Helix ALM License Server

Admin Guide

Version 2017.2

PERFORCE

www.perforce.com

Copyrights

Perforce Software, Inc. and its subsidiaries
400 N 1st Avenue
Suite 200
Minneapolis, Minnesota 55401
USA
+1 510.864.7400

documentation@seapine.com

Contents

About the Helix ALM License Server

The Helix ALM License Server stores license, user, and customer information on one networked computer. You must have a license server running on your network that other Helix ALM products, including Surround SCM, can access. See Starting the Helix ALM License Server, page 7.

Use the Helix ALM License Server Admin Utility to perform the following tasks:

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

Installing the License Server and Admin Utility

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

> **Note:** A web-based license server admin utility is also available. After installing the web admin utility, you must perform additional configuration on the web server that hosts the admin utility. See the Helix ALMor Surround SCM installation help for information.

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

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

About the license server database

Helix ALM License Server data, including user information and product licenses, is stored in a Relational Database Management System (RDBMS). By default, the license server uses SQLite as the native backend database, which does not require any additional configuration before or after installation. Oracle, PostgreSQL, and SQL Server are also supported, but a qualified database administrator (DBA) must manually install and configure these databases to use with the license server.

When installing the license server, a SQLite server database file (LSServer.db) is created in the LicenseServerDb directory in the Helix ALM License Server application directory. After installation, you can use this server database as is or convert it to a different RDBMS type, such as SQL Server. You must create an empty database before storing license server data in it. See Setting Up RDBMS Databases, page 71.

About the 64-bit license server

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

- 32-bit Helix ALM and Surround SCM clients and the 32-bit Helix ALM License Server Admin Utility can communicate with the 64-bit license server and vice versa.
- The 64-bit license server has different system requirements than the 32-bit server. Make sure the server computer meets the recommended system requirements.

New installations

If you are performing a new 64-bit license server installation, a SQLite server database is created automatically the first time you start the license server. You can configure the server database to use a different RDBMS. See Setting Up RDBMS Databases, page 71 and Configuring the server database, page 47.

Upgrade installations

If you are upgrading from the 32-bit license server, you must perform the steps in Migrating from the 32-bit License Server to the 64-bit License Server on the Same Computer.

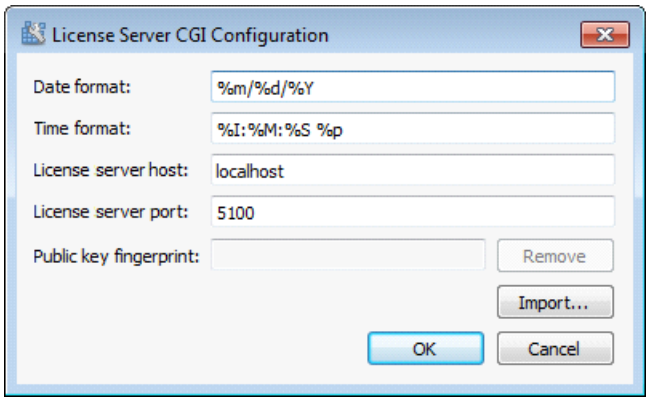
Changing web server admin utility CGI settings

If you use the Helix ALM License Server Web Admin Utility, you can change the CGI settings using the License Server CGI Configuration utility. You can change the format of date and time values displayed in the admin utility, license server address and port if it is running on a different computer than the CGI, and manage public keys used if RSA key exchange is enabled for the license server.

> **Note:** You must run the configuration utility as an administrator user on the computer that hosts the admin utility CGI.

1. Start the CGI configuration utility.
   - **Windows**—Choose **All Programs > Perforce > Helix ALM License Server > Helix ALM License Server CGI Configuration** on the Start menu.
   - **Linux**—Enter `/usr/bin/lscgiconfig`.

   The License Server CGI Configuration dialog box opens.



2. Make any changes.

Field	Description
Date format	Format for date values in the web server admin utility. The default is the operating system format on the computer the license server is installed on. You may want to change the format if the CGI is hosted in a different region than the license server and a different format is preferred. Use specifiers based your operating system.

Field	Description
Time format	Format for time values in the web server admin utility. The default is the operating system format on the computer the license server is installed on. You may want to change the format if the CGI is hosted in a different region than the license server and a different format is preferred. Use specifiers based your operating system.
License server host	IP address or domain name of the computer the license server is running on. You must change this value if the license server and CGI are hosted on different computers.
License server port	Port number the license server listens on. You must change this value if the license server and CGI are hosted on different computers. The default port is 5100.
Public key fingerprint	Key used when connecting to the license server from the web server admin utility. Required if RSA key exchange is enabled for the license server. See Configuring RSA key exchange, page 46. Click **Import** to import the key from the file exported from the admin utility. Select the file and click **Open** to add the key. To remove the key, click **Remove**.

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

Getting Started

The Helix ALM License Server and Helix ALM License Server Admin Utility are installed when you install Helix ALM products.

After it is installed:

1. Start the license server.
2. Start the admin utility and add a server connection.
3. Log in to start adding licenses and users.

Starting the Helix ALM License Server

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

> **Tip:** If Helix ALM applications cannot connect to the license server, an administrative user needs to troubleshoot. See Surround SCM Cannot Connect to the License Server and 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 License Server Admin Utility

You need to add licenses and users the first time you start the license server and admin utility. See Adding licenses, page 12 and Adding users, page 22.

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

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

   Linux—Enter `/usr/bin/lsadmin`.

   The Helix ALM License Server Login dialog box opens.

2. Select the **Server** you want to connect to. See Adding server connections, page 8 if you need to add a server.
3. Enter a **Username** and **Password** or select **Use single sign-on** to log in using the workstation credentials.

   Note: Single sign-on must be enabled and is only available for Windows.
4. Select **Always log in with this username and password** to automatically log in with the credentials you entered when the admin utility starts.
5. Click **Connect**.

   The admin utility starts.

   Note: 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 computer that hosts the license server and verify that the key displayed in the server options matches the key displayed when you logged in from the other computer. See Configuring RSA key exchange, page 46. If the fingerprint is correct, click **Yes**. If a different fingerprint is displayed in the server options, a hack may be in progress.

Adding server connections

Before you can access a license server from the admin utility, you need to add a server connection.

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

   The login dialog box opens.
2. Click **Setup**.

   The Setup Server Connections dialog box opens.
3. Click **Add**.

   The Add License Server dialog box opens.
4. Enter a **Server Name**.

   Use a name that uniquely identifies the server. For example, Satellite Office.
5. Enter the **Server Address** of the computer the license server is installed on and the **Port** number.

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

   Note: If RSA key exchange is enabled for the license 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 license server. See Configuring RSA key exchange, page 46.
6. Click **OK**.

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

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

7. Click **Close** when you finish.

Editing and deleting server connections

You can edit server connections to update the name, host address, or port number. You can also delete connections if they are no longer needed.

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

   The login dialog box opens.

2. Click **Setup**.

   The Setup Server Connections dialog box opens.

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

4. Click **Close** when you finish.

Finding license servers

You can quickly find all license servers on the network.

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

   The login dialog box opens.

2. Click **Setup**.

   The Setup Server Connections dialog box opens.

3. Click **Find**.

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

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

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

   The Add License Server dialog box opens.

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

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

6. Click **OK**.

   The server is added.

Connecting to a different server

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

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

   The login dialog box opens.
2. Select the server you want to connect to and click **Connect**.

Managing Licenses

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

Floating vs. named licenses

Helix ALM products include floating and named licenses. Named licenses are best for users who log in frequently while floating licenses are best for users who log in occasionally.

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

> **Note:** Users with floating licenses use multiple licenses when logged in to a Helix ALM client application and a third-party application integrated with a Helix ALM product at the same time. Make sure users know to log out of clients and disconnect third-party applications from Helix ALM products when they finish working to make licenses available to other users.

Helix ALM licenses

Helix ALM licensing includes separate licenses for issue management, requirements management, and test case management to provide users access to the features they need to work with. You can use a combination of area-specific licenses or a Helix ALM suite license to access all areas. Keep the following in mind:

- Helix ALM suite licenses provide access to issue management, requirements management (full license), and test case management. If a user is assigned a Helix ALM suite license and a license for a specific Helix ALM area, such as requirements management, is already assigned, the suite license is assigned instead of the other license. If the user is already assigned a Helix ALM suite license and an area-specific license is assigned, the suite license is unassigned and the user will not have access to any other areas except the specific one assigned, unless other licenses are also assigned. When a user with a floating Helix ALM suite license logs in, licenses for all Helix ALM areas are in use.
- Requirements Management full licenses provide access to all requirements management functionality. Reviewer licenses only provide read-only access to requirements and requirement documents in Helix ALM Web. Only one requirements management license type can be assigned to each user.
- Each Helix ALM license includes a license for the SOAP-based SDK, except for requirements reviewer licenses.

License duration

Evaluation, perpetual, or subscription licenses are available depending on the duration needed.

License type	Use to:	Provides access to:	When they expire
Evaluation	Try products for a trial period	A specific product version and technical support during evaluation period.	Licenses stop working and users can no longer use them to access products.
Perpetual	Make a one-time purchase with annual maintenance renewal for upgrades and technical support	A specific product version. Technical support and product upgrades are also available as long as maintenance is current.	Users can continue using the product version that licenses are associated with, but access to upgrades and technical support is no longer provided.
Subscription	Subscribe to products for a specific period of time determined at the time of purchase	A specific product version, technical support, and product upgrades as long as subscription term is current.	Licenses stop working and users can no longer use them to access products.

Use the license server admin utility to track when maintenance, evaluation periods, or subscription terms expire. See Viewing license details, page 19. To continue using products after evaluation periods or subscription terms expire, or to upgrade products after maintenance for perpetual licenses expires, contact Perforce Sales to purchase new licenses or renewal extensions.

Adding licenses

When you purchase a new product license or receive a maintenance extender key, you need to add the key to the license server before the product can be used. See Managing Licenses, page 11 for information about license types and expiration.

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

1. Click **Licenses**.

   The Licenses dialog box opens.
2. Click **Add**.

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

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

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

Configuring license pools

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

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

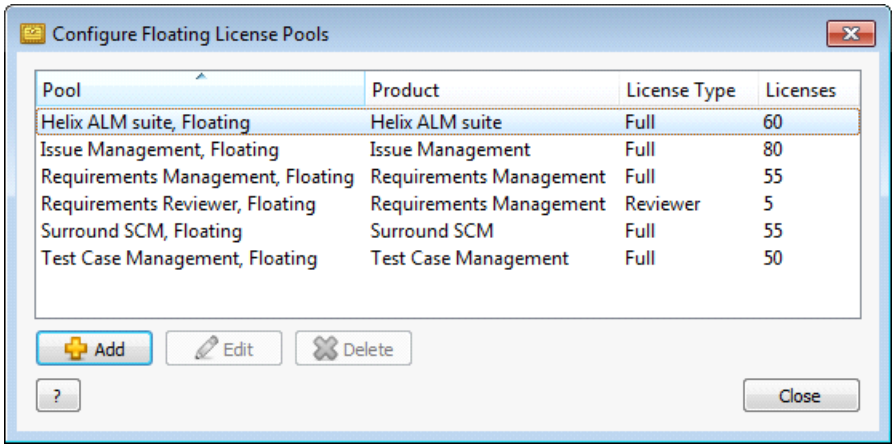
Note: Requirements Management full and reviewer licenses cannot be added to the same pool.

1. Click **Licenses**.

   The Helix ALM Licenses dialog box opens.

2. Click **Configure Floating Pools**.

   The Configure Floating License Pools dialog box opens.



3. Click **Add** to create a new license pool. See Adding license pools, page 13.
4. Select a pool and click **Edit** to modify it. See Editing and deleting license pools, page 14.
5. Select a pool and click **Delete** to delete it. See Editing and deleting license pools, page 14.
6. Click **Close** when you finish.

Adding license pools

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

1. Click **Licenses**.

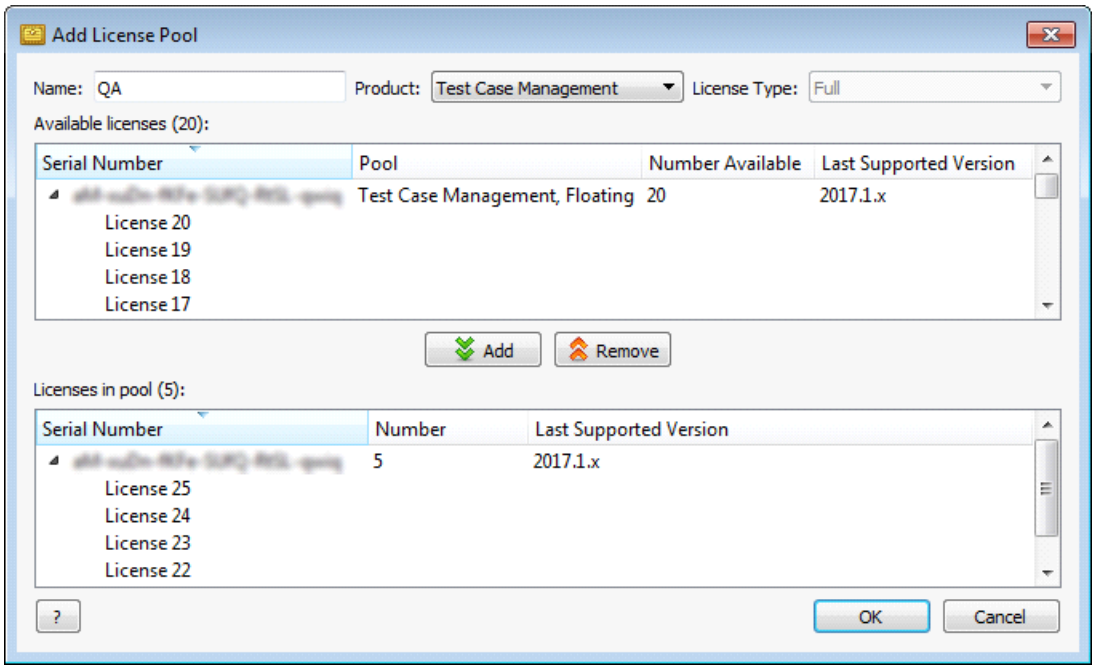
   The Helix ALM Licenses dialog box opens.

2. Click **Configure Floating Pools**.

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

3. Click **Add**.

   The Add License Pool dialog box opens.



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

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

5. Select a **Product**.

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

6. If you are pooling Requirements Management licenses, select a **License Type**.

   Requirements Management full and reviewer licenses cannot be added to the same pool.

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

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

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

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

9. Click **OK**.

   The license pool is added. The licenses in the pool can only be used by the users assigned to the pool. See Assigning users to license pools, page 15.

Editing and deleting license pools

You can edit a license pool to add or remove licenses included in it. You can also delete pools if they are no longer needed.

Note: You cannot edit or delete the default license pools for each license type.

1. Click **Licenses**.

   The Helix ALM Licenses dialog box opens.

2. Click **Configure Floating Pools**.

   The Configure Floating License Pools dialog box opens.

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

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

Assigning users to license pools

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

Tip: To assign multiple users to a license pool, select the users in the Global Users list and replace the license field values for the users. See Replacing license field values, page 31.

1. Click **Global Users**.

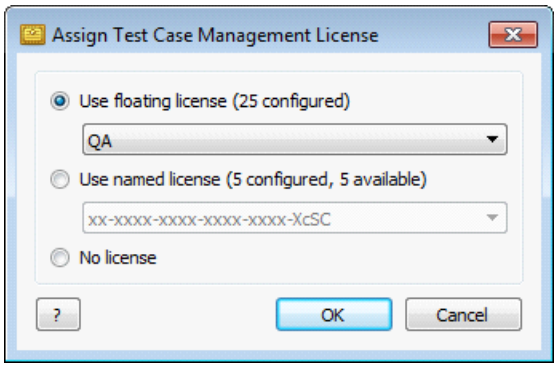
   The Global Users dialog box opens.

2. Click **Add** to assign a new user to a license pool or select an existing user from the Global Users list and click **Edit**.

   The Add User or Edit User dialog box opens.

3. Click the **Licenses** tab.
4. Click the corresponding product license button.

   The Assign License dialog box opens.



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

   The user is assigned to the license pool.

Assigning licenses

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

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

1. Click **Global Users**.

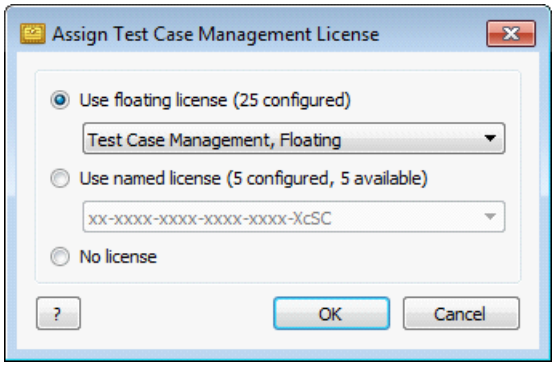
   The Global Users dialog box opens.

2. Select the users to assign licenses to.

   To select multiple users, **Ctrl+click** each user.

3. Click the corresponding product button. Buttons are only available for products with licenses entered in the admin utility.

   The Assign License dialog box opens.



4. Select a license type.

   You cannot assign named licenses to inactive users.

   > **Note:** If a user is already assigned a license for a specific Helix ALM area, such as requirements management, and a Helix ALM suite license is assigned, the suite license is used instead of the other license. If the user is already assigned a suite license and an area-specific license is assigned, the suite license is unassigned and the user will not have access to any other areas except the specific one assigned, unless other licenses are also assigned.

5. Click **OK**.

   The licenses are assigned to the users.

Associating users with named licenses

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

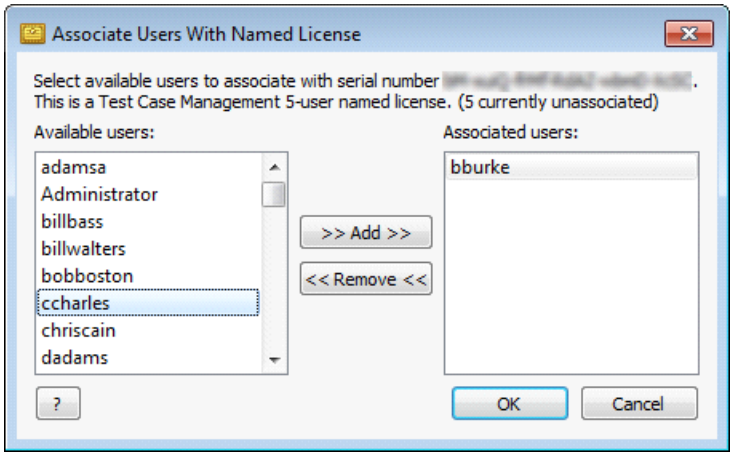
Note: You can also assign or change user licenses from the Global Users dialog box. See Assigning licenses, page 16.

1. Click **Licenses**.

   The Licenses dialog box opens.

2. Select a named license and click **Associate Users**.

   The Associate Users with Named License dialog box opens.



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

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

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

Viewing licenses in use

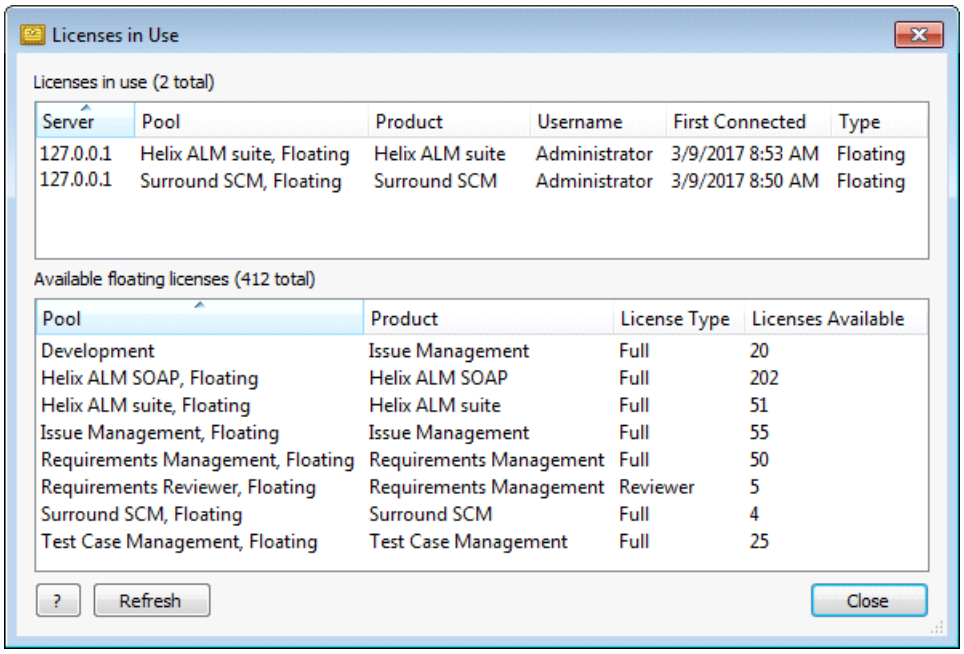
You can view the number of licenses currently in use, which users are using a floating license, and when users logged in. Use this information to determine if you need to add additional licenses or make changes to license pools. See Configuring license pools, page 13.

1. Click **Licenses**.

   The Helix ALM Licenses dialog box opens.

2. Click **Licenses in Use**.

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



> **Note:** The server where licenses are in use is also displayed. Server names that include ::1 or 127 indicate the Helix ALM product server is running on the same computer as the license server.

3. Click **Refresh** to update the list.
4. Click **Close** when you finish.

Viewing license counts

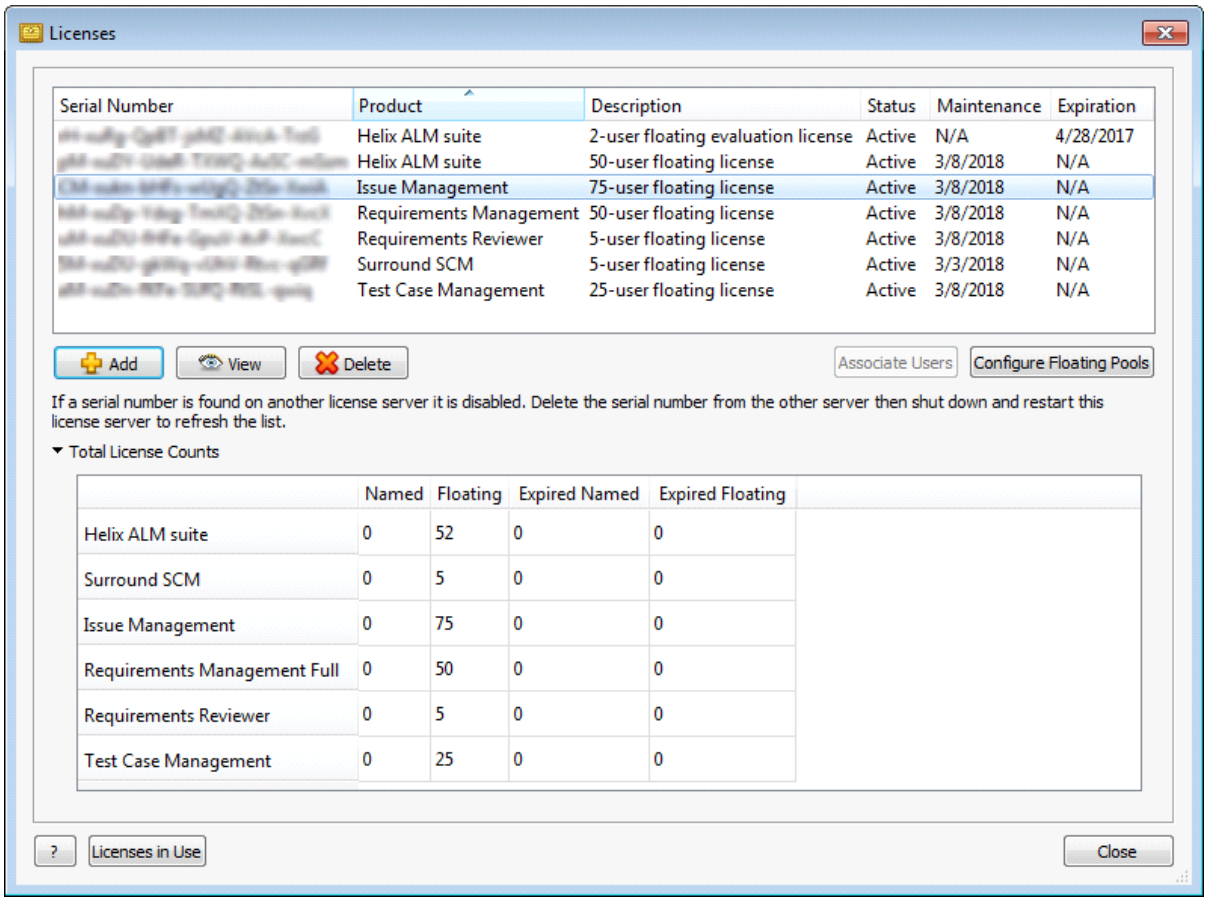
You can view the number of current and expired licenses stored on the license server by type and product.

1. Click **Licenses**.

   The Licenses dialog box opens.

2. Expand the **Total License Counts** area.

   The license counts are displayed.



Viewing license details

You can view details about licenses and information about maintenance or term extensions.

1. Click **Licenses**.

   The Licenses dialog box opens.

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

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

Deleting licenses

You can delete licenses that are no longer needed.

1. Click **Licenses**.

   The Licenses dialog box opens.

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

   You are prompted to confirm the deletion.

3. Click **Yes**.

   The license is deleted.

Managing Global Users

Create global users on the license server to give users and customers access to Helix ALM products. User records include usernames, passwords, and license assignments.

Global users can be shared among Helix ALM products. When you set up Helix ALM and Surround SCM, you can retrieve global users from the license server and then add them to security groups to control actions they can perform and information they can view. See the Helix ALM or Surround SCM help for information.

> **Tip:** You can also create global users directly in Helix ALM products. See the Helix ALM or Surround SCM help for information.

Use the Helix ALM License Server Admin Utility to:

- Add users. If the license server is configured to connect to an LDAP or Active Directory server, you can retrieve users from the database.
- View users. You can customize the Global Users list and set up the columns to display information you need.
- Edit user information and change usernames. You can also resync and edit LDAP/Active Directory users.
- Activate or inactivate users
- Unlock users after logins fail
- Delete or undelete users
- Bulk change user fields to update information for multiple users at the same time
- Control admin utility access

Customizing the Global Users list

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

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

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

Changing column contents

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

1. Right-click a column heading.

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

2. Select a column.

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

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

Sorting columns

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

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

Filtering columns

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

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

Adding users

Add users to the license server to provide access to Helix ALM products. Users you add to the license server are identified as global users in other products.

See Adding LDAP users, page 24 for information about adding users from LDAP and Active Directory.

> **Note:** Users with usernames and passwords longer than 32 characters cannot use Surround SCM or TestTrack 2016.0 and earlier.

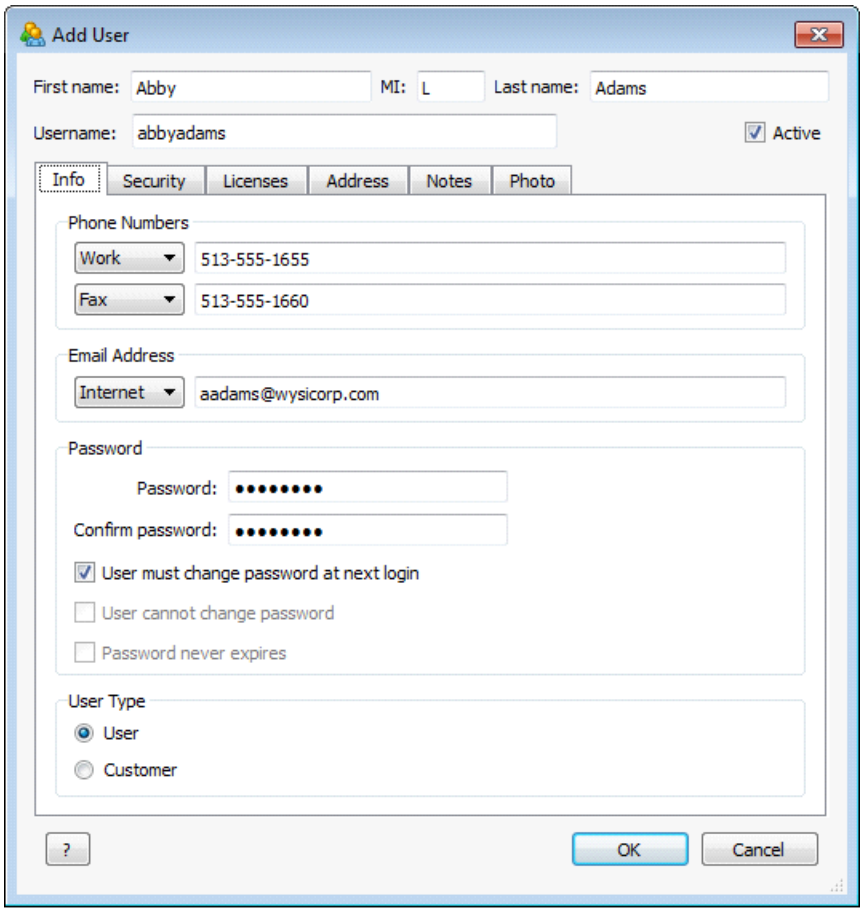
1. Click **Global Users**.

   The Global Users dialog box opens.

   > **Tip:** You can customize the information displayed in the Global Users list. See Customizing the Global Users list, page 21.

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

   The Add User dialog box opens.



3. Enter the **First name, MI** (middle initial), **Last name**. You can enter up to 32 characters for the first and last names and up to 8 characters for the middle initial.

   > **Note:** Multiple users can have the same first and last names. Make sure to enter additional contact information to distinguish between these users in Helix ALM applications.

4. Enter a unique **Username**. You can enter up to 128 characters.
5. Clear **Active** to create an inactive user. You may want to create an inactive user to temporarily restrict access to Helix ALM products until the user needs it.
6. On the **Info** tab, enter phone numbers and an email address, create a password, and select a user type.

Password options

You can enter up to 128 characters for the password. You can also set the following password options for users.

- **User must change password at next login** prompts users to change the password the next time they log in to a Helix ALM product.
- **User cannot change password** restricts users from changing the password.
- **Password never expires** prevents the password from expiring so users do not need to change the password on a regular basis.

User type

Global users are typical users who need access to Helix ALM products. You may want to create a global customer if you want to provide customers limited access to the products.

7. Enter or select additional information.

Tab	Use to:
Security	Select license server security permissions for the user. See Controlling Helix ALM License Server Admin Utility access, page 34.
Licenses	Assign licenses for the user. See Managing Licenses, page 11 and Assigning licenses, page 16.
Address	Enter the address and enter or select the company, division, and department. If you enter a company, division, or department value, it is saved and can be selected for other users and customers in the project, which can help you group related users. You can enter up to 64 characters. The Division values are based on the selected Company value, and the Department values are based on the selected Division value.
Notes	Enter any notes about the user.
Photo	Add a photo of the user. Photos are only displayed in Helix ALM products that support them. The following image file formats are supported: BMP, GIF, JPEG, JPG, PBM, PGM, PNG, PPM, SVG, and XPM.

8. Click **OK** to add the user.

Adding LDAP users

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

> **Note:** The license server does not support LDAP users with empty Name or Username fields or usernames longer than 128 characters. If you create an LDAP schema, make sure you enter the custom attributes when you add the LDAP server. See Setting LDAP options, page 52.

1. Click **Global Users**.

   The Global Users dialog box opens.

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

   The Add LDAP Users dialog box opens.

3. Select any **Filter** criteria to narrow the search results.

   Do not select any search criteria if you want to return a list of all LDAP users.

   - **Name** searches for LDAP users by name. This field supports wildcards.
   - **Username** searches for LDAP users by username. This field supports wildcards.
   - **Exclude existing license server users** excludes existing users on the license server based on the specified username.

- **Limit results to** limits the number of returned records to the specified amount. The default value is 200.

4. Click **Query LDAP Servers**.

   A list of matching users is displayed in the Search Results area.

5. Select the users to add to the license server.
   - To add multiple users and assign licenses later, click **Add**. After the users are added, make sure you assign license types and set security permissions for each user. See Assigning licenses, page 16 and Editing users, page 25. You can also select multiple users and perform bulk changes to assign the same license type and security permissions to the selected users. See Changing fields for multiple users, page 30.
   - To add one user and assign a license and set security permissions now, click **Advanced Add**. The Add User dialog box opens. Most of the user information is populated from the LDAP record and cannot be edited. Assign a license to the user and set server security permissions. You can also enable single sign-on if it is enabled for the LDAP server. See Editing users, page 25.

   > **Note:** Users with usernames and passwords longer than 32 characters cannot use Surround SCM or TestTrack 2016.0 and earlier.

6. Click **Close** when you finish.

   LDAP users can access Helix ALM products after they are added to the license server and assigned a license. It may take a few minutes for the changes to take effect.

Viewing users

You can view read-only user information.

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Select a user and click **View**.

   The View User dialog box opens.

3. Click **Close** when you finish.

Editing users

You can edit users to update contact information, change security settings, and assign licenses.

See Editing LDAP users, page 27 for information about editing LDAP and Active Directory users.

> **Tip:** You can also use the Quick Edit menu to change users to customers or vice versa, enable or disable single sign-on, inactivate or activate users, unlock users, and update fields for multiple users at the same time.

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Select a user and click **Edit**.

   The Edit User dialog box opens.

3. Make any changes to the information.

   Multiple users can have the same first and last names. Make sure to enter additional contact information to distinguish between these users in Helix ALM applications. You may also be able to change usernames. See Changing usernames, page 26.

Tab	Use to:
Info	Enter phone numbers and an email address, create a password, and select a user type.
Security	Select license server security permissions for the user. See Controlling Helix ALM License Server Admin Utility access, page 34.
Licenses	Assign licenses to the user. See Managing Licenses, page 11 and Assigning licenses, page 16.
Address	Enter the address and enter or select the company, division, and department. The Division values are based on the selected Company value, and the Department values are based on the selected Division value. You cannot change this information for LDAP users.
Notes	Enter any notes about the user.
Photo	Add, update, or remove a user photo. Photos are only displayed in products that support them. The following image file formats are supported: BMP, GIF, JPEG, JPG, PBM, PGM, PNG, PPM, SVG, and XPM.

   Note: Users with usernames and passwords longer than 32 characters cannot use Surround SCM or TestTrack 2016.0 and earlier.

4. Click **Set LDAP Association** to associate the user with an LDAP record. See Associating users with an LDAP server, page 28.
5. Click **OK** to save the changes.

Changing usernames

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

You can only edit usernames if **Enable renaming of usernames** is selected in the server options. See Setting server options, page 41.

Note: Users with usernames and passwords longer than 32 characters cannot use Surround SCM or TestTrack 2016.0 and earlier.

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Select a user and click **Edit**.

   The Edit User dialog box opens.

3. Enter a new username and click **OK**.

   You are prompted to confirm the username change.

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

   The username is changed. The old username is added to the Notes tab.

Editing LDAP users

You can edit LDAP user type, security, and license information. You can also remove the user association with the LDAP or Active Directory server.

> **Tip:** You can also use the Quick Edit menu to change users to customers or vice versa, enable or disable single sign-on, inactivate or activate users, unlock users, change the LDAP server association, and update fields for multiple users at the same time.

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Select a user and click **Edit**.

   The Edit User dialog box opens.

3. Make any changes to the information.

   You cannot edit most information on the Info category and any information in the Address or Photo categories for LDAP users.

Tab	Use to:
Info	Change the user type. You cannot edit phone numbers, email addresses, or passwords for LDAP users.
Security	Select license server security permissions for the user. See Controlling Helix ALM License Server Admin Utility access, page 34.
Licenses	Assign licenses to the user. See Managing Licenses, page 11 and Assigning licenses, page 16.
Address	View the user's company, division, department, and address information imported from LDAP or Active Directory.
Notes	Enter any notes about the user.
Photo	View the user's photo imported from LDAP or Active Directory. Photos are only displayed in products that support them. Only available if the User Photo field is mapped to an LDAP photo attribute in the server settings. To remove the photo, unmap the User Photo field. See Mapping LDAP attributes, page 58.

4. Select **Allow user to authenticate using single sign-on** to enable single sign-on.

   Single sign-on allows users to log in to Helix ALM products using their network credentials. This option is only available for LDAP users and if single sign-on is enabled for the LDAP server. See Setting LDAP options, page 52 and Enabling single sign-on for users, page 63.

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

5. Click **Remove LDAP Association** to change the user to a global non-LDAP user.

> **Note:** If you remove the LDAP association by mistake, click **Set LDAP Association** to reset it before saving the changes. See Associating users with an LDAP server, page 28.

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

Associating users with an LDAP server

You can associate users on the license server with an LDAP user record to sync them with the LDAP or Active Directory server.

1. Click **Global Users**.

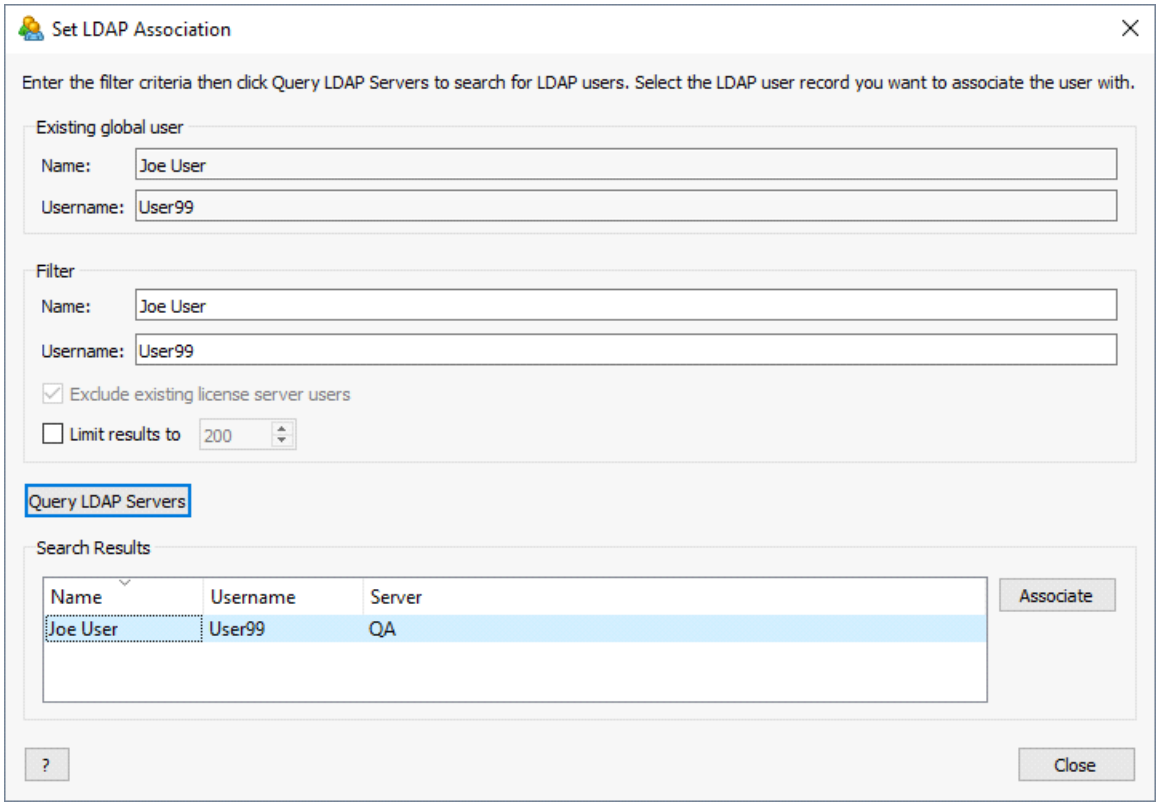
   The Global Users dialog box opens.

2. Select a user and click **Edit**.

   The Edit User dialog box opens.

3. Click **Set LDAP Association**.

   The Set LDAP Association dialog box opens. The user's name and username are added as filters.



4. Select **Limit results to** and enter a value to limit the number of records returned from the LDAP servers. The default value is 200.
5. Click **Query LDAP Servers**.

   A list of matching users is displayed in the Search Results area.

6. Select the record to associate the user with and click **Associate**.

   A message is displayed to indicate the user was associated with the LDAP record.

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

   The user changes to a global LDAP user.

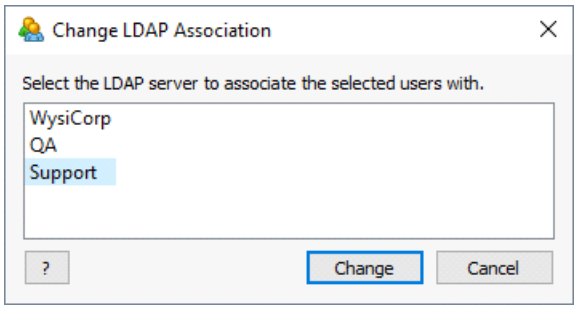
Changing LDAP server association

If you are migrating LDAP or Activate Directory servers, you can change the server association for LDAP users to sync them with a different server.

> **Note:** To change the server association, a user with the same username must already exist on the new LDAP server.

1. Select the LDAP users to associate with a different server in the Global Users list.
2. Click **Quick Edit** and then select **Change LDAP Association**.

   The Change LDAP Association dialog box opens.



3. Select the server to associate the users with.

   This list contains the LDAP server connections configured on the license server. If you need to add a server connection, see Adding LDAP servers, page 53 and Adding Active Directory servers, page 55.
4. Click **Change**.

   The Change LDAP Association Status dialog box opens and displays a message to indicate the change status.

   If usernames are not found on the selected LDAP server, a list of users that cannot be changed is returned. Verify users with these usernames are available on the server before trying to change the association again.
5. Click **Close** when you finish.

Resyncing LDAP users

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

1. Click **Global Users**.

   The Global Users dialog box opens.
2. Select the users to resync.

   All LDAP users are resynced if you do not select specific users.
3. Click **Resync LDAP Users**.

   The user information is resynced.

Note: You can also set the server to resync automatically. See Setting LDAP options, page 52.

Changing fields for multiple users

Use bulk changes to change multiple user records at the same time. You can:

- Update user information, such as phone number, email address, password settings, and user type.
- Change security settings, including license server security permissions and single sign-on or external authentication options.
- Assign product licenses, change license types, and assign users to license pools.
- Update address information, including the company, division, and department.
- Enter notes about users.

Note: Users must have security permissions to administer all license server functions or manage global users to perform bulk changes. See Adding users, page 22.

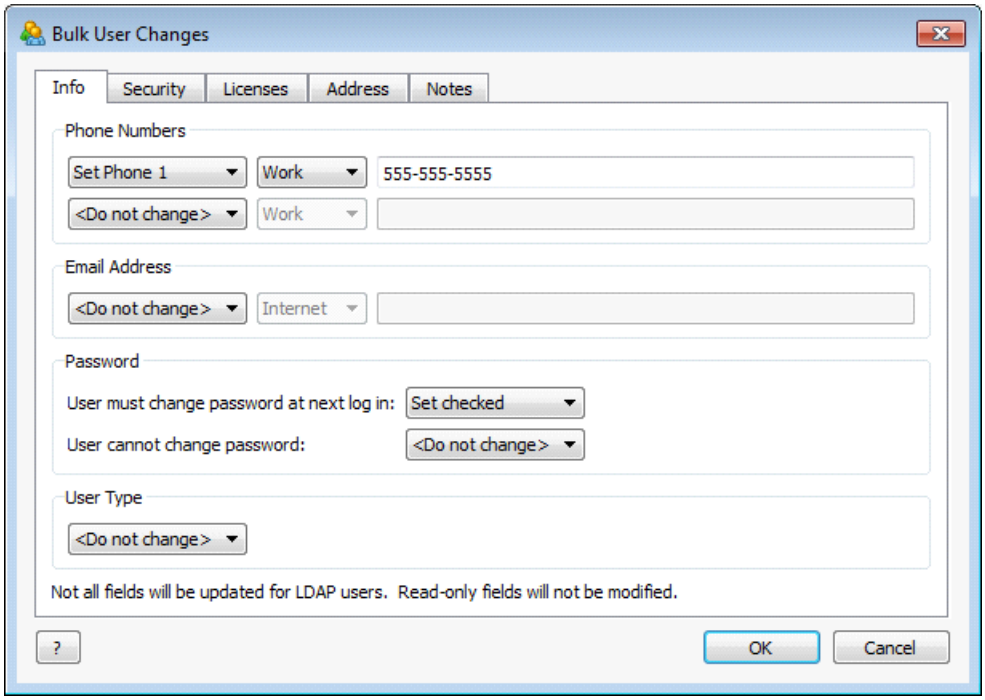
Replacing info field values

You can update general information, such as phone number, email address, password settings, and user type, for multiple users at the same time.

Note: LDAP user phone numbers and email addresses cannot be modified.

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

   The Bulk User Changes dialog box opens.



3. Make any changes. The available options depend on the field type.

   To set the field to a new value, select **Set** and enter a value.

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

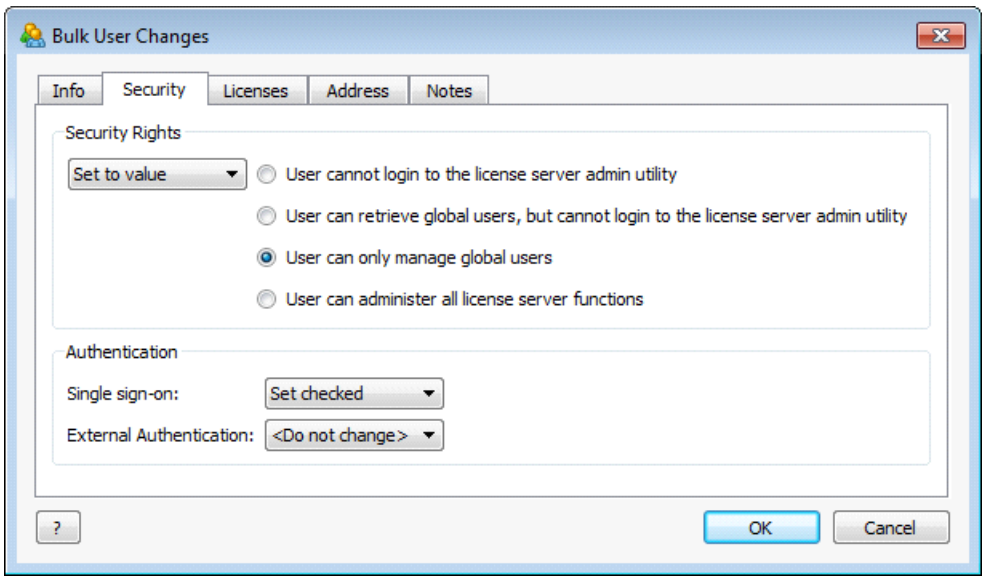
Replacing security field values

You can update security settings for multiple users at the same time.

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

   The Bulk User Changes dialog box opens.

3. Click the **Security** tab.



4. Make any changes. The available options depend on the field type.
   - To change the security rights, select **Set to value** and select a value.
   - To enable single sign-on, select **Set checked**. To disable single sign-on, select **Set unchecked**.
   - To enable or require external authentication, select **Set Allowed** or **Set Required**. To disable external authentication, select **Set Not Allowed**.
5. Click **OK** to save the changes.

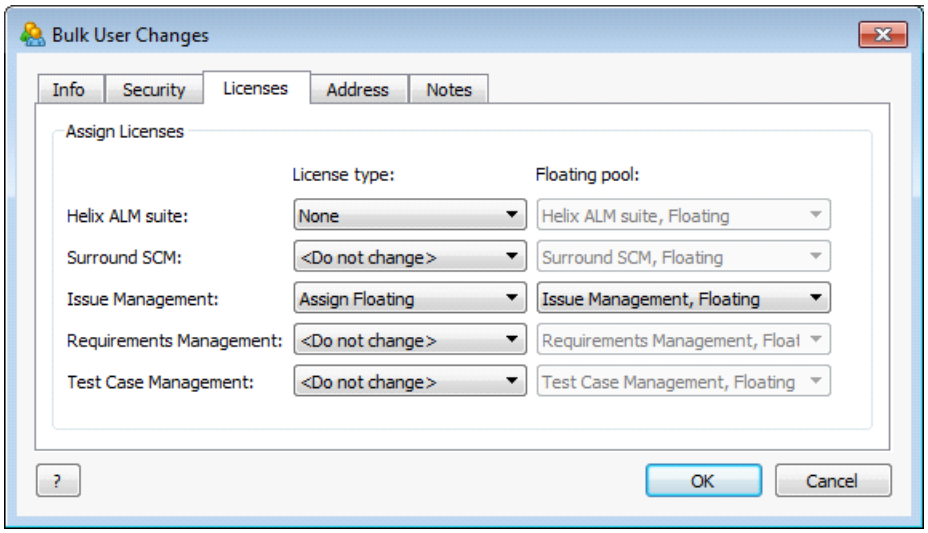
Replacing license field values

You can update license information for multiple users at the same time. For example, you may want to add multiple users to a new license pool.

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

   The Bulk User Changes dialog box opens.

3. Click the **Licenses** tab.



4. Make any changes to the license type.
   - **Assign floating** assigns floating licenses. You can also select a license pool to assign users to if a pool is available for the license type. See Adding license pools, page 13.
   - **Assign named** assigns named licenses. Named licenses cannot be assigned to inactive users.
   - **None** removes the license assignments.
5. Click **OK** to save the changes.

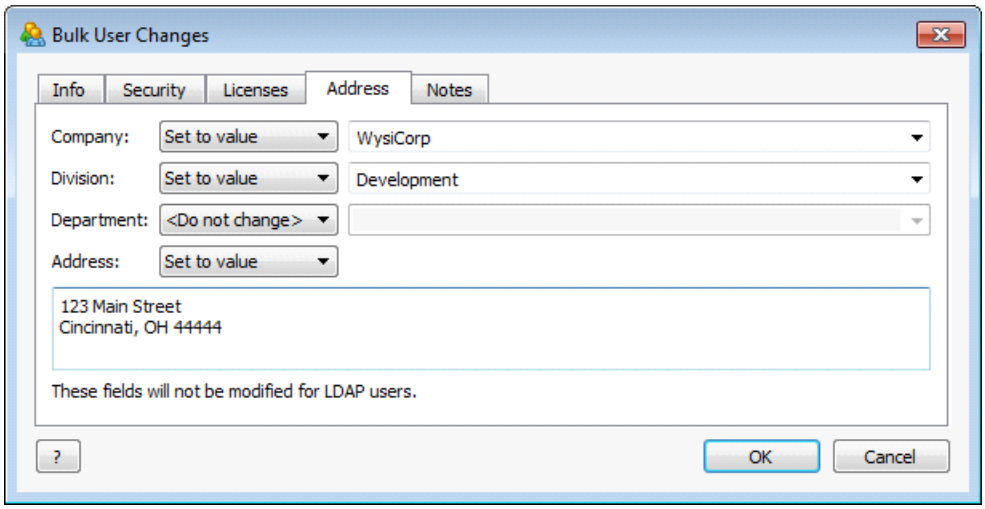
Replacing address field values

You can update address information for multiple users at the same time.

> **Note:** LDAP user address information cannot be modified.

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

   The Bulk User Changes dialog box opens.
3. Click the **Address** tab.



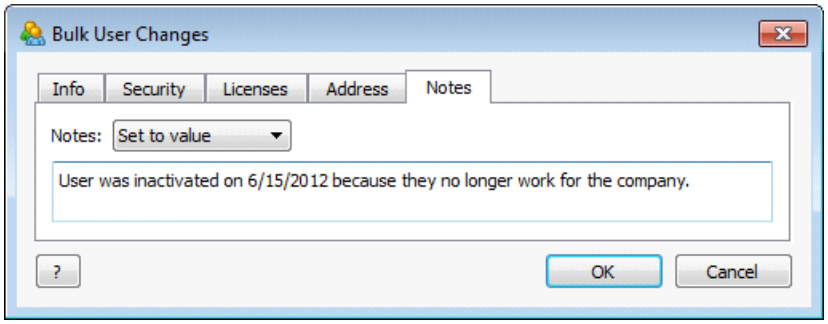
4. Make any changes. The available options depend on the field type.
   - To set the field to a new value, select **Set to value** and enter or select a value.
   - To add text to the beginning of a text field value, select **Prepend** and enter the text.
   - To add text to the end of a text field value,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

Replacing notes field values

You can update notes about multiple users at the same time.

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

   The Bulk User Changes dialog box opens.
3. Click the **Notes** tab.



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

Controlling Helix ALM License Server Admin Utility access

Users cannot log into the Helix ALM License Server Admin Utility by default, but you can change security permissions for users you want to allow access to retrieve global users in Helix ALM products, manage all global users, or administer all license server functionality. For example, you may want to provide Helix ALM or Surround SCM administrators access to retrieve global users and Helix ALM Data Warehouse users full license server administrative rights to configure the data warehouse.

1. Click the **Security** tab when you are adding or editing a user.

   > **Tip:** You can also set security rights multiple users at the same time. See Replacing security field values, page 31.

2. Select the security rights to assign to the user.
   - **User cannot login to the license server admin utility** prevents users from accessing the admin utility. This is the default option and is recommended for most users.
   - **User can retrieve global users, but cannot login to the license server admin utility** allows users to only retrieve global users in Helix ALM products.
   - **User can only manage global users** allows users to create and maintain global users.
   - **User can administer all license server functions** provides access to all admin utility commands. You should only select this option for administrative users.
3. Click **OK** to save the changes.

Inactivating users

To prevent users who no longer need access to Helix ALM products from logging in and keep the user records to use again later, you can inactive users instead of deleting them.

1. Click **Global Users**.

   The Global Users dialog box opens.
2. Select the user to inactivate.
3. Click **Quick Edit** and then select **Inactivate**.

   The user is inactivated.

   > **Note:** If the user is assigned a named license, you are prompted to confirm the inactivation. Click **Yes** to confirm the inactivation.

Activating users

Activate an inactive user to allow them to log in.

1. Click **Global Users**.

   The Global Users dialog box opens.
2. Select the user you want to activate.
3. Click **Quick Edit** and then select **Activate**.

   The user is activated. You may need to assign a license to the user. See Assigning licenses, page 16.

Unlocking users

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

> **Note:** You can set failed login lockout options on the license server. See Setting password options, page 51.

1. Click **Global Users**.

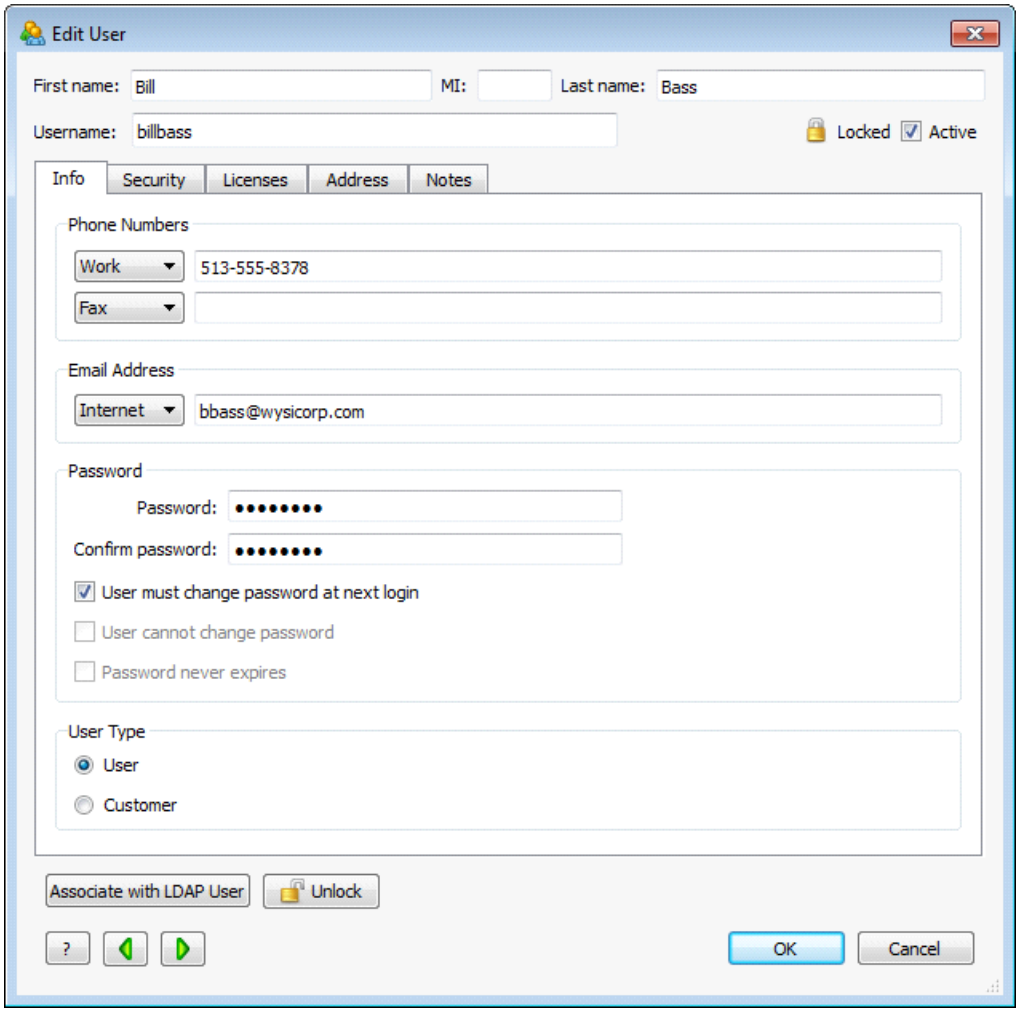
   The Global Users dialog box opens.

2. Select a locked user.

   > **Note:** To unlock multiple users, select the users in the Global Users list, click **Quick Edit**, and then select **Unlock**. You can add the Locked column to the Global Users list to easily see which users are locked. See Customizing the Global Users list, page 21.

3. Click **Edit**.

   The Edit User dialog box opens. The locked indicator is displayed.



4. Click **Unlock**. This button is only available if the user is locked.

The user is unlocked and can log in.

Exporting user information

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

> **Note:** License pool information for assigned licenses is not exported.

1. Choose **File > XML Export**.

   The Export dialog box opens.

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

   The default filename is Untitled.xml.

3. Click **Save**.

   The file is exported.

Importing user information

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

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

> **Note:** See Exporting user information, page 36 for information about exporting users.

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

   The XML Import dialog box opens.

2. Click **Browse** to select a file.

3. Select the file and click **Open**.

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

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

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

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

   The user information is imported.

Deleting users

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

1. Click **Global Users**.

   The Global Users dialog box opens.

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

You are prompted to confirm the deletion.

3. Click **Yes**.

   The user is deleted.

Undeleting users

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

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

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Click **Undelete Users**.

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

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

   The users are undeleted and removed from the list.

Printing the global users list

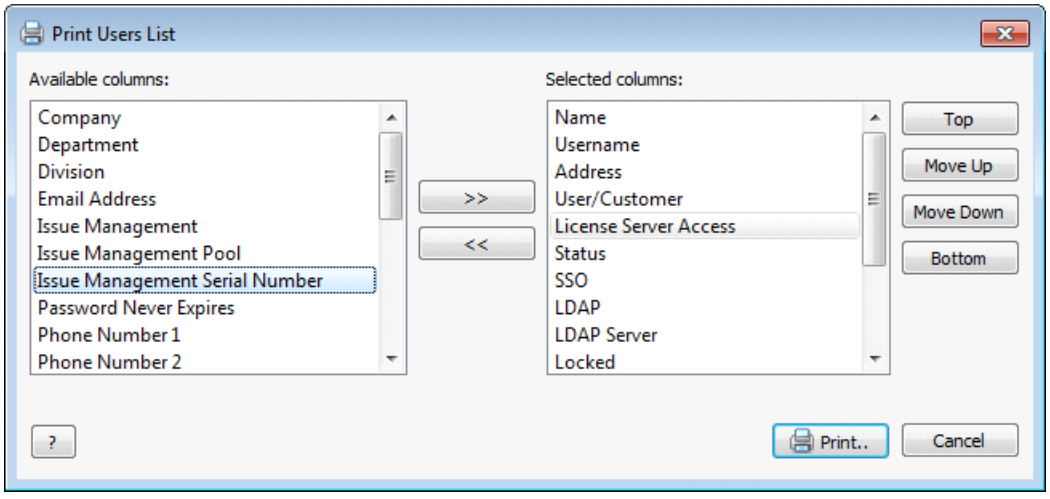
You can print the information in the Global Users dialog box.

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Click the **Print** button.

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



3. Select the column to add in the Available columns list and click >> to move it to the Selected columns list.

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

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

   The Print dialog box opens.
6. Select any options and click **Print**.

Configuring the Server

You can configure various license server options including log levels, password options, the database type, and LDAP options.

Options	Use to:	Additional information
Log	Select the type of information to add to the server log.	Setting server log options, page 39
Server	Set server communication options, such as enabling encryption, changing the server port, and setting the communications password, and enable renaming of usernames and external authentication.	Setting server options, page 41
Server Database	Configure the license server database location, change or convert the server database, and specify how often to validate RDBMS connections.	Configuring the server database, page 47
LDAP	Enable LDAP support and add LDAP and Active Directory servers.	Setting LDAP options, page 52, Adding LDAP servers, page 53, and Adding Active Directory servers, page 55
Passwords	Specify password requirements and restrictions.	Setting password options, page 51

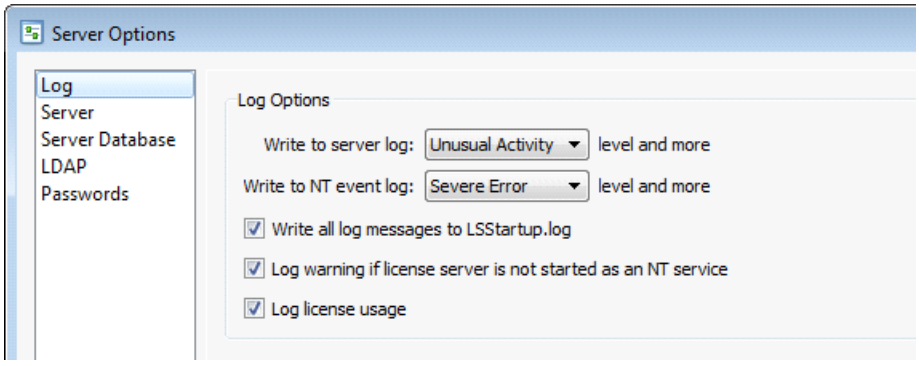
Setting server log options

The license server creates log files that record events, such as severe errors or unusual activity. The log files can help you monitor the server's operation and troubleshoot any issues. See Viewing the server log, page 69 and Troubleshooting, page 79.

1. Click **Server Options**.

   The Server Options dialog box opens.

2. Select the **Log** category.



3. Select any log options.

- **Write to server log** specifies the types of events to write to the log. See Server log levels, page 40.
- **Write to NT event log** or **Write to Unix system log** specifies the types of events to write to the event or system log. This option is named based on the operating system the license server is running on.
- **Write all log messages to LSStartup.log** writes all messages to the log file. Select this option if you are experiencing server problems and want to log messages that occur after startup. Startup errors are always logged to this file even if this option is not selected. The LSStartup.log file is stored in the Helix ALM License Server application directory on Windows and in `/var/log` on Linux. You can email the log file to Perforce support for help resolving problems.
- **Log warning if license server is not started as a service** writes a warning to the log file if the license server is started as an application. Most companies run the license server as a service. If it runs as an application, the license server is shut down by the operating system when a user logs out of the server computer, which can negatively affect other users. Only available on Windows.
- **Log license usage** tracks when licenses are used. You can use this information to determine the appropriate time to perform system maintenance and to see if additional licenses are needed. You can also clear the data as needed. See Clearing the license usage log, page 40.

> **Note:** The license server only provides usage reports for Helix ALM licenses, Surround SCM 2009 and later floating licenses, Surround SCM 2010 and later named licenses, and TestTrack 2009 and later licenses.

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

Server log levels

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

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

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

Clearing the license usage log

Depending on how you use license usage data, you may want to occasionally clear the license usage log. For example, you may want to archive your organization's license usage for a specific timeframe, such as on a monthly basis.

Note: Database queries are used to clear license usage information from the server database. If you use the native SQLite database format, you need to install the sqlite3 command line utility to execute the queries. If you are not familiar with database queries, or your server database is stored in a different RDBMS, ask your DBA for help.

1. Click **Server Options**.

   The Server Options dialog box opens.
2. Select the **Log** category.
3. Clear **Log license usage**.
4. Click **OK** to save the changes.
5. In the license server database, remove the rows from the following tables:
   - EVENT
   - EVENTDETAILS
   - EVENTUSER
6. If you want to maintain a record of license usage to the current date, use the following queries to copy data from the master tables to archive tables:
   - INSERT INTO Event_ARCHIVE (SELECT * FROM Event)
   - INSERT INTO EventDetails_ARCHIVE (SELECT * FROM EventDetails)
   - INSERT INTO EventUser_ARCHIVE (SELECT * FROM EventUser)
7. To delete data from the master table after it is archived, use the following queries:
   - DELETE FROM Event;
   - DELETE FROM EventDetails;
   - DELETE FROM EventUser;
8. To maintain unique identifiers for the archived data, use the following queries:
   - INSERT INTO Event_ARCHIVE(SELECT * FROM Event WHERE id < (SELECT MAX(id) FROM Event))
   - INSERT INTO EventDetails_ARCHIVE(SELECT * FROM EventDetails WHERE id < (SELECT MAX(id) FROM Event))
   - INSERT INTO EventUser_ARCHIVE(SELECT * FROM EventUser WHERE id < (SELECT MAX(id) FROM EventUser))
   - DELETE FROM Event WHERE id (SELECT MAX(id) FROM Event))
   - DELETE FROM EventUser WHERE id (SELECT MAX(id) FROM EventUser))
   - DELETE FROM EventUser WHERE id (SELECT MAX(id) FROM EventUser))
9. After the log is cleared, re-enable license usage logging. See Setting server log options, page 39.

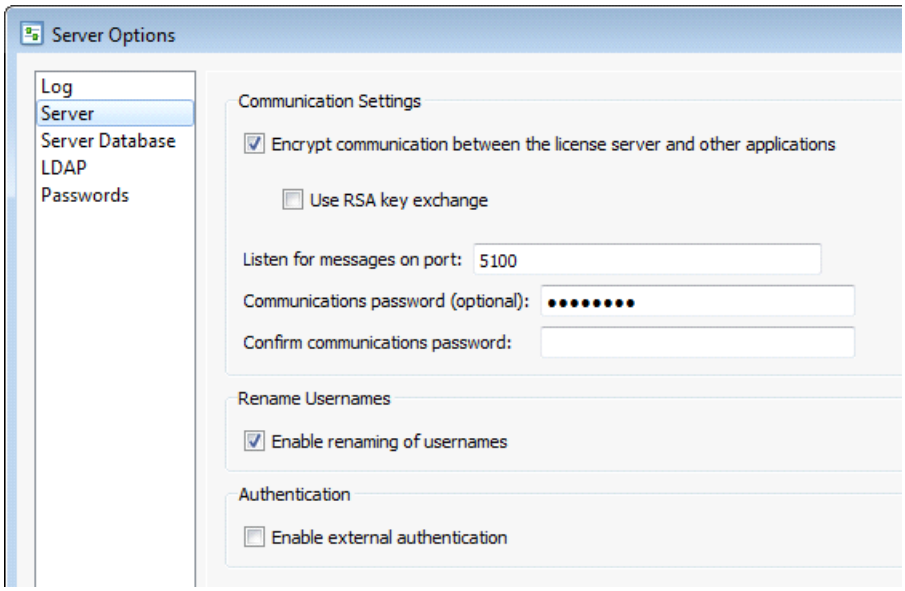
Setting server options

You can configure server options to encrypt communication between the license server and other applications, set a communications password, allow usernames to be changed, and enable external authentication.

1. Click **Server Options**.

   The Server Options dialog box opens.

2. Select the **Server** category.



3. Select or enter any **Communication Settings**.

   - **Encrypt communication between the license server and other applications** encrypts all communication between the license server, admin utility, API, and other Helix ALM product servers. Encryption scrambles data to prevent interception by hackers, or eavesdropping, as it passes between the license server and other applications. Encryption increases security, but may slightly affect performance. Select this option if you organization's network is secure and no license server client or Helix ALM server applications outside of the network communicate with license server. See Securing communication between the license server and other applications, page 44 for information about encryption, authentication, and key exchange methods used by the license server.
   - **Use RSA key exchange** provides strong key exchange for communication between the license server and license admin utility applications. 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 the license server 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 license server admin clients that access the license server. See Configuring RSA key exchange, page 46 for information about setting up RSA. This option is only available if **Encrypt communication between the license server and other applications** is selected.
   - **Listen for messages on port** specifies the port number the license server uses to communicate with Helix ALM products. The default port is 5100.
   - **Communications password** provides additional security by requiring Helix ALM product servers to use the specified password to communicate with the license server. If you change the communications password, you must also change the password in the other products or users cannot log in.

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

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

4. Select **Enable renaming of usernames** to allow administrators to change usernames.

   Only select this option if you have a specific reason to change usernames, such as corporate security restrictions that require a standard username format. See Changing usernames, page 26.

5. Select **Enable external authentication** to allow users to log in to Helix ALM products using credentials for your external authentication system. See Using External Authentication, page 65.

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

Changing key exchange options

If you change key exchange options, license server client applications and the web server that hosts the license server web admin client 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 native server admin utility users need to import in the server connection settings. If you use the web server admin utility, import the file from the License Server CGI Configuration utility on the web server computer. See Changing web server admin utility CGI settings, page 4
RSA key exchange	No encryption or basic encryption (Encrypt server communication between the license server and other applications is selected)	Remove the public key fingerprint from any clients that connect to the server. Click **Remove** in the Edit Server Connection dialog box in native clients and in the License Server CGI Configuration utility for web clients.

See Configuring RSA key exchange, page 46 for information about adding and removing keys for the server admin utilities.

Securing communication between the license server and other applications

Keeping your Helix ALM License Server and other Helix ALM product data secure is critical. To prevent hackers from compromising your data, encrypt communication between license server and other applications, specifically Helix ALM product servers, license server admin clients, and the license server API.

The following information explains how the license server encrypts data, how authentication works, and how key exchange is used for different authentication methods. See Setting server options, page 41 for information about configuring secure communication.

Encryption

Encryption scrambles data to prevent interception, or eavesdropping, as it passes between the license server and other applications. The license server uses the OpenSSL implementation of Advanced Encryption Standard-256 (AES-256) to encrypt communication between in Helix ALM License Server 2014.1 and later. RC4 encryption is used for backward compatibility with earlier versions.

Communication between the license server and other license servers, Helix ALM product servers, license server admin clients, and the license server API is encrypted when you select **Encrypt communication between the license server and other applications** in the Server category in the server options. See Setting server options, page 41.

> **Note:** Always use encryption unless you are evaluating Helix ALM products or troubleshooting a performance issue. Passwords are always encrypted even if communication is not.
>
> Login credentials sent from the Helix ALM License Server Web Admin Utility and the CGI is 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 to the license server. The following authentication methods are used by the license server.

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 license server. The server sends different mathematical proof that it knows the password to the other application.
LDAP	Using single sign-on—Credentials proving the user's identity are sent from the LDAP server to the license server and verified.
	Not using single sign-on—The username and password are sent to the license server.
External authentication	Data from the organization's authentication system is sent to the license 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 license server.

Key exchange method	When it is used	How it works	To use it:
Secure Remote Password (SRP)	User is authenticated by 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 **Encrypt communication between the license server and other applications** in the 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 **Encrypt communication between the license server and other applications** in the server options.
RSA	RSA key exchange is enabled in the server options. Only used in communication between the license server and license server admin utility clients.	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 **Encrypt communication between the license server and other applications** and **Use RSA key exchange** in the 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 applications outside of the network can communicate with the license server.

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

- Your organization stores sensitive information in Helix ALM products.
- Your network is potentially insecure.

- Users log in to client applications from outside your network.
- Users are authenticated to the license server using LDAP, single sign-on, or external authentication.

Using RSA requires additional setup for users. See Configuring RSA key exchange, page 46.

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 products and administrators use the license server admin utility clients outside of your network and log in with a username and password.

If you use RSA key exchange, a public key fingerprint must be imported to all license server admin clients that connect to the license server.

1. Click **Server Options**.

   The Server Options dialog box opens.

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

   You are prompted that all admin users will need to modify their server settings if RSA is enabled.

4. Click **Yes**.

   A public key is generated on the license 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 License Server application directory on the server computer. To keep these key files secure, make sure only the user that runs the license server has read and modify access to them.

   > **Note:** If you clear the **Use RSA key exchange** option, you are prompted that all admin 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 native server admin utility clients and in the License Server CGI Configuration utility for the web server admin utility client.

5. Click **Download Public Key** to save an XML file that contains the license server address, port number, and public key fingerprint.

   This file must be distributed to users so they can import it to license server admin 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 license server installation could be hacked.

   > **Note:** The server address in the XML file includes the default hostname of the license server computer. If users with license server admin permissions 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.

6. Click **OK** to save the changes.
7. Import the server settings file to license server admin clients or CGIs that connect to the server.

- Native admin client—See Adding server connections, page 8.
- Web admin clients—See Changing web server admin utility CGI settings, page 4.

Tip: If you suspect the private key on the license 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 license server admin utility clients that connect to the server.

Configuring the server database

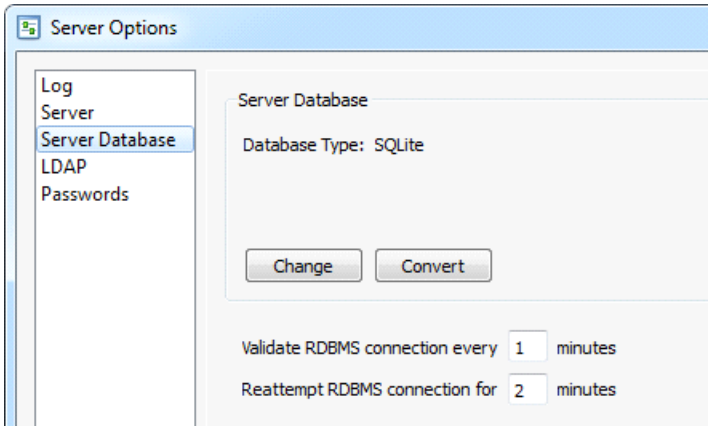
The license server uses SQLite for the backend database by default. You can change the database location or convert the database to a use a different Relational Database Management System (RDBMS).

1. Click **Server Options**.

   The Server Options dialog box opens.

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

   The current database type and location are displayed.



3. Click **Change** to change the database location. See Changing the server database, page 48.
4. Click **Convert** to convert the database to a different type. See Converting the server database, page 49.
5. Make any changes to the RDBMS connection options.
   - **Validate RDBMS connection** specifies how often the license server validates the RDBMS connection. The default is every 5 minutes. You may want to decrease the value if network or performance issues occur and you want to validate connections more frequently. Valid values are 1-60 minutes.
   - **Reattempt RDBMS connection** specifies how long the license server attempts connecting to an RDBMS server before initializing the server database. The default is every 2 minutes. Valid values are 0-10 minutes. There is a 20 second delay between each attempt. If you stop the license server while it is connecting to an RDBMS server, it stops after the 20 second delay ends. You cannot log in to the license server while it is connecting to an RDBMS server.
6. Click **OK** to save the changes.

Changing the server database

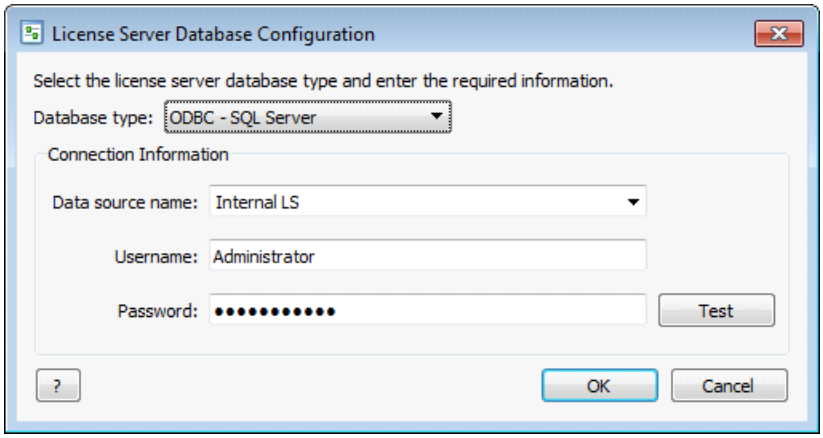
You can configure the license server to use a different server database location. For example, you may need to change the server database if you move it to another computer or experience problems and want to use a backup copy. You should not need to frequently change the server database location.

Note: Back up the server database before changing the configuration. See Backing up the server database, page 50.

1. Make sure you are logged into the license server that uses the database to change. Choose **File > Connect to Server** to connect to a different server.
2. Click **Server Options**.

   The Server Options dialog box opens.
3. Select the **Server Database** category.
4. Click **Change**.

   The License Server Database Configuration dialog box opens.



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

   The available fields change based on the selected database type.
7. Click **Test** to test the connection.

   The Test Connection dialog box opens and displays the results.

   Tip: If the test connection fails, contact your DBA or internal support department for help.
8. Click **Close** to close the Test Connection dialog box.
9. Click **OK** to change the database location.

   The following information is verified if you selected ODBC - SQL Server or Oracle Native:

   - The specified information connects to a valid database.
   - The database is not used by another license server.

- The required database tables exist and are accessible. If the database does not contain any license server tables, you are prompted to create them. See Automatically creating Helix ALM License Server tables, page 50.

You return to the Server Database category.

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

    Stop and restart the license server to complete the process.

Converting the server database

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

Keep the following in mind before you start the conversion:

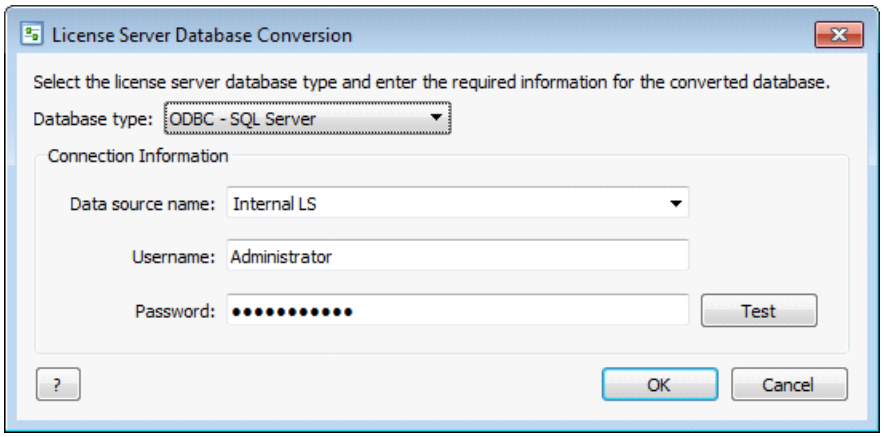
- The database you are converting to must be created before the conversion (except SQLite).
- All tables in the physical database must be empty (except SQLite).
- The database you are converting cannot be in use by another Helix ALM application or another license server.
- All other users must be logged out of the license server and admin utility.
- Hard drive crashes or conversion errors can result in data loss. It is important to back up the server database regularly. See Backing up the server database, page 50.

Note: If you are converting to ODBC - SQL Server, we recommend that you manually create the server database tables. The license server can also create the tables during the conversion. See Automatically creating Helix ALM License Server tables, page 50.

1. Make sure you are logged into the license server to convert the database for. Choose **File > Connect to Server** to connect to a different server.
2. Click **Server Options**.

   The Server Options dialog box opens.
3. Select the **Server Database** category.
4. Click **Convert**.

   The License Server Database Conversion dialog box opens.



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

   The available fields change based on the selected database type.

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

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

   The Test Connection dialog box opens and displays the results.

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

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

   You are prompted to start the conversion.

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

    If you do not select this option, you can manually change the database the license server is using after the conversion. See Changing the server database, page 48.

11. Click **Yes**.

    The Conversion Status dialog box opens and the conversion starts.

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

Automatically creating Helix ALM License Server tables

When you upgrade or convert the license server database, the physical database and empty tables must be created before data can be converted. If the tables do not exist, you are prompted to allow the license server to create them. See Setting Up RDBMS Databases, page 71.

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

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

Backing up the server database

The Helix ALM License Server database should be backed up regularly.

SQLite databases

By default, the server database is stored in the following locations on the computer that hosts the license server:

- Windows—C:\Program Files\Perforce\License Server\LicenseServDb
- Linux—/var/lib/splicsvr/LicenseServDb

To back up the server database:

1. Stop the license server.
2. Copy the LicenseServDb directory to a backup directory.
3. Restart the license server.

Other RDBMS databases

If the server database is stored in an RDBMS database, ask your DBA for help with backups.

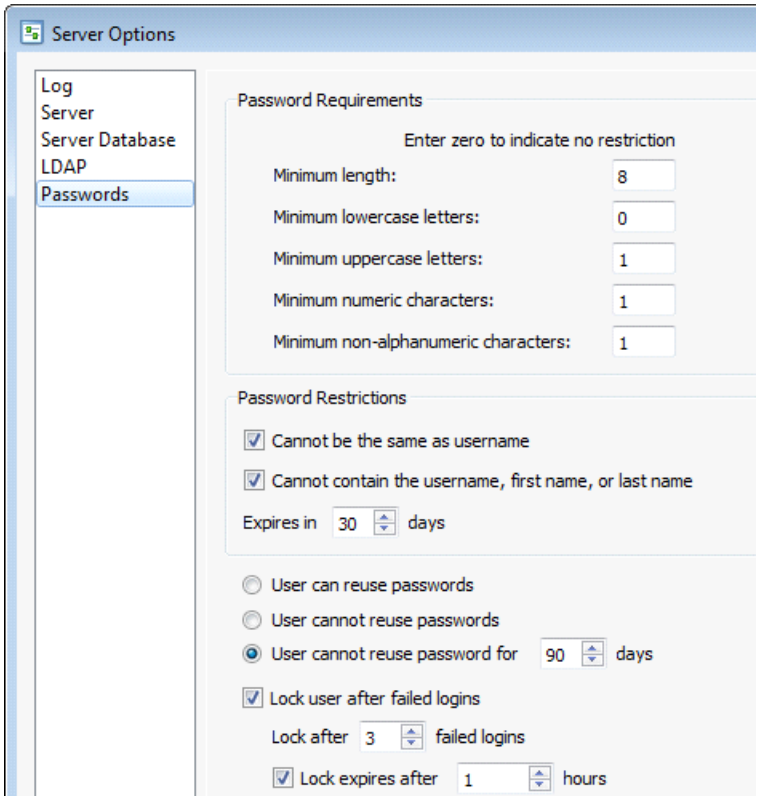
Setting password options

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

1. Click **Server Options**.

   The Server Options dialog box opens.

2. Select the **Passwords** category.



3. Enter any **Password Requirements** to require a minimum password length or minimum number of specific character types. This can help you set strict password requirements that make it more difficult for unauthorized users to crack.
4. Select any **Password Restrictions**.
   - **Cannot be the same as username** restricts users from using their username as their password.
   - **Cannot contain the username, first name, or last name** restricts users from using their username, first name, or last name as their password.
   - **Expires in** specifies how often passwords expire. Requiring users to change passwords periodically enhances security and may also be required by compliance programs, such as 21 CFR Part 11.
5. Select a password reuse option. Preventing users from reusing passwords minimizes the risk of unauthorized users finding and using passwords.
6. Select **Lock user after failed logins** to prevent users from logging in to Helix ALM products after the specified number of failed logins.

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

   > **Note:** If a user is locked, an administrator must unlock them on the license server before they can log in. See Unlocking users, page 35. Restarting the license server does not release locks, but it resets the number of failed logins to 0.

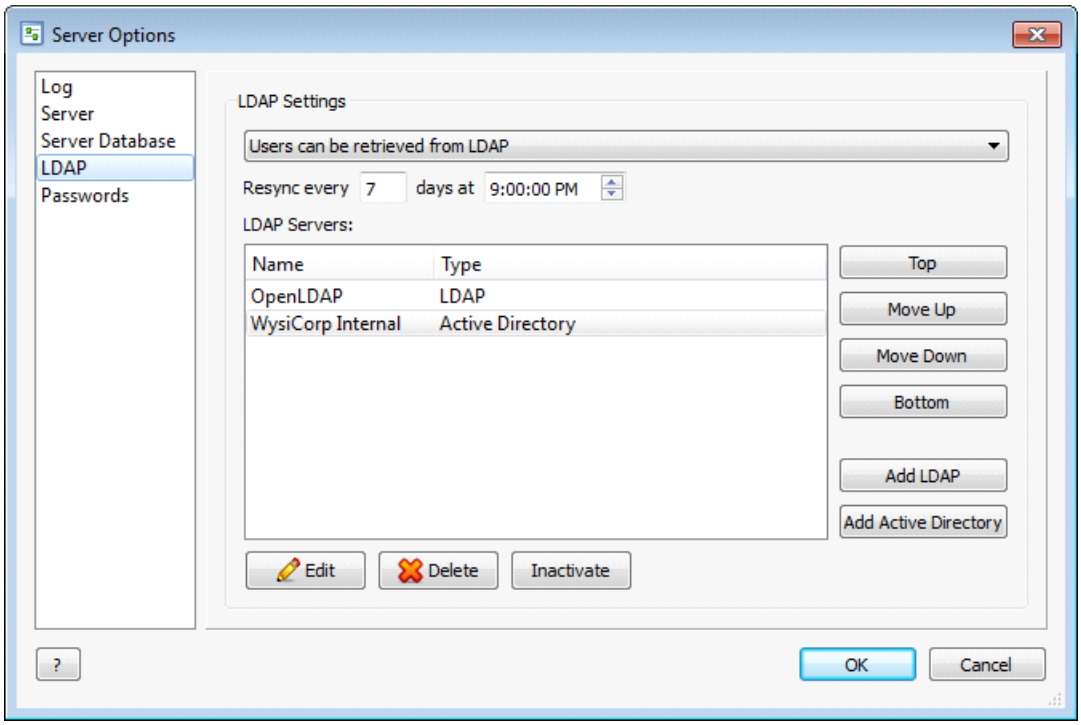
7. Click **OK** to save the changes.

Setting LDAP options

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

1. Click **Server Options**.

   The Server Options dialog box opens.
2. Select the **LDAP** category.



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

   Note: You can also manually re-sync LDAP users. See Resyncing LDAP users, page 29.
5. Click **Add LDAP** to add an LDAP server or click **Add Active Directory** to add an Active Directory server. See Adding LDAP servers, page 53 or Adding Active Directory servers, page 55.
6. Click **OK** to save the changes.

Adding LDAP servers

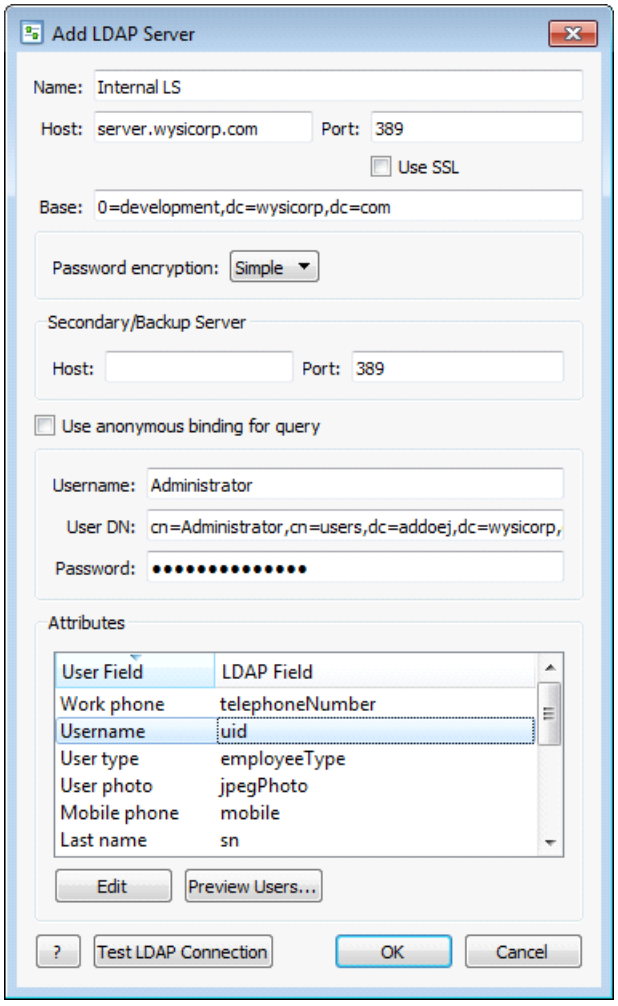
Add an LDAP server to retrieve users from it.

Note: The license server only retrieves LDAP users configured in the following objectClass types: person, organizationalPerson, and inetOrgPerson.

1. Click **Server Options**.

   The Server Options dialog box opens.
2. Select the **LDAP** category.
3. Click **Add LDAP**.

The Add LDAP Server dialog box opens.



4. Enter a server **Name**, the LDAP server IP address or alias as the **Host**, and the **Port** number. The default port is 389.

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

5. Enter the **Base** directory DN to specify where to start searching from in the LDAP tree. For example, your Base DN is wysicorp.com and includes development, sales, and support nodes. Entering o=sales, dc=wysicorp, dc=com instructs the license server to start searching from sales.
6. Select **Use SSL** to encrypt authentication messages sent over the network.

   Selecting this option requires the license server to use the Secure Sockets Layer (SSL) protocol when sending and receiving authentication transmissions between the license server, the LDAP server, and Helix ALM products. We recommend selecting this option if the license server is configured to use simple password encryption.
7. Select the type of **Password encryption** to use when sending usernames and passwords over the network.

- **Simple** sends usernames and passwords as plain text. We recommend selecting the **Use SSL** option if you use simple password encryption. The Username and Password fields are required if this option is selected.
- **DIGEST-MD5** sends usernames and passwords as encrypted text. This option is only available if the license server is running on Linux. The Username, User DN, and Password fields are required if this option is selected.

8. Optionally enter the **Host** address and **Port** number of a backup server.

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

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

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

10. Enter a **Username**, **User DN**, and **Password** if anonymous binding is not enabled.
    - **Username** is the name of the user to use to connect to the LDAP server. The license server will try to automatically connect to the LDAP server using one of the supported SASL authentication mechanisms.
    - **User DN** is the distinguished name (DN) of the user. This sequence of attributes and values specifies the location of an entry in the LDAP tree. For example: cn=Administrator, cn=users, dc=addoej, dc=wysicorp,dc=com.
    - **Password** is the password of the user to use to connect to the LDAP server.
11. Select an LDAP user attribute and click **Edit** to map the attribute to a license server user field. See Mapping LDAP attributes, page 58.
12. Click **Test LDAP Connection** to test the LDAP server connection.

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

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

    The server is added.

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

Adding Active Directory servers

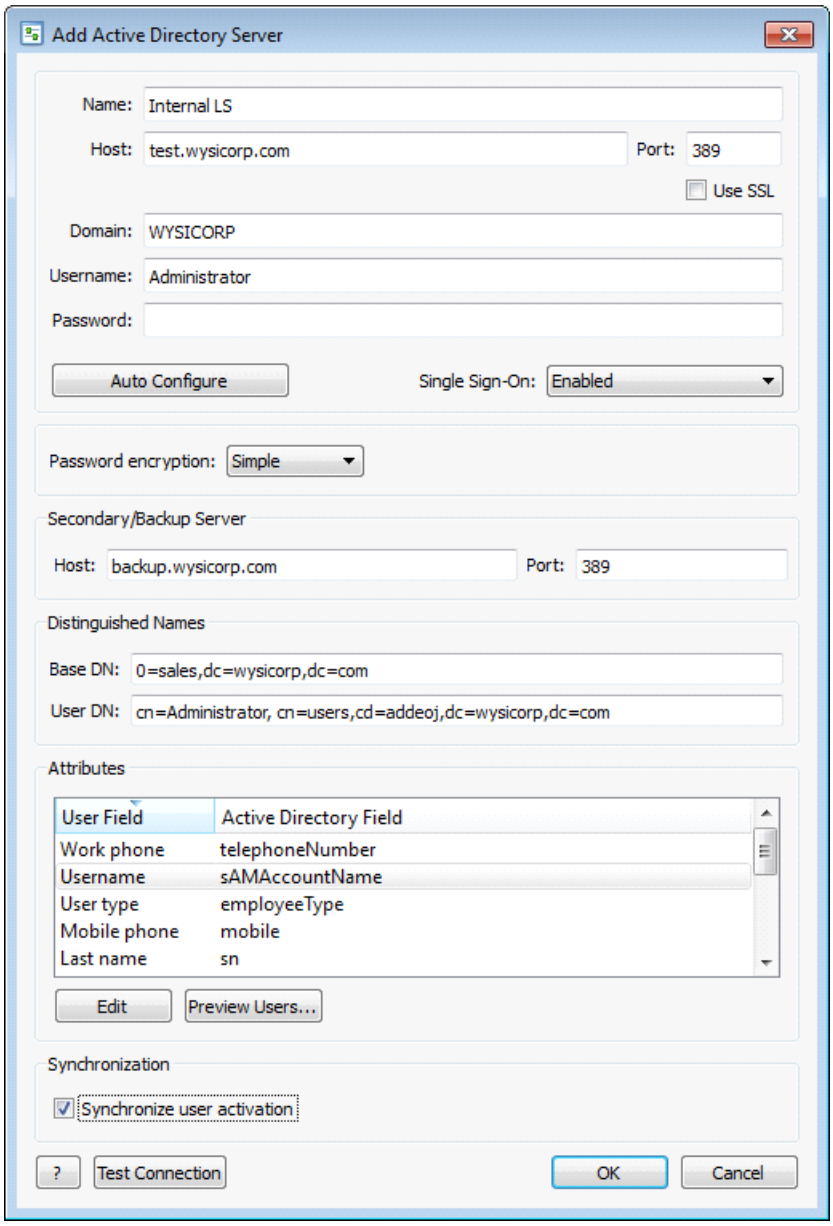
Add an Active Directory server to retrieve users from it.

1. Click **Server Options**.

   The Server Options dialog box opens.

2. Click **Add Active Directory**.

   The Add Active Directory Server dialog box opens.



3. Enter a server **Name**, the IP address or alias for the Active Directory server as the **Host**, and the **Port** number where the Active Directory server resides. The default port is 389.

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

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

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

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

   Single sign-on allows LDAP users to automatically log in to Helix ALM products using the same credentials used to log in to their computer. For example, your organization may use a non-password login method, such as a secure ID token or biometrics. Single sign-on uses the same authentication to log in to Helix ALM products. See Configuring single sign-on for LDAP servers, page 61.
8. Click **Auto Configure** to query the Active Directory server for the configuration information.

   To manually enter the information, click **Advanced**.

   - **Base DN** specifies where to start searching from. For example, your Base DN is wysicorp.com and includes development, sales, and support nodes. Entering o=sales, dc=wysicorp, dc=com instructs the license server to start searching from sales.
   - **User DN** specifies the location of an entry based on a sequence of attributes and values. For example: cn=Administrator, cn=users, dc=addoej, dc=wysicorp, dc=com.
   - Optionally enter the **Host** address and **Port** number of a backup server. The backup server is only queried if the primary server cannot be reached.
   - To map an LDAP attribute to a license server user field, select it and click **Edit**. See Mapping LDAP attributes, page 58.

   > **Note:** When you auto configure the settings, the license server queries the Active Directory server for rootDSE information and retrieves the Base DN information. Next, the license server searches for the authentication user's User DN. After this DN is found, the user's CN value is removed and the remaining data is used as the final Base DN. For example, the license server queries an Active Directory server for rootDSE information and retrieves "dc=wysicorp,dc=com" as the Base DN. Next, the license server queries the Active Directory server for the authentication user's User DN and retrieves "cn=Virtual User, cn=Users,dc=wysicorp,dc=com". Finally, the license server trims off the user's CN value and uses "cn=Users,dc=wysicorp,dc=com" as the Base DN.
   >
   > Due to performance reasons, we recommend using a subtree Base DN (e.g., cn=Users, dc=wysicorp, dc=com) instead of the topmost Base DN (e.g., dc=wysicorp,dc=com). If the topmost Base DN is used, it may cause a large amount of unnecessary network traffic. If users are dispersed across the Active Directory tree, we also recommend that you create multiple Active Directory server entries.
9. Select the type of **Password encryption** to use when sending usernames and passwords over the network.

   - **Simple** sends usernames and passwords as plain text. We recommend selecting the **Use SSL** option if you use simple password encryption. The Username and Password fields are required if this option is selected.
   - **DIGEST-MD5** sends usernames and passwords as encrypted text. The Domain, Username, User DN, and Password fields are required if this option is selected.
   - **GSSAPI** uses advanced encryption for usernames and passwords. This option is only available if the license server is running on Windows and is recommended to ensure secure authentication.

10. Select **Synchronize user activation** to automatically sync user activation between Active Directory and the license server. If a user is disabled or enabled in Active Directory, the user is inactivated or activated on the license server.
11. Click **Test Connection** to test the Active Directory server connection.

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

    The server is added.

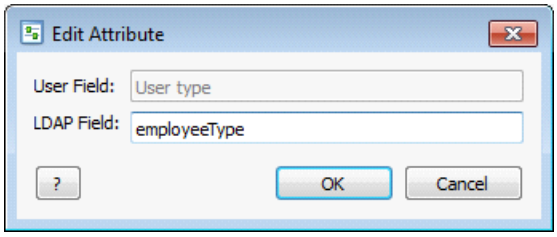
> **Tip:** Servers are queried in the order they are displayed. To reorder the servers, select a server and click **Top**, **Move Up**, **Move Down**, or **Bottom**.

Mapping LDAP attributes

You can map license server user fields to LDAP and Active Directory fields to import information in a user record to the license server. See Default mappings, page 59 for a list of default mappings.

1. Select a user attribute and click **Edit** when you are adding or editing an LDAP or Active Directory server.

   The Edit Attribute dialog box opens.



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

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

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

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

3. To preview the field mappings, click **Preview Users** in the Add Server or Edit Server dialog box. See Previewing mapped LDAP attributes, page 59.
4. Click **OK** to save the changes.

Default mappings

The following LDAP and Active Directory attributes are mapped to license server user fields by default.

License server user field	LDAP/Active Directory attribute
Address	postalAddress
Company	company
Department	department
Division	division
Email	mail
First name	givenName
Initials	initials
Last name	sn
Mobile phone	mobile
User photo Displayed in products that support photos.	jpegPhoto Can also use photo or thumbnailPhoto.
User type	employeeType
Username	uid (LDAP) SAMAccountName (Active Directory)
Work phone	telephoneNumber

Previewing mapped LDAP attributes

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

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

   The Preview LDAP Users dialog box opens.

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

   The Preview LDAP Mapping dialog box opens. LDAP data from the field mappings is displayed in the Info, Address, and Photo categories.

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

3. Click **Close** when you finish.

Editing and deleting LDAP servers

You can edit LDAP server connection or attribute information. You can also delete LDAP servers you no longer need to retrieve users from.

> **Note:** When you delete an LDAP or Active Directory server, any users associated with it are inactivated and cannot access Helix ALM products.

1. Click **Server Options**.

   The Server Options dialog box opens.
2. Select the **LDAP** category.
3. Edit or delete the server.
   - To edit a server, select it and click **Edit**. Make any changes and click **OK**.
   - To delete a server, select it and click **Delete**. Click **Yes** to confirm the deletion.

Inactivating LDAP servers

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

1. Click **Server Options**.

   The Server Options dialog box opens.
2. Select the **LDAP** category.
3. Select the server to inactivate and click **Inactivate**.

   The server is no longer active and will not be queried.
4. Click **OK** to save the changes.

Using Single Sign-On

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

Perform the following tasks to use single sign-on.

1. Review the single sign-on requirements. See Single sign-on requirements, page 61.
2. Enable single sign-on for the Active Directory server connection on the license server. You can require all users to use single sign-on or enable it for individual users. See Configuring single sign-on for LDAP servers, page 61.
3. If you want to let users use single sign-on to log in to Helix ALM Web and the license server web admin utility, enable Windows authentication on the web server that hosts these clients. See Configuring Microsoft IIS for single sign-on from Helix ALM web clients, page 62.
4. If you only want some users to use single sign-on, enable it for the individual users. See Enabling single sign-on for users, page 63.

Single sign-on requirements

- The license server must be running on Windows as a service in an Active Directory domain.
- By default, the server computer Local System account is used to run the license server application. If a different user runs the application, the user must be a trusted delegate in the Active Directory domain.
- Users can use single sign-on for the following Helix ALM client applications. Client and server applications can run on any of the supported platforms.
  - Helix ALM License Server Admin (client and web)
  - Helix ALM Client
  - Helix ALM Server Admin (client and web)
  - Helix ALM Web
  - Surround SCM Client
  - Surround SCM CLI
- Helix ALM client applications must run in the same Active Directory domain as the license server or in a subdomain as part of the Windows forest (group of domain trees).
- Helix ALM and the license server must be hosted by an IIS web server with Windows Integrated Authentication enabled. See Configuring Microsoft IIS for single sign-on from Helix ALM web clients, page 62.

Configuring single sign-on for LDAP servers

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

1. Click **Server Options**.

   The Server Options dialog box opens.
2. Select the **LDAP** category.
3. Select the Active Directory server you want to enable single sign-on for and click **Edit.**

   If you need to add a new server connection, click **Add Active Directory**. See Adding Active Directory servers, page 55.

The Edit Active Directory Server dialog box opens.

4. Select a **Single Sign-On** option.
   - **Disabled** disables single sign-on for all LDAP users associated with the Active Directory server. Users must manually log in to Helix ALM products.
   - **Enabled** enables single sign-on for all LDAP users associated with the Active Directory server.
   - **Required** enables single sign-on for all LDAP users associated with the Active Directory server and restrict them from logging in using a username and password. Single sign-on is automatically enabled for all users associated with the Active Directory server.

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

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

   If you enabled single sign-on, you must also enable it for users. See Enabling single sign-on for users, page 63.

Configuring Microsoft IIS for single sign-on from Helix ALM web clients

Helix ALM applications support single sign-on for Active Directory users, which lets users use their network credentials to log in instead of entering a separate username and password.

To use single sign-on in Helix ALM Web and the license server web admin utility, the clients must be hosted by a Microsoft Internet Information Services (IIS) web server with Windows integrated authentication enabled.

Keep the following in mind:

- The Helix ALM Web and license server web admin utility components must be configured on the web server before you can enable single sign-on for them. See the Helix ALM installation help for information.
- On Mac and Linux, users are prompted to enter a username and password the first time they log in to the web client. If users save the credentials, they can use single sign-on the next time they log in.

IIS 7 and later

Enabling Windows authentication

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

Enabling authentication for web clients

1. Open IIS Manager.
2. In the Connections pane, expand the server computer and Sites nodes.
3. Expand the **Default Web Site**.

4. Select the **Scripts** folder.
5. Double-click **Authentication**.
6. Select **Anonymous Authentication** and then click **Disable** in the Actions pane.
7. Select **Windows Authentication** and then click **Enable** in the Actions pane.
8. To use single sign-on for Helix ALM Web, select the ttweb folder and repeat steps 5 -7.
9. To use single sign-on for the license server web admin utility, select the lsweb folder and repeat steps 5 - 7.
10. Restart IIS.

IIS 6

1. Open IIS Manager.
2. Expand the server computer and **Web Sites** nodes.
3. Right-click **Default Web Site** and choose **Properties**. The Properties dialog box opens.

   > **Note:** Helix ALM and license server web components are installed in the default web site by default. If the ttweb or lsweb folder is added to a different web site, right-click it instead of Default Web Site.

4. Click the **Directory Security** tab.
5. Clear the **Anonymous access** option.
6. Select **Integrated Windows authentication**.
7. Click **OK** to close the Properties dialog box.
8. Click **OK** to save the changes.
9. Restart IIS.

Enabling single sign-on for users

After you enable single sign-on for the LDAP server, you must enable it for users. Single sign-on can only be enabled for users retrieved from the LDAP database. See Adding LDAP users, page 24.

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

1. Click **Global Users**.

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

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

Disabling single sign-on for users

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

1. Click **Global Users**.

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

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

Using External Authentication

Helix ALM License Server supports integration with external authentication systems to allow users to log in to Helix ALM products using credentials from your organization's existing login methods.

Only one external authentication system can be used at a time. If external authentication is configured on the license server, single sign-on cannot be used.

> **Note:** The license server, Helix ALM, and Surround SCM only support external authentication usernames and passwords up to 128 characters. Users with usernames and passwords longer than 32 characters cannot use Surround SCM or TestTrack 2016.0 and earlier.

Perform the following tasks to integrate an external authentication system with the license server.

1. Verify the Helix ALM applications you are using support external authentication. See Products that support external authentication, page 65.
2. Create plug-ins and web server components for Helix ALM product servers and clients. See the External Authentication Integration help or contact Perforce Services for information.
3. Install the external authentication plug-ins and web components. See Installing external authentication integration components, page 66.
4. Enable external authentication on the license server. See Setting server options, page 41.
5. Enable external authentication for users. See Enabling external authentication for users, page 67.

> **Note:** The license server cannot sync users with external authentication systems.

Products that support external authentication

The following Helix ALM products support external authentication.

Helix ALM

- Helix ALM Client
- Helix ALM Web
- Outlook, Visual Studio, Surround SCM, and QA Wizard Pro Add-ins
- Server Admin Utility
- Web Server Admin Utility

> **Note:** Helix ALM electronic signatures also support external authentication.

Helix ALM License Server

- Admin Utility
- Web Admin Utility

QA Wizard Pro

- Helix ALM and Surround SCM integrations

Surround SCM

- Client
- CLI
- Helix ALM Add-in
- IDE integrations

Installing external authentication integration components

After external authentication server plug-ins or web components are created, they must be installed in Helix ALM application directories on the server computer or web server. Client plug-ins must be installed in the Helix ALM application directories on each user's computer.

Server plug-in default directories

Administrators must create a server_authentication directory in the Helix ALM License Server application directory to use external authentication and add the server plug-in to it.

Application	Platform	Default directory
Helix ALM License Server	Windows	C:\Program Files\Perforce\License Server\server_authentication
	Linux	/var/lib/spliscvr/server_authentication

Client plug-in default directories

Users who need to use external authentication to log in to the following products must create a client_ authentication directory in the application directory and add the client plug-in to it:

- Helix ALM Client
- Helix ALM License Server Admin Utility
- Surround SCM

Client	Platform	Default directory
Helix ALM	Windows	C:\Program Files\Perforce\Helix ALM\client_ authentication
	Mac	/Applications/Helix ALM/client_authentication
	Linux	/var/lib/Helix ALM/client_authentication
Helix ALM License Server Admin Utility	Windows	C:\Program Files\Perforce\License Server\client_ authentication
	Linux	/var/lib/splicsvr/client_authentication

Client	Platform	Default directory
Surround SCM	Windows	C:\Program Files\Perforce\Surround SCM\client_ authentication
	Mac	/Applications/Surround SCM/client_authentication
	Linux	/var/lib/Surround SCM/client_authentication

Web component default installations

Administrators must install web integration components in the HTML files directory on the web server for users to access the following products:

- Helix ALM License Server Web Server Admin Utility
- Helix ALM Web
- Helix ALM Web Server Admin Utility

Web client	Platform	Default directory
Helix ALM License Server Web Admin Utility	Windows	IIS—C:\InetPub\wwwroot\lsweb\admin
		Apache—C:\Program Files\Apache Software Foundation\Apache <version>\htdocs\lsweb\admin
	Linux	/var/www/html/lsweb/admin
Helix ALM Web	Windows	IIS—C:\InetPub\wwwroot\ttweb
		Apache—C:\Program Files\Apache Software Foundation\Apache <version>\htdocs\ttweb
	Linux	/var/www/html/ttweb
Helix ALM Web Server Admin Utility	Windows	IIS—C:\InetPub\wwwroot\ttweb\ttadmin
		Apache—C:\Program Files\Apache Software Foundation\Apache <version>\htdocs\ttweb\ttadmin
	Linux	/var/www/html/ttweb/ttadmin

Enabling external authentication for users

After you enable external authentication on the license server, you must enable it for users. You can allow, not allow, or require users to use it.

> **Tip:** You can enable, require, or disable external authentication for multiple users at the same time. See Replacing security field values, page 31.

1. Click **Global Users**.

   The Global Users dialog box opens.

2. Select the user you want to enable external authentication for and click **Edit.**

   The Edit User dialog box opens.
3. Click the **Security** tab.
4. Select an **Authentication** option.
   - **User cannot use external authentication** restricts users from using external authentication.
   - **User can use external authentication** allows users to use external authentication.
   - **User must use external authentication** requires users to use external authentication.
5. Click **OK** to save the changes.

> **Note:** Users must install a client plug-in for the authentication system in their Helix ALM application directories. See Installing external authentication integration components, page 66.

Managing the Server Log

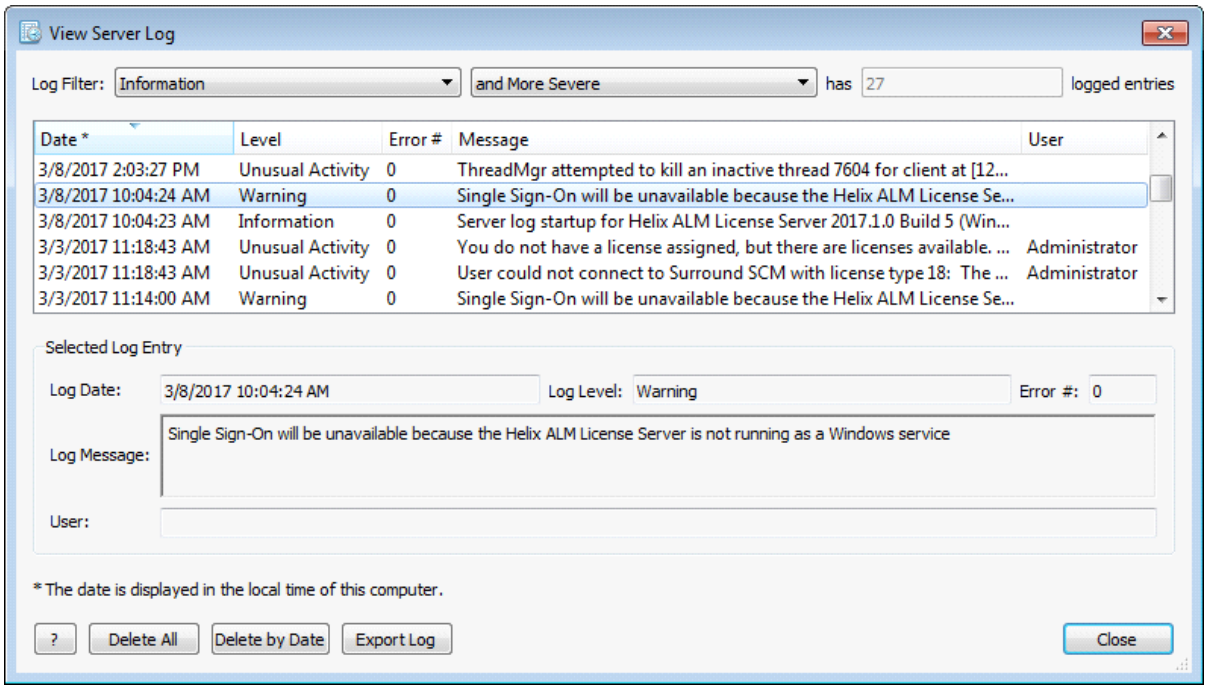
The license server log records server activity and any problems that may occur including errors, warnings, and timeout and user activity information. The amount of information in the log depends on the server options you set.

Viewing the server log

Use the server log to review server activity and troubleshoot any issues. See Troubleshooting, page 79.

1. Click **Server Log**.

   The View Server Log dialog box opens.



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

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

4. Select the entry to view.

   The details are displayed in the Selected Log Entry area.

Exporting the server log

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

1. Click **Server Log**.

   The View Server Log dialog box opens.

2. Click **Export Log**.

   The Export File dialog box opens.

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

4. Click **Save**.

   The log is exported.

Deleting all log entries

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

1. Click **Server Log**.

   The View Server Log dialog box opens.

2. Click **Delete All**.

   You are prompted to confirm the deletion.

3. Click **Yes**.

   The entries are deleted from the log.

Deleting log entries by date

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

1. Click **Server Log**.

   The View Server Log dialog box opens.

2. Click **Delete by Date**.

   The Delete Log Entries dialog box opens.

3. Enter a date in the **Date** field.

4. Click **OK**.

   All log entries, including any entries that occurred on the date you entered, are deleted.

Setting Up RDBMS Databases

The Helix ALM License Server database is stored in a Relational Database Management System (RDBMS). SQLite is the default database type and does not require any setup or configuration before or after installation.

License server 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 License Server RDBMS Support for information about supported platforms and database versions.

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

- Oracle
- PostgreSQL
- SQL Server

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 License Server tables.
- Do not directly add, edit, or delete any data in the tables.
- Do not create different primary keys. This will adversely affect application performance.
- Do not create complex triggers on any of the tables. Triggers may cause severe database issues and correcting these issues is not covered by Perforce.
- Create a process to back up database tables on a regular schedule.
- Running Oracle and the Helix ALM License 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 License Server automatically creates tables when you start the server or convert the server database. The LSServerDB.sql script file, which is located in the Oracle directory in the Helix ALM License Server application directory, is used to create the tables.

Creating Oracle users

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

Database character set

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

Sizing, memory, and tuning

Oracle sizing and tuning settings should be consistent with your corporate standards. Review the SQL scripts for schema creation installed with Helix ALM License 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 License Server tables.
- Do not directly add, edit, or delete any data in the tables.
- Do not create different primary keys. This will adversely affect application performance.
- Do not create complex triggers on any of the tables. Triggers may cause severe database issues and correcting these issues is not covered by Perforce.
- Create a process to back up database tables on a regular schedule.
- Running PostgreSQL and the Helix ALM License 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 License Server automatically creates tables in PostgreSQL when you start the server or convert the server database. The LSServerDB.sql script file, which is located in the PostgreSQL directory in the Helix ALM License Server 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 License Server tables.
- Do not directly add, edit, or delete any data in the tables.
- Do not create different primary keys. This will adversely affect application performance.
- Do not create complex triggers on any of the tables. Triggers may cause severe database issues and correcting these issues is not covered by Perforce.
- Create a process to back up database tables on a regular schedule.
- Running SQL Server and the Helix ALM License 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 License Server 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 License Server computer. See Creating DSNs for SQL Server Databases for information.

Creating server database tables

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

Troubleshooting RDBMS connections

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

> **Note:** If the Helix ALM License Server cannot connect to the server database, errors are added to the LSStartup.log file in the Helix ALM License Server 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 License Server if you drop server or tables from an RDBMS and

need to re-create them. You must also stop and restart the server if you reconfigure the destination database in the ODBC Data Source Administrator.

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

Mismatched UUID affects server database lock

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

ODBC connection issues

Try the following if you are experiencing ODBC connection problems.

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

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

2. Make sure the DSN is a system DSN.

   The data source you are trying to connect to must be configured as a system DSN in the ODBC Data Source Administrator. The Helix ALM License Server Admin Utility only displays system DSNs.

ODBC connection errors

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

SQL Server connection errors

Error	Cause
[Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user '(null)'. Reason: Not associated with a trusted SQL Server connection. QODBC3: Unable to connect	Occurs on Windows. A username is not specified for the RDBMS connection and the ODBC data source was not configured to run 'With Windows NT authentication using the network login ID' in the ODBC Data Source Administrator.
[Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user '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 Setting up Oracle databases, page 71 for information about downloading the installers.
ORA-12705: invalid or unknown NLS parameter value specified QOCI: Unable to logon	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: ■ Windows—`NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252` ■ Linux—`NLS_LANG=American_America.UTF8` You can also remove the following registry entry to help resolve the issue: `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\NLS_LANG` **Note:** Refer to Oracle Metalink article 179133.1, "The Correct NLS_LANG in a Windows Environment," for information about the correct setting, which varies based on the Windows version.
ORA-12514: TNS:listener does not currently know of service requested in connect descriptor QOCI: Unable to logon	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. 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.
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 License Server could not connect to the server or translate the host name	The Helix ALM License Server cannot connect to the PostgreSQL service. Check the following and then restart the server: ■ The PostgreSQL service is running. ■ The host name and port number are correct. ■ A firewall is not blocking the port. ■ If connecting to a remote PostgreSQL server, the server is configured to accept remote connections.

Using the License Server API

The Helix ALM License Server API provides developers with a dynamic library that can be used to create custom tools that interact with the license server. The API is available as a C library, Java library, and .NET assembly (Windows only).

The API documentation, which includes all available packages, classes, data structures, and examples, is installed with the API library files in the Helix ALM License Server application directory in the following locations:

- C API documentation—API/docs/C/index.html
- Java API documentation—API/docs/Java/index.html
- .NET API documentation—API/docs/DotNet/index.html

> **Note:** The APIs are not thread safe. Limit using the license server API to a single thread.

Troubleshooting

View the license server log for additional information when troubleshooting issues. See Viewing the server log, page 69.

> **Note:** If server issues occur, make sure the **Write all log messages to LSStartup.log** option is enabled in the server log options. This writes messages for all errors that occur after startup to the LSStartup.log file, which gives you more information to use for troubleshooting. See Setting server log options, page 39.

The Helix ALM or Surround SCM Server cannot connect to the license server

If the Helix ALM or Surround SCM Servers cannot connect to the license server, check the following and try reconnecting:

- Make sure the computer that hosts the license server is running.
- Make sure you are connected to the network, intranet, or Internet.

If the applications still cannot connect to the license server, check the following to make sure the connection is configured correctly.

1. Start the license server and the Helix ALM or Surround SCM Server.
2. Start the Helix ALM Server Admin Utility or Surround SCM and log in using your admin username and password.

   If a connection error occurs, you are prompted to use the local admin password to log in. Enter **admin** as the password. This password only provides access to the license server configuration.
3. Go to the License Server options.
   - Helix ALM Server Admin Utility—Click **Server Options** and select the **License Server** category.
   - Surround SCM—Choose **Tools > Administration > Server Options** and select the **License Server** category.
4. Make sure the server address and port number are correct and click **Test Connection**.

   If the connection is successful, stop and restart the Helix ALM or Surround SCM Server for the changes to take effect.

   If the connection is not successful, check the following:
   - If the servers are installed on different computers, check your network and firewall configurations to open the necessary ports.
   - Check the communications password set in the License Server options. It must be the same password set on the license server. To check the password in the Helix ALM License Server Admin Utility, click **Server Options**, and then select the **Server** category.

A server database or RDBMS connection error occurs

If you are experiencing problems with the license server database, see Troubleshooting RDBMS connections, page 73.

> **Tip:** You can find additional troubleshooting help in the license server knowledgebase.

Generating support diagnostic reports

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

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

   The Generate Support File dialog box opens.

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

   The Save As dialog box opens.

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

   The default file name is LicenseServerSupportDiagnostics.txt.

4. Click **Save**.

5. Click **Close** when you finish.

Appendix A: LDAP Authentication

Windows supported protocols

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

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

Unix supported protocols

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

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

LDAP technical notes

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

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

Microsoft Active Directory technical notes

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

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

Appendix B: Third-Party Software Licenses

The OpenLDAP Public License

Version 2.8, 17 August 2003

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

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

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

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

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

OpenLDAP Copyright

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

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

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

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

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

This work also contains materials derived from public sources.

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

Portions Copyright 1998-2003 Kurt D. Zeilenga.

Portions Copyright 1998-2003 Net Boolean Incorporated.

Portions Copyright 2001-2003 IBM Corporation.

All rights reserved.

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

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

Portions Copyright 1999-2003 Symas Corporation.

Portions Copyright 1998-2003 Hallvard B. Furuseth.

All rights reserved.

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

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

All rights reserved.

OpenSSL license

The following license information pertains specifically to the OpenSSL toolkit.

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

OpenSSL license

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

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

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

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

Original SSLeay license

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

All rights reserved.

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

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

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

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

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

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

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

Cyrus SASL information

CMU libsasl

Tim Martin

Rob Earhart

Rob Siemborski

Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213-3890, phone: (412) 268-4387, fax: (412) 268-7395, tech-transfer@andrew.cmu.edu.
4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

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

Index

V

W