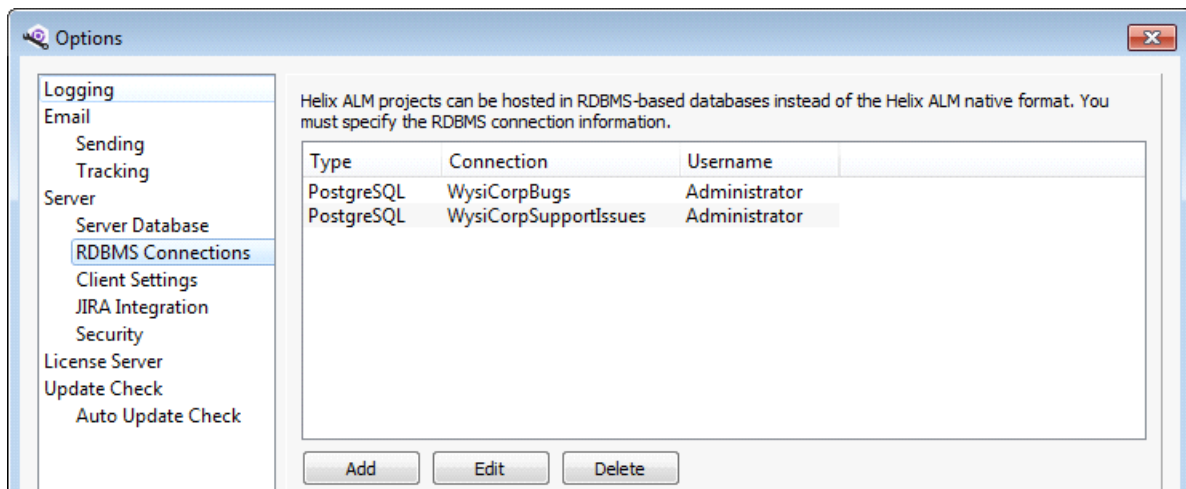
You can store the Helix ALM projects in a different RDBMS if you do not want to use the Helix ALM native database format (SQLite). You must create connections to the RDBMS databases to use.

**Note:** You can also store the Helix ALM Server database in a different RDBMS. See [Converting the server database type, page 20](#).

1. Click **Server Options**. You can also choose **View > Server Options**.

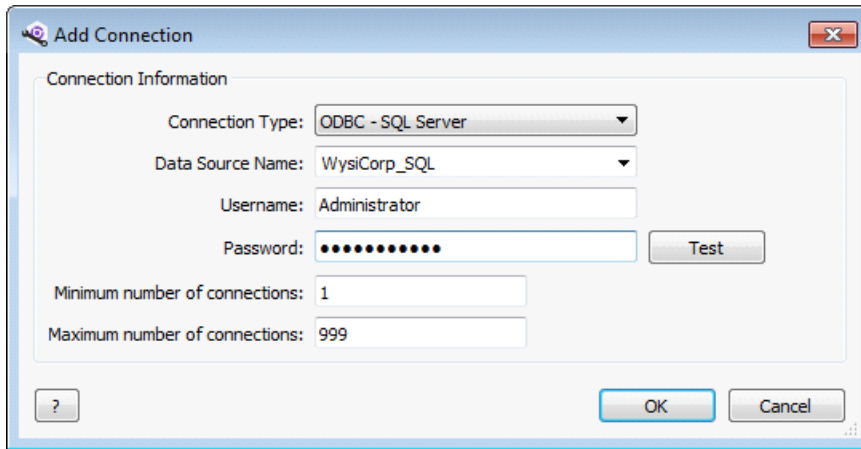
The Options dialog box opens.

2. Select the **RDBMS Connections** category.



3. Click **Add** to add a new RDBMS connection.

The Add Connection dialog box opens.



4. Select a **Connection Type**. The available fields depend on the selected type.
5. Enter the RDBMS connection information.
  - **Oracle**—Enter the **Service Name** of the host to connect to, **Port**, and **Username** and **Password**.
  - **PostgreSQL**—Enter the **Database Name**, **Host Name**, **Port**, and **Username** and **Password**.
  - **ODBC - SQL Server**—Select or enter a **Data Source Name (DSN)**. Only ODBC system DSNs are supported. Enter the SQL Server **Username** and **Password**. If the DSN is configured to use Windows NT authentication, leave these fields empty. The username and password of the logged in user on the Helix ALM Server computer is automatically used.

**Note:** If you use SQL Server, the server database and each database used to host Helix ALM projects must have a unique DSN. See [Creating DSNs for SQL Server Databases](#).

6. Enter the **Minimum number of connections** to specify the smallest number of connections to cache in the database connection pool. The default value is 1.
 

When the Helix ALM Server starts, it automatically creates the specified number of database connections. Increasing this number can improve performance because the server does not need to create a database connection later. If you increase this number, you may need to purchase additional licenses from the database vendor.
7. Enter the **Maximum number of connections** to specify the largest number of connections to cache in the database connection pool.

The default number of connections is 999. Only change this number if you have a large number of projects and are using too many connections to the backend database.

**Note:** If you are using Oracle, you may need to decrease this number to match the number of Oracle connections you have licensed.

8. Click **Test** to validate the connection.
 

The Test Connection dialog box opens and displays the results. If the test connection fails, you can copy and paste the text into an email or text file and send it to your DBA for help.
9. Click **Close** to close the Test Connection dialog box.
 

You return to the Add Connection dialog box.
10. Click **OK**.

The connection is added.

## Editing and deleting RDBMS connections

You can edit the information for an RDBMS connection if it changes. If the connection is used for active projects, or inactive projects with logged in users, you can only change the number of connections.

You can also delete RDBMS connections if they are no longer used. You cannot delete an RDBMS connection if it is used for a project.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **RDBMS Connections** category.
3. Edit or delete the connection.
  - To edit a connection, select it and click **Edit**. Make any changes and click **OK**.
  - To delete a connection, select it and click **Delete**. Click **Yes** to confirm the deletion.
4. Click **OK** to save the changes.

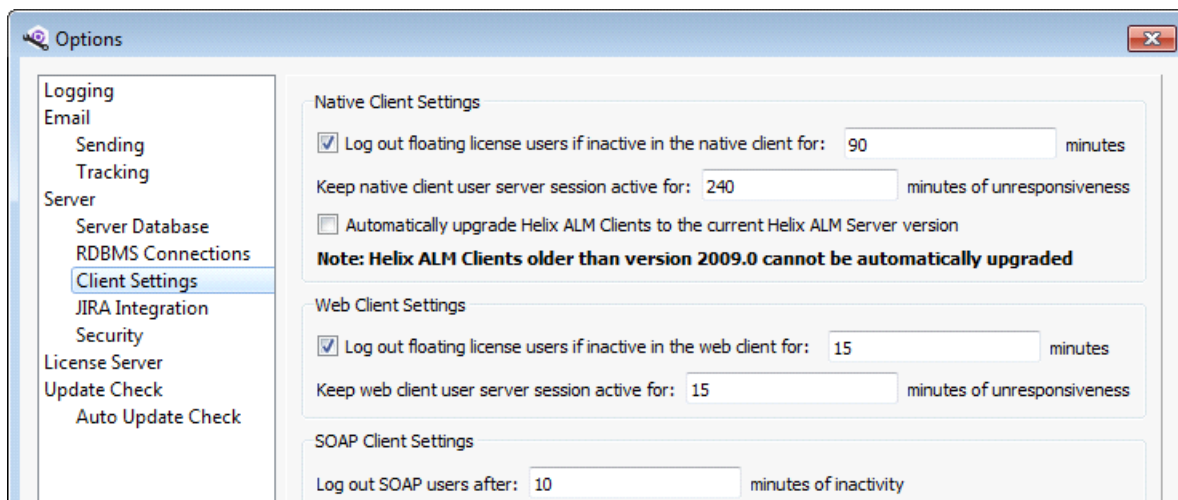
## Setting client settings

You can specify limits to automatically log out users and disconnect inactive Helix ALM clients from the server to release floating licenses for other users. You can also enable automatic client upgrades.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **Client Settings** category.



3. Select any **Native Client Settings**.
  - Select **Log out floating license users if inactive in the native client** to automatically log out floating license users from the Helix ALM Client if they do not interact with it for the specified number of minutes. A warning dialog box is displayed if users do not use the mouse or keyboard before the inactivity limit is reached. Users have 60 seconds to choose to stay logged in before all windows and

dialog boxes are closed and any unsaved changes are lost. If selected, the default value is 90 minutes and the valid range is 5-1440 minutes.

**Note:** Users are not logged out if Helix ALM is performing an action that displays a status or progress dialog box, such as duplicating items or importing an XML file. The inactivity timer continues when the action is complete.

- Enter the number of minutes to **Keep native client user server session active**. The Helix ALM Client periodically pings the Helix ALM Server. If the client cannot communicate with the server within the specified number of minutes, the user session is terminated. The client and server cannot communicate if the network connection is lost or if the client is closed. The default value is 240 minutes and the valid range is 5-1440 minutes.
- Select **Automatically upgrade Helix ALM Clients to the current Helix ALM Server version** to enable automatic upgrades of all Helix ALM clients connecting to the Helix ALM Server. Enabling automatic upgrades ensures that all users are using the correct version.

4. Select any **Web Client Settings**.

- Select **Log out floating license users if inactive in the web client** to log out floating license users from Helix ALM Web if they do not interact with it for the specified number of minutes. A warning dialog box is displayed if users do not use the mouse or keyboard in the browser before the inactivity limit is reached. Users have 60 seconds to choose to stay logged in before all pages and dialog boxes are closed and any unsaved changes are lost. If selected, the default value is 90 minutes and the valid range of minutes is 5-1440.

**Note:** Users are not logged out if Helix ALM is performing an action that displays a status or progress dialog box, such as duplicating items. The inactivity timer continues when the action is complete.

- Enter the number of minutes to **Keep web client user server session active**. Helix ALM Web periodically pings the Helix ALM Server and is considered responsive as long as the browser is open and Helix ALM Web can communicate with the server. If Helix ALM Web is no longer responsive, the user is logged out. The default value is 15 minutes and the valid range is 5-1440 minutes.

**Note:** Keep in mind that closing the browser without logging out first may not close the session and release the license. Setting the unresponsiveness limit ensures that licenses are eventually released.

5. Enter the number of minutes of inactivity to wait to automatically **Log out SOAP users**.

SOAP users are logged out of if they do not submit a request to the Helix ALM Server within the specified number of minutes. If the SOAP application does not call the Logout() method, the session remains active and the license is not released. Setting the inactivity limit ensures that licenses are eventually released. The default value is 10 minutes and the valid range is 5-1440 minutes.

**Note:** SOAP users are not prompted if the period of inactivity is reached and they are logged out.

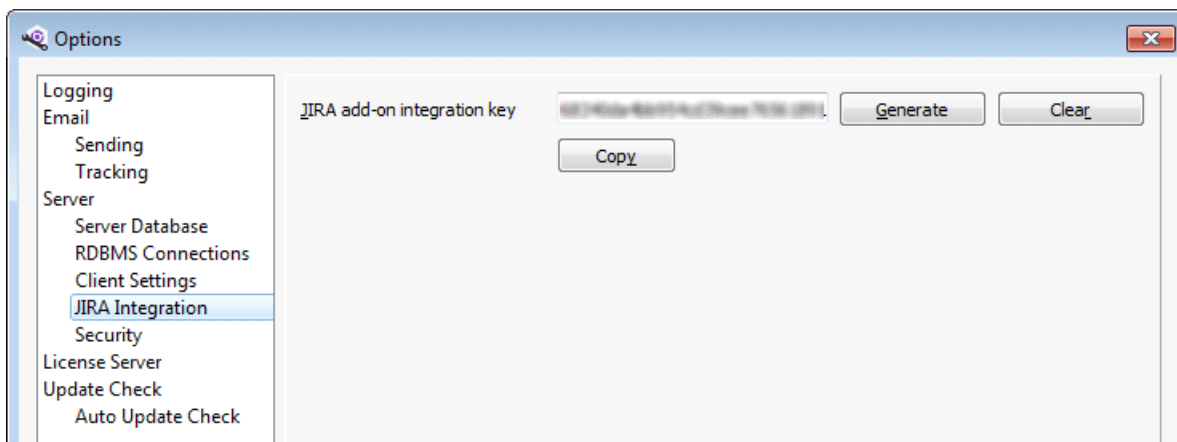
6. Click **OK** to save the changes.

## Setting JIRA integration options

To view attached Helix ALM items in JIRA, you must configure the Helix ALM for JIRA add-on in JIRA. The configuration requires an integration key, which provides security between JIRA and the Helix ALM Server.

You can generate a key from JIRA when you configure the add-on or generate it in the server admin utility. You can also copy the existing key or clear the key if you no longer use the add-on.

1. Click **Server Options**. You can also choose **View > Server Options**.  
The Options dialog box opens.
2. Select the **JIRA Integration** category.



3. Click **Generate** if a key does not exist or to generate a new key. The generated key is displayed.  
You must update the key in the add-on configuration in JIRA before users can view attached Helix ALM items.
4. Click **Copy** to copy the key to the clipboard. You can then easily paste it in the add-on configuration in JIRA.
5. Click **Clear** to delete the key and prevent JIRA from retrieving data from the Helix ALM Server.  
If you delete the key, users can no longer view attached items in JIRA.
6. Click **OK** to save the changes.

## Setting security options

You can enable encryption to secure client/server communication. Encryption scrambles data to prevent interception, or eavesdropping, as it passes between clients and the Helix ALM Server. You can also use RSA key exchange for stronger encryption keys if your network is potentially insecure or if users log in to Helix ALM from outside of your network.

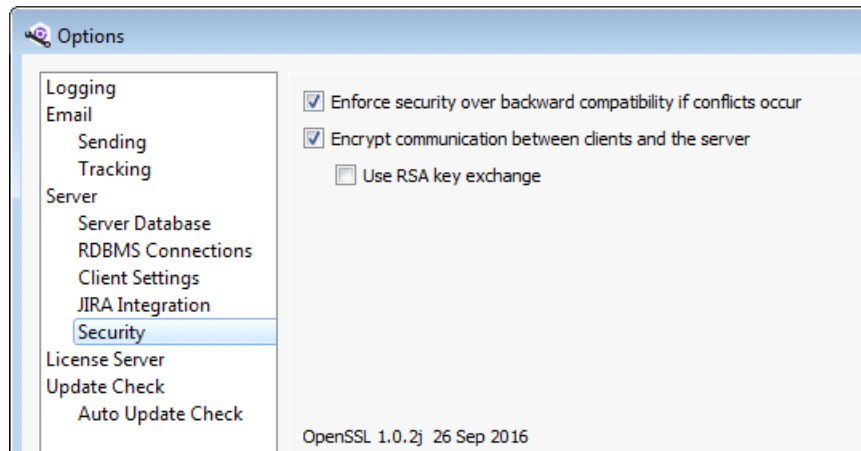
See [Securing communication between clients and the Helix ALM Server, page 28](#) for information about encryption, authentication, and key exchange methods used in Helix ALM.

**Tip:** Review the [Security Best Practices](#) for information about properly managing and securing your Helix ALM and license server data.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **Security** category.



**Tip:** The OpenSSL version used by Helix ALM is displayed. Any vulnerabilities found in OpenSSL are published on the [OpenSSL web site](http://www.openssl.org) ([www.openssl.org](http://www.openssl.org)). To check if OpenSSL version displayed in Helix ALM has vulnerabilities that impact Helix ALM, check the [knowledgebase](#) or contact [Perforce Support](#) for information.

3. Select **Enforce security over backward compatibility if conflicts occur** to always enforce the selected encryption option even if a client does not support it.

For example, if this option is selected and an old Surround SCM version is integrated with Helix ALM, a security error is displayed and the integration will not work because Surround SCM does not support the same security as Helix ALM.

4. Select **Encrypt communication between clients and the server** to encrypt all communication between clients and the Helix ALM Server, which reduces the likelihood of eavesdropping by hackers.

Encryption increases security, but may slightly affect performance. Select this option if you organization's network is secure and no client applications outside of the network communicate with the server.

**Tip:** Always use encryption to keep data secure unless you are evaluating Helix ALM or troubleshooting performance issues.

5. Select **Use RSA key exchange** to use strong key exchange for communication between clients and the Helix ALM Server.

RSA is a public key encryption algorithm that uses separate keys for encryption and decryption. Select this option if your organization stores sensitive information in Helix ALM and users log in to client applications outside of your network using a username and password. If you use RSA, the public key must be added to all clients that access the Helix ALM Server. See [Configuring RSA key exchange, page 30](#) for information about setting up RSA.

**Note:** This option is only available if **Encrypt communication between clients and the server** is selected.

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

## Changing key exchange options

If you change key exchange options, Helix ALM client applications and the web server that hosts Helix ALM web clients must be updated. The following scenarios require further action after changing security settings.

If you use:	And you change it to:	You need to:
No encryption	RSA key exchange	Download a settings file that Helix ALM client users need to import in the server connection settings. If you use Helix ALM web clients, import the file in the Helix ALM Registry Utility on the web server computer.
RSA key exchange	No encryption or basic encryption (Encrypt server communication between clients and the server is selected)	Remove the public key fingerprint from any clients that connect to the server. Click <b>Remove</b> in the server connection information in clients and in the CGI options for server in the Helix ALM Registry Utility.

See [Configuring RSA key exchange, page 30](#) for information about adding and removing keys in Helix ALM clients.

## Securing communication between clients and the Helix ALM Server

Keeping your Helix ALM data secure is critical. To prevent hackers from compromising your data, encrypt communication between clients and the Helix ALM Server.

The following information explains how Helix ALM encrypts data, how authentication works, and how key exchange is used for different authentication methods. See [Setting security options, page 26](#) for information about configuring secure client/server communication.

### Encryption

Encryption scrambles data to prevent interception, or eavesdropping, as it passes between clients (Helix ALM Client, Helix ALM Web, server admin utilities, and add-ins) and the Helix ALM Server. Helix ALM uses the OpenSSL implementation of Advanced Encryption Standard-256 (AES-256) to encrypt communication between clients and servers in Helix ALM (and TestTrack 2014.1 and later). RC4 encryption is used for backward compatibility with earlier TestTrack and Surround SCM versions.

Client/server communication is encrypted when you select **Encrypt communication between clients and the server** in the Security server options. See [Setting security options, page 26](#).

**Note:** Always use encryption unless you are evaluating Helix ALM or troubleshooting a performance issue. Passwords are always encrypted even if client/server communication is not.

Login credentials sent from web clients to the CGIs are not encrypted, even if encryption is enabled on the server. We strongly recommend configuring HTTPS to encrypt communication from the browser to the CGIs on the web server. See your web server documentation for information about configuring and using HTTPS.



## Authentication

Authentication is the process of logging in a user. The following authentication methods are used in Helix ALM.

Authentication method	How it works
Helix ALM License Server	The username and mathematical proof that the user knows the password (not the actual password) are sent to the Helix ALM Server. The server sends different mathematical proof that it knows the password to the client.
LDAP	Using single sign-on—Credentials proving the user's identity are sent from the LDAP server to the Helix ALM Server and verified.
	Not using single sign-on—The username and password are sent to the Helix ALM Server.
External authentication	Data from the organization's authentication system is sent to the Helix ALM Server.

## Key exchange

Key exchange is a method of exchanging secret keys over an insecure network connection without exposing them to eavesdroppers. The key exchange method used depends on the authentication method.

The following key exchange methods are used in Helix ALM.

Key exchange method	When it is used	How it works	To use it:
Secure Remote Password (SRP)	User is authenticated from the Helix ALM License Server and RSA key exchange is not enabled	A shared secret key is generated during authentication. To compromise the secret key or impersonate the server, a hacker must know the user's password.	Select <b>Encrypt communication between clients and the server</b> in the Security server options.
Diffie-Hellman	User is authenticated using LDAP or external authentication, and RSA key exchange is not enabled	A mathematical process is used to generate a secret key. To compromise the secret key, a hacker must have control over an intermediate network node or impersonate the real server. Does not protect against man-in-the-middle attacks.	Select <b>Encrypt communication between clients and the server</b> in the Security server options.

Key exchange method	When it is used	How it works	To use it:
RSA	RSA key exchange is enabled in the Security server options	The client generates a random, 256-bit secret key and encrypts it with the server's public key. The server hashes the secret key and signs the hash with its private key. The private key is only stored on the server hard drive and never leaves the server. To compromise the secret key or impersonate the server, a hacker must know the server's private key or substitute their own public key in client applications.	Select <b>Encrypt communication between clients and the server</b> and <b>Use RSA key exchange</b> in the Security server options.

### When to use RSA key exchange

SRP and Diffie-Hellman are low risk key exchange methods if your organization's network is secure and no client applications outside of the network can communicate with the Helix ALM Server.

We recommend using RSA key exchange to prevent hackers from eavesdropping on communication if:

- Your organization stores sensitive information in Helix ALM.
- Your network is potentially insecure.
- Users log in to client applications from outside your network.
- Users are authenticated to Helix ALM using LDAP, single sign-on, or external authentication.

Using RSA requires additional setup for users. See [Configuring RSA key exchange, page 30](#).

## Configuring RSA key exchange

RSA is a public key encryption algorithm that uses separate keys for encryption and decryption. You may want to use RSA key exchange if your organization stores sensitive information in Helix ALM and users log in using a username and password from client applications outside of your network.

If you use RSA key exchange, a public key fingerprint must be imported to all client applications that connect to the Helix ALM Server.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **Security** category.
3. Select **Encrypt communication between clients and the server** and **Use RSA key exchange**.

A public key is generated on the Helix ALM Server. The Fingerprint field displays the public key fingerprint, which is a short version of the public key. Public and private keys are stored in the rsakeys directory in the Helix ALM application directory on the server computer. To keep these key files secure, make sure only the user that runs the Helix ALM Server has read and modify access to them.

**Note:** If you clear the **Use RSA key exchange** option, you are prompted that all users will need to modify their server settings. Click **OK** if you no longer want to use RSA. Make sure the public key fingerprint is removed from server connection settings in desktop clients and server settings in the Helix ALM Registry Utility for web clients.

- Click **Download Public Key** to save an XML file that contains the Helix ALM Server address, port number, and public key fingerprint.

This file must be distributed to users so they can import it to clients that connect to the server. Make sure the file is securely stored and only administrative users have access to modify it. If a hacker has unauthorized access to the file, changes it, and it is imported to clients, your installation could be hacked.

**Note:** The server address in the XML file includes the default hostname of the server computer. If users connect to the server from outside the local network, you must manually update the server address in the server settings file before providing it to users.

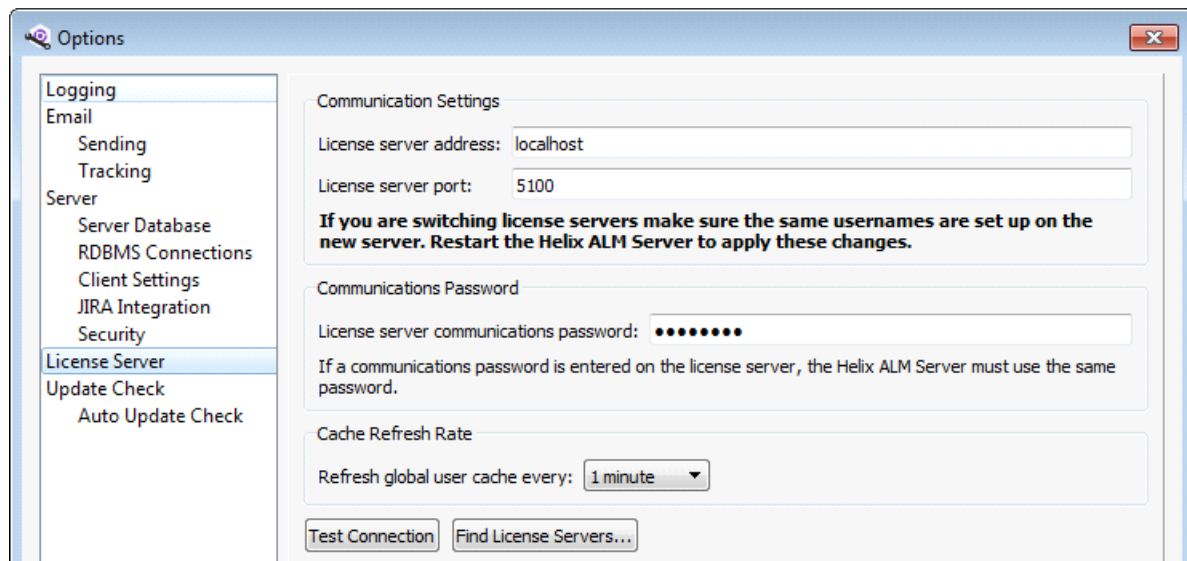
- Click **OK** to save the changes.
- Import the server settings file to Helix ALM clients or CGIs that connect to the server.
  - Helix ALM Client and add-ins—See the [Helix ALM help](#).
  - Helix ALM Server Admin Utility—See [Adding server connections, page 4](#).
  - Helix ALM web clients—See the [Registry Utility help](#).

**Tip:** If you suspect the private key on the server was compromised because of unauthorized server access, regenerate the public and private key pair. Click **Regenerate Key Pair** and click **OK** when you are prompted to generate the new keys. If you regenerate the keys, you must download a new server settings file and update all client applications that connect to the server.

## Setting license server options

Change the license server address and port if you move or use a different license server. You can also set a communications password and how often to update the global user cache.

- Click **Server Options**. You can also choose **View > Server Options**.  
The Options dialog box opens.
- Select the **License Server** category.



- Enter the **License server address** and **port** you want the Helix ALM Server to connect to.

Click **Find License Servers** to search for available servers. See [Finding license servers, page 32](#).

**Note:** If you change the license server address or port, you must restart the Helix ALM Server to apply the changes.

4. Optionally enter a **License server communications password**.  
The password provides additional security by preventing unauthorized users from using licenses. If you change the communications password, you must use the same password in Helix ALM. Users cannot log in to Helix ALM if the passwords do not match.
5. Select a **Cache Refresh Rate** to specify how often the Helix ALM Server checks with the license server for new users or changes to existing users.
6. Click **Test Connection** to test the license server connection.  
If the connection fails, check the address, port number, and password.
7. Click **OK** to save the changes.

## Finding license servers

If you do not know the Helix ALM License Server address, you can search for license servers running on your network and connect to the correct one.

1. Click **Server Options**. You can also choose **View > Server Options**.  
The Options dialog box opens.
2. Select the **License Server** category.
3. Click **Find License Servers** to find all license servers on the network.  
When the search is complete, the Find License Servers dialog box opens. To find servers with an IPv6 address, select **Include IPv6 in scan** and click **Refresh**.
4. Select the license server to use and click **Select**.  
The license server is selected.

## Setting software update check options

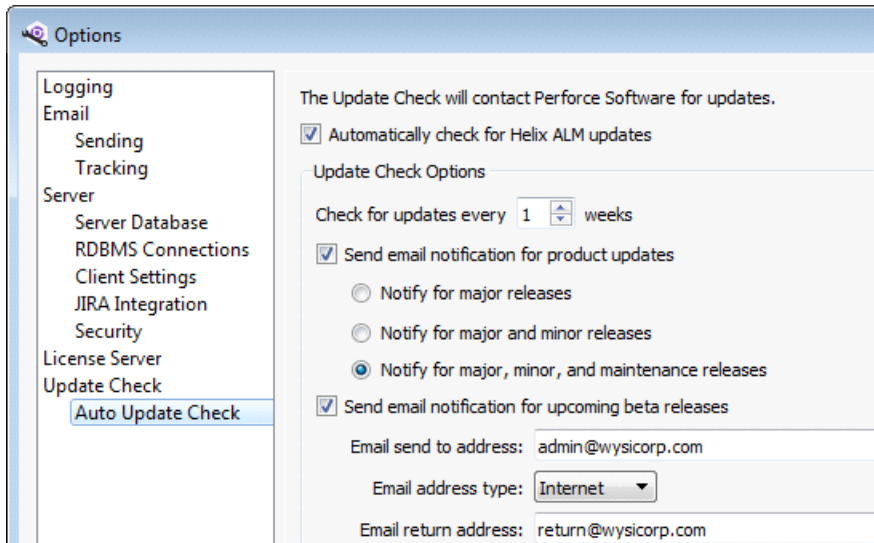
You can configure Helix ALM to check for updates or to notify you about beta releases. Software is not automatically downloaded and installed.

The Helix ALM Server encodes the following information and sends it to the Perforce update server, which returns update information.

- **Unique user ID**—A unique ID, generated by the Helix ALM Server, used to identify each server. It does not include any information that identifies your company or users.
- **Helix ALM version**—The installed Helix ALM Server version.
- **Operating system and version**—The operating system and version of the computer hosting the Helix ALM Server, including if it is 32-bit or 64-bit.
- **Client connections**—The timestamp when Helix ALM clients connect to the Helix ALM Server. This information also includes the client type, browser used by web clients, and the client operating system.

- **Licenses**—The number of Helix ALM licenses on the Helix ALM License Server and if they are evaluation licenses.
- **Product components**—Specifies if the following components are used: issue management, requirements management, test case management, SoloSubmit, multiple logins, stamping, email tracking, email sending, controlled hyperlinks, RSS feeds, audit trail, and electronic signatures.
- **JIRA integrations**—The number of configured JIRA integrations and attached items on the Helix ALM Server.
- **Configuration settings**—Specifies if the following settings are configured: security groups, dashboards, dashboard widgets, triggers, reports, filters, custom fields, pop-up menu values, folders, and link definitions.

1. Click **Server Options**. You can also choose **View > Server Options**.  
The Options dialog box opens.
2. Select the **Auto Update Check** category.



3. Select **Automatically check for Helix ALM updates** to enable the update check.  
After an update check is performed, information about available upgrades is displayed in the Update Check category. See [Viewing software update information, page 34](#).
4. Select any **Update Check Options**.
  - Enter how often Helix ALM should check for updates.
  - Select **Send email notification for product updates** to receive emails about updates. The email includes the product version and release notes. Select the type of releases to be notified about.
  - Select **Send notification for upcoming beta releases** to be notified about beta programs.
  - Enter your email information if you enabled either notification option.
5. Click **OK** to save the changes.

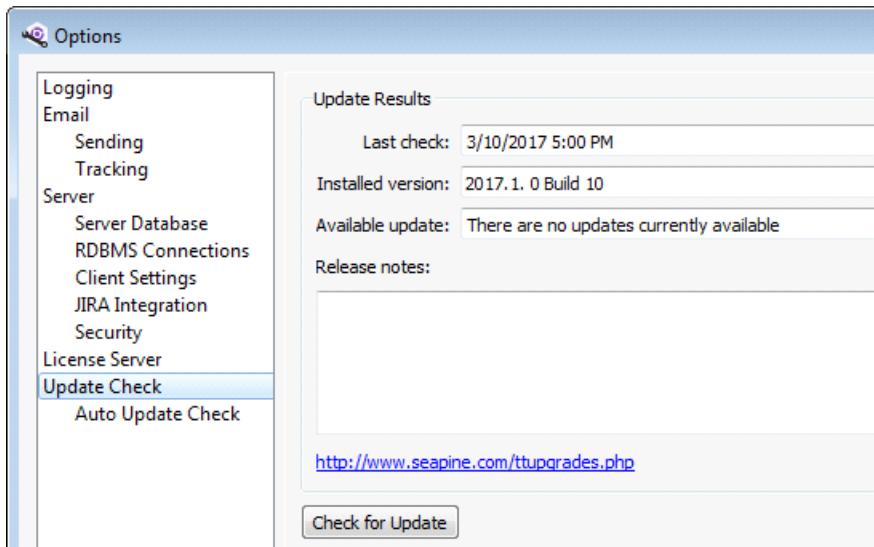
## Viewing software update information

You can manually check for Helix ALM software updates or view update information after an automatic update check is performed.

1. Click **Server Options**. You can also choose **View > Server Options**.

The Options dialog box opens.

2. Select the **Update Check** category.



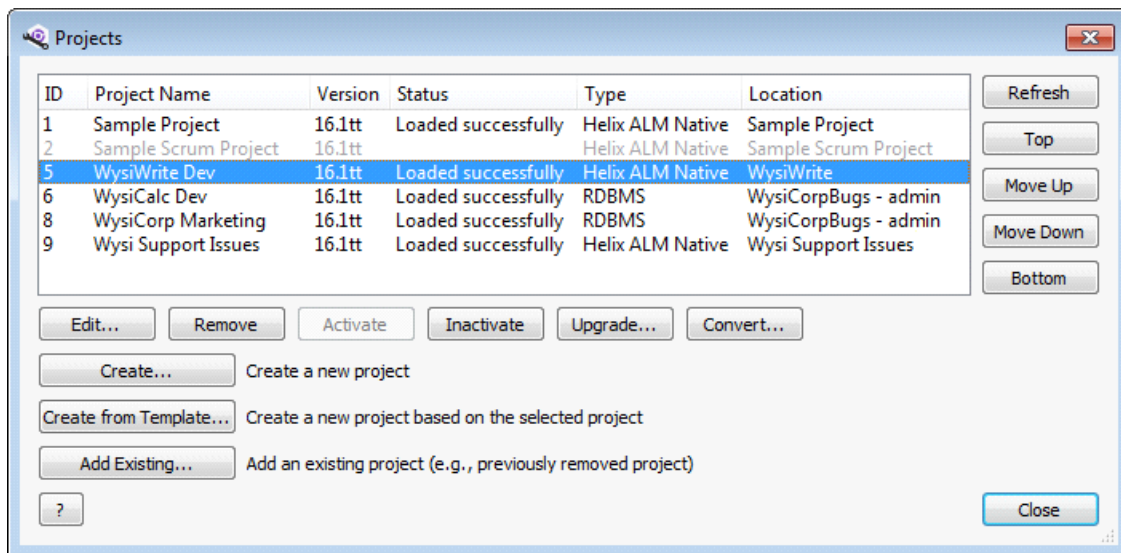
3. Click **Check for Update**.

If an update is available, the release notes are displayed. To download an update, click the link to go to Perforce's web site.

# Managing Projects

Helix ALM projects contain all the information your team tracks, including issues, test cases, test runs, requirements, requirement documents, security groups, users, customers, filters, test configurations, and workbook tasks. Projects are created on the Helix ALM Server and managed using the Helix ALM Server Admin Utility. See [Creating Projects, page 7](#).

The Projects dialog box displays the Helix ALM native and RDBMS projects on the server. From this dialog box, you can create new projects or add, edit, remove, activate, and inactivate existing projects. You can also upgrade projects to the current version, convert Helix ALM native projects to RDBMS projects, and change RDBMS projects to use different databases.



- To view the projects list, click **Projects**. You can also choose **View > Projects**.
- To create a new project, click **Create**. See [Creating native projects, page 7](#) and [Creating RDBMS projects, page 9](#). To create a project based on an existing project, select the project to use as the template and then click **Create from Template**. See [Creating projects from templates, page 10](#).
- To add an existing project, click **Add Existing**. See [Adding existing Helix ALM native projects, page 36](#) and [Adding existing RDBMS projects, page 37](#).
- To edit a project, select it and click **Edit**. See [Editing project settings, page 39](#).
- To inactivate or activate a project, select it and click **Inactivate** or **Activate**. See [Inactivating and activating projects, page 41](#).
- To upgrade a project to the current Helix ALM version, select it and click **Upgrade**. See [Upgrading projects, page 47](#).
- To convert a project to different database format, select it and click **Convert**. See [Converting projects, page 47](#).
- To reorder the projects list, select a project and click **Top**, **Move Up**, **Move Down**, or **Bottom**. If you have a large number of projects, you may want to reorder them so the most frequently used are displayed at the top of projects list in Helix ALM login dialog boxes.

- To remove a project no longer in use, select it and click **Remove**. See [Removing projects, page 41](#). You may also be able to permanently delete removed projects. See [Deleting Helix ALM native projects, page 41](#) and [Deleting RDBMS projects, page 42](#).

**Note:** Back up projects frequently. Hard drive crashes or user error can result in the loss of important data. It is important to perform routine backups. See [Backing up Helix ALM databases, page 43](#).

## Adding existing Helix ALM native projects

If you removed a Helix ALM native project and did not delete any of the files, you can re-add it to the Helix ALM Server.

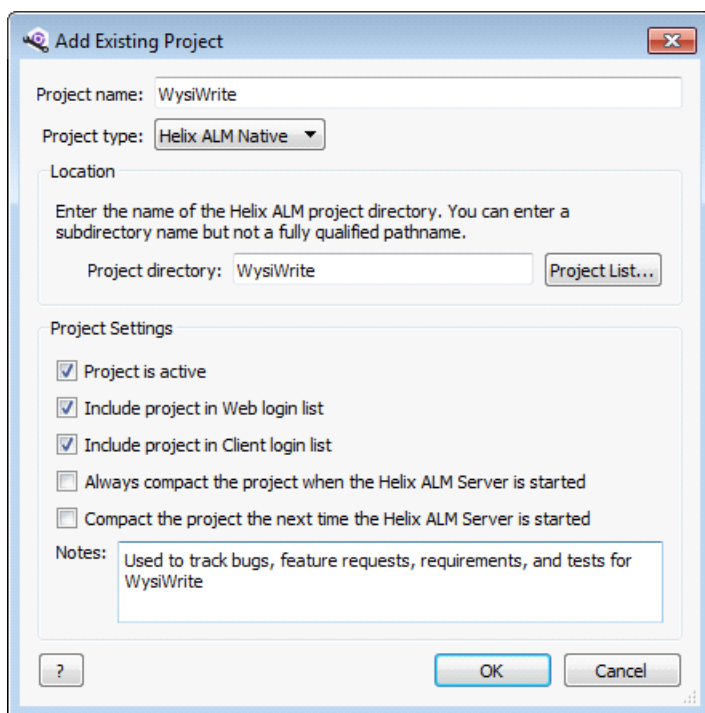
**Note:** If you use the 64-bit server, you must upgrade legacy TestTrack 2011.1 or earlier native projects before adding them. See [Upgrading projects, page 47](#).

1. Choose **View > Projects**.

The Projects dialog box opens.

2. Click **Add Existing**.

The Add Existing Project dialog box opens.



3. Select **Helix ALM Native** from the Project type list.
4. Enter the name of the **Project directory** to re-add or click **Project List** to select a removed project. The Project name and Project directory fields are automatically populated if you select a project.

Projects are stored in the TTServDb/TTDBs directory in the Helix ALM application directory by default. You may be able to enter a full directory path depending on the server settings.



**Note:** The path cannot exceed 247 characters, including the drive specifier (e.g., C:\) and names of subdirectories that Helix ALM creates in the specified directory.

5. Enter or change the **Project name**. The name is displayed when users log in to Helix ALM.
6. Select the **Project Settings**.
  - **Project is active** creates an active project. Users cannot access inactive projects.
  - **Include project in Web login list** includes the project in the list for Helix ALM Web users.
  - **Include project in Client login list** includes the project in the list for Helix ALM Client users.
  - **Always compact the project when the Helix ALM Server is started** compacts the project when the server starts. Compacting removes space and rebuilds the index files but may increase initialization time.
  - **Compact the project the next time the Helix ALM Server is started** compacts the project the next time the server starts.
7. Enter any project **Notes**. For example, you can explain what the project is used for or why it was added.
8. Click **OK**.

The project is re-added to the server and displayed in the projects list.

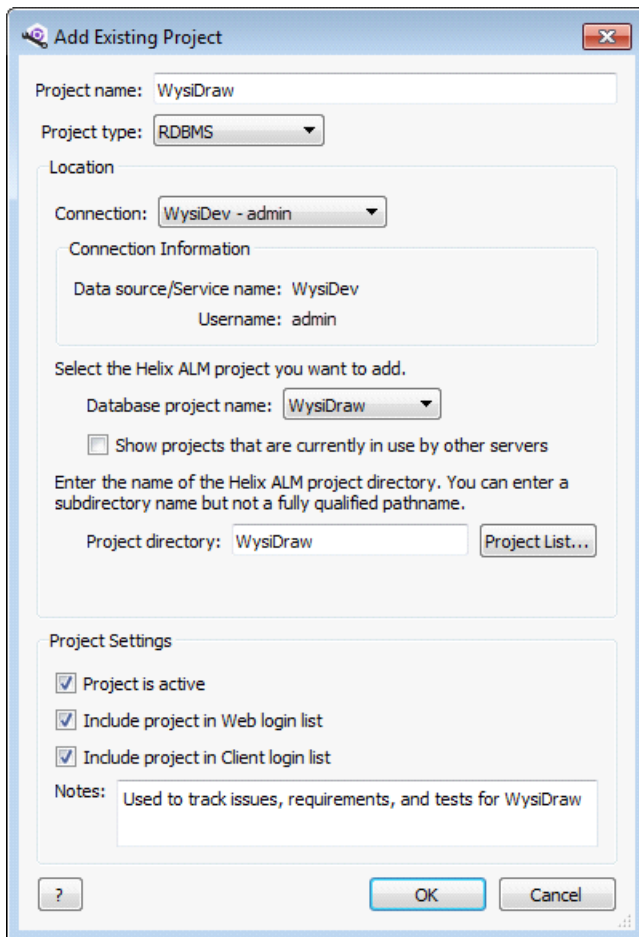
## Adding existing RDBMS projects

If you removed an RDBMS project but did not delete the records from the RDBMS database, you can re-add it to the Helix ALM Server.

When you add an existing project, you must specify a directory to store attachments, SoloBug files, and report stylesheets in. These files are stored on the server and not in the database.

**Note:** If the project directory has not been created, you must manually create it before adding the project.

1. Click **Projects**. You can also choose **View > Projects**.  
The Projects dialog box opens.
2. Click **Add Existing**.  
The Add Existing Project dialog box opens.



3. Select **RDBMS** from the Project type list.
4. Select the **Connection** for the RDBMS database to add the project to.

The list includes RDBMS connections configured for the Helix ALM Server. See [Adding RDBMS connections, page 22](#) if you need to add a connection.

5. Select the project to add from the **Database project name** list.

Optionally select **Show projects that are currently in use by other servers** to add a project from a server that is experiencing problems. You should only select a project that another server is using if the server computer is experiencing problems and you need to move the project to another server.

**Note:** The **Project name** field is automatically populated with the name stored in the database for the selected project. You can change the project name to display a different one when users log in to Helix ALM.

6. Enter the name of the **Project directory** to add the project files to or click **Project List** to use an existing project directory.

Project directories are stored in the TTServiceDb/TTDBs directory in the Helix ALM application directory by default. The project directory contains subdirectories for attachments, SoloBug files, and report stylesheets. You may be able to enter a full path depending on the server settings.

**Note:** The path cannot exceed 247 characters, including the drive specifier (e.g., C:\) and names of subdirectories that Helix ALM creates in the specified directory.

7. Select the **Project Settings**.
  - **Project is active** creates an active project. Users cannot access inactive projects.
  - **Include project in Web login list** includes the project in the list for Helix ALM Web users.
  - **Include project in Client login list** includes the project in the list for Helix ALM Client users.
8. Enter any project **Notes**. For example, you can explain what the project is used for or why it was added.
9. Click **OK**.

The project is re-added to the server and displayed in the projects list.

## Editing project settings

You can edit a project's description, directory location, settings, and notes. Keep the following in mind:

- To change the project directory location, you must inactivate the project first. See [Moving project directories, page 39](#) or [Moving RDBMS projects, page 40](#).
  - To change the project type, you must convert the project. See [Converting projects, page 47](#).
1. Click **Projects**. You can also choose **View > Projects**.

The Projects dialog box opens.

2. Select the project to edit and click **Edit**.

The Edit Project dialog box opens.

3. Make any changes and click **OK**.

**Note:** If you change the project directory location, you are prompted to copy the directory to the new location before saving the changes. Move the directory and then click **Save Changes**.

## Moving project directories

By default, project files are located in the TTServDb\TTDBs directory in the Helix ALM application directory. The project directory includes attachments, SoloBug files, and report stylesheets. For Helix ALM native projects, the directory also includes the project database file.

You can move project files to any directory on the server computer's local hard drive or a mapped network drive.

**Note:** The following steps explain how to move native projects and project data stored on the Helix ALM Server for both native and RDBMS projects. See [Moving RDBMS projects, page 40](#) for information about moving RDBMS projects to a different database or different server.

1. Inactivate the project to move. See [Inactivating and activating projects, page 41](#).
2. Make a backup copy of the project directory to move including all subdirectories.

By default, project directories are in the following locations:

- Windows—C:\Program Files\Perforce\Helix ALM\TTServDb\TTDBs
  - Linux—/var/lib/HelixALM/TTServDb/TTDBs
3. Copy the project directory and all subdirectories to the new location.
  4. Select the inactive project to move in the projects list and click **Edit**.  
The Edit Project dialog box opens.
  5. Enter the new **Project Directory** name or the full path to the project directory.  
The path cannot exceed 247 characters, including the drive specifier (e.g., C:\) and names of subdirectories that Helix ALM creates in the specified directory. The default directory path for projects and the ability to enter fully qualified pathnames is controlled using the Helix ALM Registry Utility. See the [Registry Utility help](#) for information.  
**Note:** If a 'Directory name cannot contain any of the following characters' error is returned when you save the project changes, you do not have permission to enter the full path.
  6. Select **Project is active** to reactivate the project.
  7. Make any other changes to the project information.
  8. Click **OK**.  
You are prompted to move the project directory to the new location. Copy the project directory to the new location if you have not already.
  9. Click **Save Changes**.  
The project is moved.  
**Note:** See [Moving Databases and Projects](#) for troubleshooting information.
  10. Optionally delete the project directory in the old location.

## Moving RDBMS projects

You can move RDBMS projects to different databases or Helix ALM Servers.

**Note:** See [Moving Databases and Projects](#) for troubleshooting information.

### Moving projects to a different database

Projects can be hosted in multiple RDBMS databases. This may help alleviate performance or disk space restriction issues. To move a project to a different database, you need to convert it. During the conversion, project data is copied to the destination RDBMS database and is not deleted from the original database.

1. Inactivate the project to move. See [Inactivating and activating projects, page 41](#).
2. Convert the project to copy it to the other database. See [Converting projects, page 47](#).
3. Activate the project. See [Inactivating and activating projects, page 41](#).
4. Optionally delete the project tables from the original RDBMS database. You must manually delete the project from the RDBMS unless you have permission to permanently delete RDBMS projects. Ask your DBA for help deleting tables.
5. Repeat steps 1 - 4 for each project to copy to the new database.

## Moving projects to a different Helix ALM Server

To host an RDBMS project on a different Helix ALM Server, you need to move the project files from the old server to the new server.

1. Inactivate the project to move. See [Inactivating and activating projects, page 41](#).
2. Remove the project from the current server. See [Removing projects, page 41](#).
3. Move the project files to the new server. See [Moving project directories, page 39](#).
4. Log in to the new server.
5. Add the project to the new server. See [Adding existing RDBMS projects, page 37](#).

## Inactivating and activating projects

Users can only access and work with active projects. You can inactivate projects that you do not want users to access but do not want to remove.

1. Click **Projects**. You can also choose **View > Projects**.  
The Projects dialog box opens.
2. To inactivate a project, select the project and click **Inactivate**. The project is inactivated and displayed in gray.  
To activate a project, select the inactive project and click **Activate**. The project is activated and can be accessed by Helix ALM users.

## Removing projects

Remove projects if they are not currently used but you want to save the project data. Removed projects are not displayed in the projects list and users cannot access them.

If you want to use a removed project later, re-add it in the server admin utility. See [Adding existing Helix ALM native projects, page 36](#) or [Adding existing RDBMS projects, page 37](#).

1. Click **Projects**. You can also choose **View > Projects**.  
The Projects dialog box opens.
2. Select the project and click **Remove**.  
You are prompted to confirm the removal.
3. Click **Yes**.  
The project is removed. A dialog box opens with information about the removed project.
4. Click **OK** to close the dialog box.

## Deleting Helix ALM native projects

To delete a Helix ALM native project, you must manually delete the project directory and files from the server computer. You cannot delete these projects using the server admin utility.

**Note:** You must remove the project in the server admin utility before it can be deleted. See [Removing projects, page 41](#).

1. On the computer that hosts the Helix ALM Server, delete the subdirectory that contains the project to delete.

By default, each project is stored in a subdirectory of the TTServDb/TTDBs directory in the Helix ALM application directory.

## Deleting RDBMS projects

Delete inactive projects if they are no longer used. If you want to save project data, you can remove projects instead of deleting them. See [Removing projects, page 41](#).

**Note:** You can only delete projects if the **Allow administrator to permanently destroy inactive projects** option is selected in the Helix ALM Registry Utility. See the [Registry Utility help](#) for information.

1. Click **Projects**. You can also choose **View > Projects**.  
The Projects dialog box opens.
2. Select the inactive RDBMS project and click **Delete**.  
You are prompted to confirm the deletion.
3. Click **Permanently Delete** to delete the project.  
The local directory and all files in it are deleted. Project table entries are also deleted from the database.

# Managing Databases

Each Helix ALM Server has a server database, which stores configuration information for the server. Every Helix ALM project is stored in its own database, which contains all project information, including issues, requirements, requirement documents, test cases, test runs, local customers and users, filters, test configurations, security groups, and reports.

Whether you store the server database and projects in a Helix ALM native database or RDBMS databases, it is important to regularly back up the server database and projects, and to use caution when modifying data directly in the database.

## Modifying Helix ALM databases

You may store Helix ALM data in an RDBMS database instead of the Helix ALM native database format. You can modify the internal database format and data from the RDBMS, but we do not recommend it. Your maintenance contract does not include support for recovering from these types of database changes.

### Configuration changes

For both native and RDBMS databases, you can configure field names, custom fields, workflows, notification rules, and more. We recommend making these changes using the Helix ALM Client rather than at the database level. Making changes directly in the database requires a full understanding of the database format and the rules enforced at the software level.

### Database table changes

Do not reconfigure the database format. When you rename a field in the client application, the database column names do not reflect this change. Do not change database tables/column names, modify column size/attributes, or make any other structural database changes because it will result in errors using Helix ALM.

### Live updates

Helix ALM caches data to improve the performance of complex reports and filters. Do not perform live updates of Helix ALM at the database level unless the Helix ALM Server has been shut down. Adding, editing, or deleting data while the server is running results in errors and potential data loss. Your changes may be overwritten next time the item is modified because database changes are not immediately read into the memory cache.

The native database format prevents users from opening the database in read/write mode while the Helix ALM Server is running. However, Helix ALM does not implement similar locks when running against an RDBMS database. To perform live data updates, use SOAP, bulk field changes, or other methods available in Helix ALM clients.

**Note:** You can read and view information from the database using database vendor-specific methods.

## Backing up Helix ALM databases

Back up the Helix ALM Server database and project databases regularly.

## Helix ALM native server database

1. Stop the Helix ALM Server.
2. Copy the contents of the TTServDb directory on the Helix ALM Server computer. Following are the default locations:
  - Windows—C:\Program Files\Perforce\Helix ALM\TTServDb
  - Linux—/var/lib/HelixALM/TTServDb

**Note:** Only copy the project subdirectories if you are using TestTrack 2011.2 and earlier and want to back up projects at the same time.

3. Restart the Helix ALM Server.

## Helix ALM native projects

### Helix ALM (or TestTrack 2012 - 2016.1)

Use the Native Database Backup Command Line Utility to safely back up project databases without stopping the Helix ALM Server. Download the utility from the [Add-ons page](#).

### TestTrack 2011.2 and earlier

Each project is stored in a subdirectory in the TTServDb directory. Projects may be stored in other locations depending on your configuration.

1. Stop the Helix ALM Server.
2. Copy the directories to back up.
  - To copy all projects, copy the TTDbs directory and all subdirectories. This also copies the server database.
  - To copy an individual project, copy the appropriate directory in the TTDbs directory and all subdirectories.
3. Restart the Helix ALM Server.

## Oracle, PostgreSQL, and SQL Server server and project databases

If the server database or projects are stored in a different RDBMS, ask your DBA for help with backups.

When you back up the server database and projects from the RDBMS, make sure to also back up the project directories on the Helix ALM Server that contain attachments, SoloBug files, and report stylesheets. Copy the project subdirectories to back them up.

## Linux examples

### Single native database backup

```
cp -R /var/lib/HelixALM/TTServDb/TTDbs/SampleDB/* /tape/bkup
```



## Full native databases backup

```
cp -R /var/lib/HelixALM/TTServDb/* /tape/bkup
```



# Upgrading and Converting Projects

## Upgrading projects

You need to upgrade projects to the current format as part of the Helix ALM upgrade process. See [Upgrading projects, page 47](#).

**Note:** Legacy projects from TestTrack 2011.1 and earlier must be upgraded to TestTrack 2015.1 before you can upgrade them to the current Helix ALM version. Contact [Perforce Support](#) for help.

## Converting projects

Project data must be stored in Helix ALM native or another RDBMS format, such as Oracle or Microsoft SQL Server. If existing projects are stored in a database that is no longer used or supported, you can convert them to a different format to move the data. See [Converting projects, page 47](#).

## Upgrading projects

You must upgrade existing projects to the current Helix ALM version before users can access them.

**Note:** Legacy projects from TestTrack 2011.1 and earlier must be upgraded to TestTrack 2015.1 before you can upgrade them to the current Helix ALM version. Contact [Perforce Support](#) for help.

1. Click **Projects**. You can also choose **View > Projects**.

The Projects dialog box opens.

**Tip:** To upgrade a project that is not in the projects list, you must add it first. See [Adding existing Helix ALM native projects, page 36](#) or [Adding existing RDBMS projects, page 37](#).

2. Select the project to upgrade.

You can select multiple projects. It may take several minutes to upgrade each project.

**Note:** If you upgrade an RDBMS project, all projects in the database are upgraded.

3. Click **Upgrade**.

The Confirm Project Upgrade dialog box opens.

4. Click **Yes** to start the upgrade.

You return to the Projects dialog box and the upgrade starts. The Status column displays upgrade progress information.

## Converting projects

You can convert projects from Helix ALM native to RDBMS and vice versa.

- Helix ALM native projects can only be converted to RDBMS. RDBMS projects can be converted to native format or to a different RDBMS connection.

- If a project needs to be upgraded, you must upgrade it before converting it. See [Upgrading projects, page 47](#).
- Projects must be inactivated before they can be converted. See [Inactivating and activating projects, page 41](#).
- Legacy TestTrack 2011.1 or earlier native projects must be upgraded or converted to RDBMS before upgrading to the 64-bit server. See [Upgrading projects, page 47](#).

1. Click **Projects**. You can also choose **View > Projects**.

The Projects dialog box opens.

**Note:** To convert a project that is not in the projects list, you must first add it. See [Adding existing Helix ALM native projects, page 36](#) or [Adding existing RDBMS projects, page 37](#).

2. Select the project to convert.

You can select multiple projects. It may take several minutes to convert each project.

3. Click **Convert**.

The Project Destination dialog box opens.

4. If you are converting the project to RDBMS format, select a **Connection** and enter a **Project Name** and **Project Directory**.

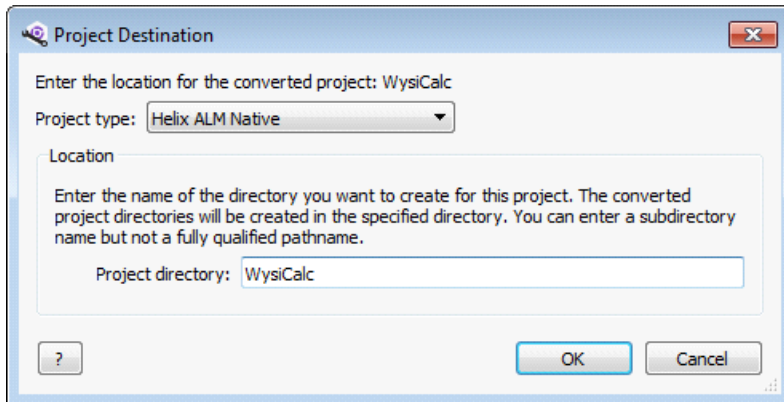
You can only select one RDBMS destination. If you convert multiple projects, they are all added to the selected RDBMS. Helix ALM also automatically generates project names based on current names. By default, projects are created in the TTServDb/TTDBs directory in the Helix ALM application directory. You may be able to enter a full path depending on the server settings.

**Note:** The path cannot exceed 247 characters, including the drive specifier (e.g., C:\) and names of subdirectories that Helix ALM creates in the specified directory.

The screenshot shows a 'Project Destination' dialog box. At the top, it says 'Enter the location for the converted project: WysiWrite'. Below that is a 'Project type' dropdown menu set to 'RDBMS'. Under the 'Location' section, there is a 'Connection' dropdown menu set to 'WysiDev - admin'. Below that is a 'Connection Information' box containing 'Data source/Service name: WysiDev' and 'Username: admin'. At the bottom, there are two text input fields: 'Database project name' with 'WysiWrite' and 'Project directory' with 'WysiWrite'. The dialog box has a question mark icon on the bottom left and 'OK' and 'Cancel' buttons on the bottom right.

5. If you are converting the project to native format, enter a **Project Directory** name.

By default, projects are created in the TTServDb/TTDBs directory in the Helix ALM application directory. You may be able to enter a full path depending on the server settings.



6. Click **OK**.

The Confirm Project Conversion dialog box opens. The available options depend on the project type.

7. Select **Store file attachments** and enter a file size if you are converting a native project to RDBMS format and want to store file attachments in the database.

The minimum value is 1 MB and the maximum value is 25 MB. Any attachment larger than the size you enter is stored as a file on the Helix ALM Server.

8. Click **OK** to start the conversion.

**Note:** After conversion is complete, make sure to activate the project so users can access it. See [Inactivating and activating projects, page 41](#).



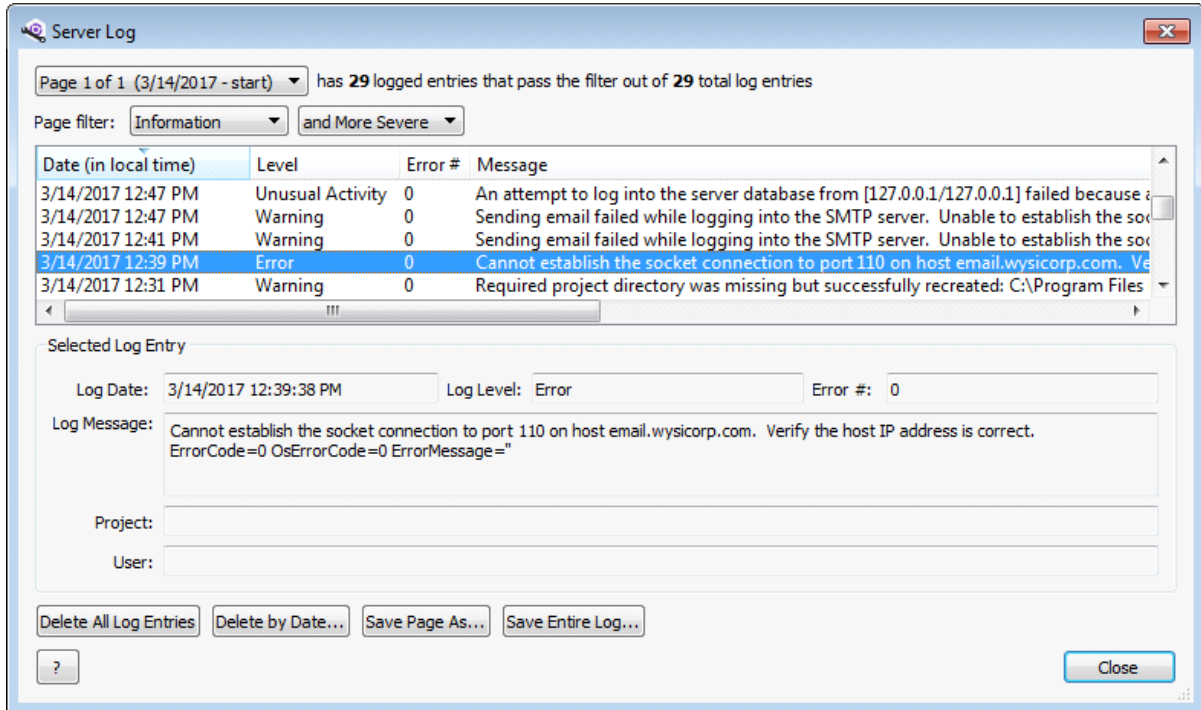
# Working with the Server Log

The server log records Helix ALM Server events, such as severe errors or unusual activity, and helps you monitor the server operation.

The amount of information in the log depends on the server options you set. The server can also send email notifications based on events. See [Setting log options, page 14](#).

1. Click **Server Log**. You can also choose **View > Server Log**.

The Server Log dialog box opens.



2. Select a **Page filter** to filter the entries by log level. See [Server log levels, page 52](#).

Select one of the following options to further narrow the entries displayed:

- **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 to the filtered log entries.

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

3. Select the entry to view.

The details are displayed in the Selected Log Entry area.

4. Click **Save Page As** to save the current page of log entries or click **Save Entire Log** to save all log entries. The log is saved as a text file that can be used for analysis or report generation with other tools.

The Export File dialog box opens. Select a Save in location, enter a File name, and click **Save**.

5. Click **Delete All Log Entries** to delete all the log entries or click **Delete by Date** to delete log entries created before the specified time and date.
6. Click **Close** when you finish.

## Server log levels

Server log levels indicate the severity of messages and errors returned by the Helix ALM Server. The logging level selected in the server options controls level of detail displayed in the log. A lower level, such as Unusual Activity, provides greater detail because more types of events are logged. See [Setting log options, page 14](#).

Level	An event is written to the log when:
Severe Error	A severe problem or critical condition occurs, such as a server failure.
Error	An error condition occurs, such as when a connection attempt to a client fails.
Warning	A warning condition occurs, such as RDBMS connection problems.
Unusual Activity	Unusual activity occurs, such as a user trying to log in with an incorrect username.
Information	Any significant action occurs, such as a Helix ALM Web user session timing out.

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



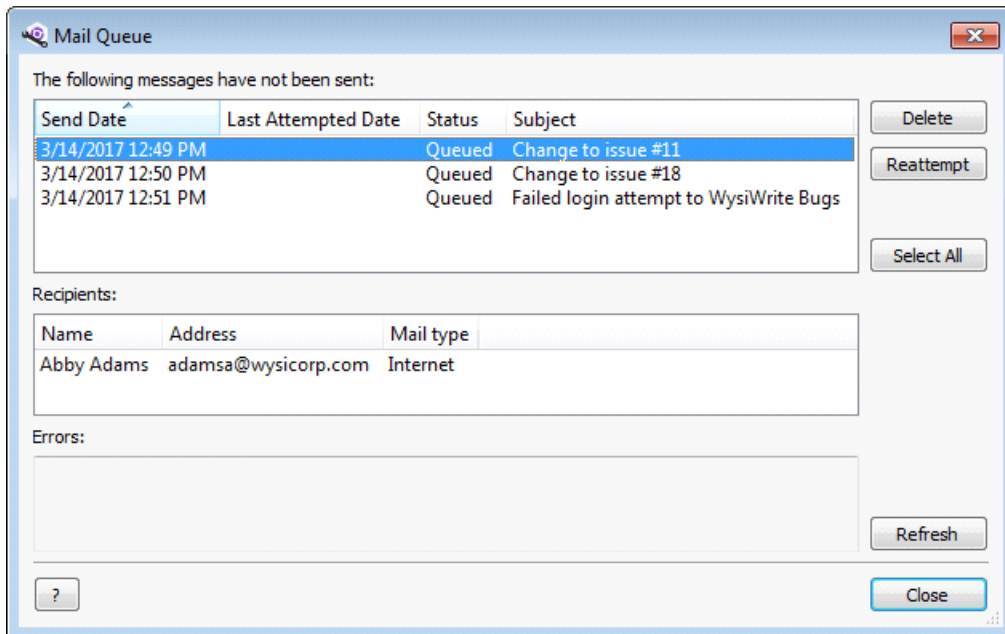
# Managing Email

Users can send email from Helix ALM and also generates automatic email notifications. When Helix ALM sends email, it is placed in the mail queue for processing by the server.

The mail queue only contains unsent email. Email is generally sent and removed from the mail queue in less than 60 seconds. An email can get stuck in the mail queue if sending is paused, the SMTP options are not properly configured, or the SMTP host is experiencing problems.

1. Click **Mail Queue**. You can also choose **View > Mail Queue**.

The Mail Queue dialog box opens. Unsent emails are displayed.



2. Select an email to view the details.

The name, email address, and mail type are displayed in the Recipients area. The send error is displayed in the Errors area.

3. Click **Reattempt** to resend the selected email. See [Resending email, page 53](#).
4. Click **Delete** to delete the selected email. See [Deleting email, page 54](#).
5. Click **Close** when you finish.

## Resending email

If email was not sent successfully on the first attempt, you can resend it from the mail queue after addressing any email configuration issues.

1. Click **Mail Queue**. You can also choose **View > Mail Queue**.

The Work with Mail Queue dialog box opens.

2. Select the email and click **Reattempt**.

You are prompted to confirm the resend.

3. Click **Yes**.

The email is resent.

**Note:** Check the server log for errors if the email is not sent. See [Working with the Server Log, page 51](#).

## Deleting email

You can delete email from the mail queue if you do not need to resend it.

1. Click **Mail Queue**. You can also choose **View > Mail Queue**.

The Mail Queue dialog box opens.

2. Select the email to delete. To delete all email in the queue, click **Select All**.

3. Click **Delete**.

You are prompted to confirm the deletion.

4. Click **Yes**.

The email is deleted.

# Setting Up RDBMS Databases

Helix ALM projects and the server database are stored in a Relational Database Management System (RDBMS). SQLite is default, native database format and does not require any setup or configuration before or after installation. See [About Helix ALM databases](#) for information about how Helix ALM data is stored.

Helix ALM data can also be stored in other RDBMS types, which allows you to leverage your existing database administration process. Microsoft SQL Server (ODBC), Oracle, and PostgreSQL are supported. See [Helix ALM RDBMS Support](#) for information about supported platforms and database versions.

Review the following information for help setting up databases for use with Helix ALM.

- [Oracle](#)
- [PostgreSQL](#)
- [SQL Server](#)

**Note:** Helix ALM License Server data is stored in a separate database. By default, the license server database is also stored in SQLite, but other RDBMS types are supported. See the [Helix ALM License Server help](#) for information about setting up license server databases.

## Setting up Oracle databases

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

Keep the following in mind:

- Do not add, delete, or modify any fields in the Helix ALM 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 Perforce.
- Create a process to back up database tables on a regular schedule.
- Running Oracle and the Helix ALM Server on the same computer can result in slow performance if not configured correctly. Make sure Oracle is configured correctly to avoid using all the system memory.

## Connecting to Oracle

The recommended method for using Oracle is via Oracle Call Interface (OCI). Download and install the required Oracle Instant Client libraries.

### Windows installers

- [32-bit](#)
- [64-bit](#)

## Linux installers

- 32-bit
- 64-bit

## Creating database tables

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

## Creating Oracle users

You must create an Oracle user for the Helix ALM 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 Helix ALM Server to determine the appropriate settings.

## Setting up PostgreSQL databases

Perforce 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 Helix ALM 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 Perforce.
- Create a process to back up database tables on a regular schedule.
- Running PostgreSQL and the Helix ALM Server on the same computer can result in slow performance if not configured correctly. Make sure PostgreSQL is configured correctly to avoid using all the system memory.

## Creating server database tables

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

## Setting up SQL Server databases

Perforce 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 Helix ALM 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 Perforce.
- Create a process to back up database tables on a regular schedule.
- Running SQL Server and the Helix ALM Server on the same computer can result in slow performance if not configured correctly. Make sure SQL Server is configured correctly 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 Helix ALM tables.

## Connecting to SQL Server

The only supported method for using SQL Server is via ODBC. After creating the database to use for the Helix ALM product, add a SQL Server data source name (DSN) on the Helix ALM computer. The server database and each database used to host Helix ALM projects must have a unique DSN. See [Creating DSNs for SQL Server Databases](#) for information.

## Creating server database tables

The Helix ALM Server automatically creates tables when you start the server or convert the server database. The TTServerDB.sql script file, which is located in the SQLServer directory in the Helix ALM 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 Helix ALM Server cannot connect to the server database, errors are added to the Startup.log file in the Helix ALM application directory.

## Server database cannot be shared

The Helix ALM Server, Helix ALM License Server, and Surround SCM Server and 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 Helix ALM 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 Helix ALM 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 Helix ALM 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 Helix ALM 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 Helix ALM 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 Helix ALM 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 'xxxx'. QODBC3: Unable to connect	The username or password entered in the RDBMS connection information is not valid.

## Oracle connection errors

Error	Cause
ORA-06401: NETCMN: invalid driver designator QOCI: Unable to logon	The Oracle Instant client drivers are not installed. See <a href="#">Setting up Oracle databases, page 55</a> 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"> <li>■ Windows—<code>NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252</code></li> <li>■ Linux—<code>NLS_LANG=American_America.UTF8</code></li> </ul> <p>You can also remove the following registry entry to help resolve the issue: <code>HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\NLS_LANG</code></p> <p><b>Note:</b> Refer to Oracle Metalink article 179133.1, “The Correct NLS_LANG in a Windows Environment,” for information about the correct setting, which varies based on the Windows version.</p>
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 Helix ALM Server could not connect to the server or translate the host name	<p>The Helix ALM Server cannot connect to the PostgreSQL service. Check the following and then restart the server:</p> <ul style="list-style-type: none"> <li>■ The PostgreSQL service is running.</li> <li>■ The host name and port number are correct.</li> <li>■ A firewall is not blocking the port.</li> <li>■ If connecting to a remote PostgreSQL server, the server is configured to accept remote connections.</li> </ul>



# Appendix A: Startup Log Codes

After the Helix ALM Server starts, a list of active projects and the number of items in each project are added to the startup log.

The following codes indicate item types in the log.

Code	Number of:
CUDDFDCT	Issue custom fields
CUDFRDMT	Requirement document custom fields
CUDFRQMT	Requirement custom fields
CUDFTSTC	Test case custom fields
CUDFTSTR	Test run custom fields
DFCT	Issues
DFLT	Filters
FLDR	Field relationships
FOLDPUB	Public folders
FOLDPVT	Private folders
FOLDTYPE	Folder types
LINK	Links between related items
MAIL	Tracked emails
RDMT	Requirement documents
RPRT	Reports
RQMT	Requirements
TASK	Tasks
TRGRESCL	Escalation rules
TRGRPOSTEXE	After save run executable triggers
TRGRPREEVT	Before save enter workflow event triggers
TRGRPREEXE	Before save run executable triggers
TRGRPREMOD	Before save modify item triggers

Code	Number of:
TRGRPNOTFY	Before save notification triggers
TRGRPREFRE	Before save prevent triggers
TSTC	Test cases
TSTR	Test runs
TYPE	Requirement types
UGRP	Security groups
USER	Users

# Index

## A

Activating projects 41

Adding

- existing Helix ALM native projects 36
- existing RDBMS projects 37
- Oracle database connections 23
- PostgreSQL database connections 23
- RDBMS connections 22
- server connections 4
- server users 5
- SQL Server database connections 23

Authentication methods 29

## B

Backing up databases 43

Browser path 6

## C

Changing the server database 19

Client settings 24

Connecting to different server 5

Converting

- 6.0 and later projects 47
- projects 47
- server database type 20

Creating

- Helix ALM native projects 7
- projects from template 10
- RDBMS projects 9

## D

Databases

- backing up 43
- modifying 43
- Oracle 55

PostgreSQL 56

SQL Server 57

Default native server database directories 19

Deleting

- email 54
- Helix ALM native projects 41
- RDBMS connections 24
- RDBMS projects 42
- server connections 4

Downloading RSA keys 31

## E

Editing

- project settings 39
- RDBMS connections 24
- server connections 4

Email

- deleting 54
- resending 53
- sending options 15
- SMTP settings 15
- tracking options 16
- viewing queue 53

Encryption 28

- setting options 26

## F

Finding license servers 32

## H

Helix ALM License Server

- finding on network 32
- starting 1

Helix ALM Server

- connecting to different 5
- starting 1

Helix ALM Server Admin Utility

- starting 2

HTTPS 28

## I

Inactivating projects 41

## J

JIRA integration settings 26

## K

Key exchange 29

- changing 28

- enabling and disabling 26

- RSA 30

## L

license server options 31

Linux

- setting the browser path 6

Local Helix ALM admin password 18

Log levels 52

Logging options 14

## M

Moving projects 39

- RDBMS 40

## N

Native projects

- adding existing 36

- creating 7

- deleting 41

## O

ODBC

- connection errors 58

- connection issues 58

Options

- client settings 24

- email sending 15

- email tracking 16

JIRA integration 26

license server 31

log 14

RDBMS connections 22

security 26

server 18

server database 19

software update check 32

Oracle

- adding database connections 23

- connecting to 55

- connection errors 59

- creating server database tables 56

- creating users 56

- database character set 56

- instant client libraries (OCI) 55

- setting up 55

- sizing, memory, and tuning 56

## P

PostgreSQL

- adding database connections 23

- connection errors 60

- creating server database tables 57

- setting up 56

Projects

- activating 41

- adding existing Helix ALM native 36

- adding existing RDBMS 37

- backing up 44

- converting 47

- converting 6.0 and later 47

- creating from template 10

- creating Helix ALM native 7

- creating RDBMS 9

- deleting Helix ALM native 41

- deleting RDBMS 42
  - editing settings 39
  - inactivating 41
  - moving 39
  - moving RDBMS 40
  - removing 41
  - upgrading 47
  - upgrading 6.0 and later 47
- R**
- RDBMS connections 22
    - adding Oracle 23
    - adding PostgreSQL 23
    - adding SQL Server 23
    - changed database configuration 58
    - deleting 24
    - dropped tables 58
    - editing 24
    - exclusive lock 58
    - mismatched UUID 58
    - server database cannot be shared 58
    - troubleshooting 57
  - RDBMS databases 55
  - RDBMS projects
    - adding existing 37
    - creating 9
    - moving 40
  - Regenerating RSA key pairs 31
  - Removing
    - projects 41
    - server users 5
  - Reports
    - support diagnostics 6
  - Resending email 53
  - RSA key exchange 30
    - downloading key pair 31
    - regenerating keys 31
- S**
- Security
    - client/server communication 28
  - Security options 26
    - RSA key exchange 30
  - Server connections
    - adding 4
    - deleting 4
    - editing 4
    - managing 3
  - Server database
    - backing up 44
    - changing 19
    - converting type 20
    - default directories 19
    - setting options 19
  - Server database tables
    - Oracle 56
    - PostgreSQL 57
    - SQL Server 57
  - Server log
    - levels 52
    - setting options 14
    - viewing 51
  - Server options 18
  - Server users
    - adding 5
    - removing 5
  - Software updates
    - setting options 32
    - viewing information 34
  - SQL Server
    - adding database connections 23
    - connecting to 57

- connection errors 59
- creating server database tables 57
- setting up 57

#### Starting

- Helix ALM License Server 1
- Helix ALM Server 1
- Helix ALM Server Admin Utility 2

Support diagnostics report 6

#### T

#### Troubleshooting

- RDBMS connections 57

#### U

#### Upgrading

- 6.0 and later projects 47
- projects 47

#### V

#### Viewing

- mail queue 53
- server log 51
- software update information 34