GxP Admin Portal Software

Version 7.2

User Guide

MOLECULAR DEVICES

GxP Admin Portal Software User Guide

This document is provided to customers who have purchased Molecular Devices equipment, software, reagents, and consumables to use in the operation of such Molecular Devices equipment, software, reagents, and consumables. This document is copyright protected and any reproduction of this document, in whole or any part, is strictly prohibited, except as Molecular Devices may authorize in writing.

Software that may be described in this document is furnished under a non-transferrable license. It is against the law to copy, modify, or distribute the software on any medium, except as specifically allowed in the license agreement. Furthermore, the license agreement may prohibit the software from being disassembled, reverse engineered, or decompiled for any purpose.

Portions of this document may make reference to other manufacturers and/or their products, which may contain parts whose names are registered as trademarks and/or function as trademarks of their respective owners. Any such usage is intended only to designate those manufacturers' products as supplied by Molecular Devices for incorporation into its equipment and does not imply any right and/or license to use or permit others to use such manufacturers' and/or their product names as trademarks.

Each product is shipped with documentation stating specifications and other technical information. Molecular Devices products are warranted to meet the stated specifications. Molecular Devices makes no other warranties or representations express or implied, including but not limited to, the fitness of this product for any particular purpose and assumes no responsibility or contingent liability, including indirect or consequential damages, for any use to which the purchaser may put the equipment described herein, or for any adverse circumstances arising therefrom. The sole obligation of Molecular Devices and the customer's sole remedy are limited to repair or replacement of the product in the event that the product fails to do as warranted.

For research use only. Not for use in diagnostic procedures.

The trademarks mentioned herein are the property of Molecular Devices, LLC or their respective owners. These trademarks may not be used in any type of promotion or advertising without the prior written permission of Molecular Devices, LLC.

Patents: http://www.moleculardevices.com/patents

Contents

Chapter 1: Introduction

1

The SoftMax® Pro GxP Software Suite controls Molecular Devices® microplate readers. This document describes how to use the GxP Admin Portal Software which is the user interface for the GxP Admin Software. GxP Admin Software version 7.2 stores data documents, audit information, and all user information in a secure Microsoft SQL database. This allows for full control over file administration and permissions of who can do what to files and within the database.

SoftMax Pro Software - GxP edition extends the SoftMax Pro Software - Standard edition into regulated laboratories that work under GMP, GLP, and FDA 21 CFR Part 11 guidelines for secure electronic records. Users must log on to the SoftMax Pro Software - GxP edition with a username and password. Permissions regulate user actions and user actions trigger events that are recorded to an audit trail for electronic records.

See the following for additional information:

- *SoftMax Pro Data Acquisition and Analysis Software - GxP Edition - Installation Guide for the Multi Computer Setup*
- *SoftMax Pro Data Acquisition and Analysis Software - GxP Edition - Installation Guide for the Single Computer Setup*
- *SoftMax Pro Data Acquisition and Analysis Software User Guide*
- Application Help

Primary Data Integrity

The integrity of raw data is a primary design consideration of SoftMax Pro GxP Software Suite. Data that the software acquires is time stamped and traceable to the user who initiates data acquisition. The software saves data in a Microsoft SQL database that cannot be manipulated. The System Audit Trail allows you to monitor over 140 events that include, but are not limited to, changes to documents, instrument settings, reduction settings, notes, electronic statements, logins and failed logins, user activities, and file creation, modification, and deletion. See Audit Events on page 65.

Documents that the SoftMax Pro Software - GxP edition create are strictly bound to features that support FDA 21 CFR Part 11. As a result, these documents cannot be opened or modified in the SoftMax Pro Software - Standard edition to ensure the integrity of the FDA 21 CFR Part 11 compliant data.

> **Note:** No software by itself can be FDA 21 CFR Part 11 Compliant. Use the SoftMax Pro GxP Software Suite features to demonstrate compliance with these regulations.

Administratively Controlled Access

SoftMax Pro GxP Software Suite has three software applications:

- **SoftMax Pro GxP Software**: The SoftMax Pro GxP Software (client) controls the microplate reader for data acquisition and statistical data analysis.
- **GxP Admin Portal Software**: The GxP Admin Portal Software is the user interface that you use to interact with the GxP Admin Software.
- **GxP Admin Software**: The GxP Admin Software (server) has no user interface and is the database and security back-end application.

Use the GxP Admin Portal Software to create users. You grant users Access permissions to allow use of the GxP Admin Portal Software and/or the SoftMax Pro GxP Software. You assign users with the SoftMax Pro Access permission to Projects that limit their access to documents. For each Project, you assign users to a Role that allows users to perform the tasks for which the users are responsible.

Application Access Permissions

Use the three Access permissions to restrict each user's access to the software applications.

- **GxP Admin** - Users with this Access permission have access to all GxP Admin Portal Software functionality. GxP Admin Access permission allows management of the users of the GxP Admin Portal Software and the users of the SoftMax Pro GxP Software including workflow permissions and password resets. GxP Admin users manage application setting such as password strength requirements and event notifications. Users with this Access permission have the System Audit Trail Access permission by default and can view the System Audit Trail in the GxP Admin Portal Software. These users cannot log on to the SoftMax Pro GxP Software unless you also grant them the SoftMax Pro Access permission.
- **System Audit Trail** - Users with this Access permission can view the System Audit Trail in the GxP Admin Portal Software. These users can confirm that the GxP Admin Software meets compliance requirements but cannot change user settings, cannot change application settings, and cannot log on to the SoftMax Pro GxP Software unless you also grant them the GxP Admin Access permission and/or the SoftMax Pro Access permission.
- **SoftMax Pro** - Users with this Access permission also require a user license to log on to the SoftMax Pro GxP Software. These users are granted permission to access the SoftMax Pro GxP Software based upon their assignment to Projects and their Role in each Project. These users cannot log in to the GxP Admin Portal Software unless you also grant them the System Audit Trail Access permission and/or the GxP Admin Access permission.

Projects - Document Access Restrictions

Each user with the SoftMax Pro Access permission must be a member of at least one Project. Projects limit which documents the user can access. Each user can be a member of multiple Projects.

Roles - Workflow Permissions

Each user with the SoftMax Pro Access permission can have one Role in each Project. Each user can be a member of multiple Projects and can have a different Role in each Project. Roles restrict the user's responsibilities in the SoftMax Pro GxP Software.

Document Workflow

The document life cycle in a compliant lab consists of multiple different development and review steps and requires a system to indicate the document state. The status system allows a Project team to track and approve documents while the document moves through the pipeline of development, review, release, and usage in a controlled environment.

There are two types of documents:

- Protocols contain instrument settings, notes, statements, group settings, graph settings, and so on. Protocols do not contain data.
- Data documents contain everything from the protocol plus the data that the instrument collects and the results of the formula calculations you set up in the protocol.

Document Statuses

The SoftMax Pro GxP Software Suite installation includes three default Roles: Scientist, Lab Technician, and Lab Manager. The default permissions for these Roles correspond to the document statuses that are present in the SoftMax Pro GxP Software. You can modify the default Role permissions, if needed.

- In Work
- Review Pending
- Reviewed
- Released
- In Progress
- Approval Pending
- Approved
- Outdated
- Canceled

The following document workflow corresponds to the default Roles. Your laboratory can define Roles and document workflows that meet your needs.
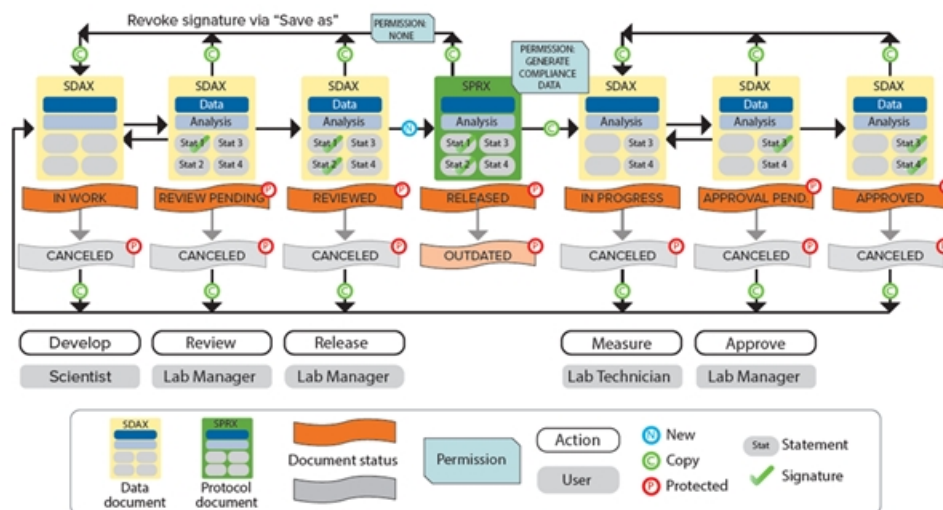
In Work Document Status - Scientist Role

Scientists open and save new data documents that contain the instrument settings in Plate sections and define data analysis settings. The software assigns a new document the status In Work. Scientists add statements to the documents to provide communication to the other users responsible for the document. Scientists sign the first statement to prevent further edits and set the document status to Review Pending.

Review Pending Document Status - Lab Manager Role

Lab managers review the data documents with the status Review Pending, sign the second statement, and set the document status to Reviewed.

Reviewed Document Status - Release Protocol - Lab Manager Role

If the data document with the status Reviewed is correct, the lab managers then release the document as a protocol. The software saves the protocols with the status Released for reuse.

If a document has a newer iteration or is incorrect, the lab managers can set documents that have the status Released to the Outdated status.

In Progress Document Status - Lab Technician Role

Lab technicians open protocols with the Released status and the software prompts the lab technicians to save the protocols as data documents before the lab technicians can run the experiments. Because the Lab Technician Role has the Generate Compliance Data permission, the software sets the data document status to In Progress and removes the two signed statements. This allows lab technicians to run experiments and generate the compliance data.

When lab technicians finish their work, they sign a statement to prevent further changes and set the document status to Approval Pending.

Approval Pending Document Status - Lab Manager Role

Lab managers confirm that documents with the Approval Pending status meet regulatory requirements, sign a statement, and set the document status to Approved. If the lab manager determines the document is incorrect, they can set an Approved document back to the In Progress status.

Canceled Document Status

Users with appropriate permissions can set the document status to Canceled at the applicable points in the document workflow.

Audit Trail

The GxP Admin Software and the SoftMax Pro GxP Software generate audit trails that record the events that user actions trigger. For each event instance, the audit trail records the date and time, the username of the person who was logged on, and the event action. Users cannot alter the audit trail, nor can they edit or delete audit trail entries.

GxP Admin Software Events

The GxP Admin Software saves the audit trail to the database and you view the System Audit Trail in the GxP Admin Portal Software.

For a list of the events that trigger a System Audit Trail entry, see .

SoftMax Pro GxP Software Events

In addition to the GxP Admin Software System Audit Trail, the SoftMax Pro GxP Software records document-specific events to an audit trail for the document. You view the document-specific audit trail in the .

The document audit trail records events that pertain to the document that is active in the Workspace and saves the document-specific events with the document. Additionally, the document audit trail includes general activities such as log in and log out when a document is open during those events.

The audit trail for each Plate section in a document includes the following information:

- The name of the user who logged in when the read began.
- The instrument type used to do the read and the instrument ROM version number. For the SpectraMax® i3x Multi-Mode Detection Platform and the SpectraMax® Paradigm® Multi-Mode Microplate Reader, the audit trail also includes the serial number of the detection cartridge.

Password Management

During installation, you create the password for the first user that you will use to login to the software. This user has the GxP Admin Access permission and the System Audit Trail Access permission.

The multi computer setup supports the creation of both Custom Credentials users and the integration with Windows Credentials, Active Directory (LDAP) users.

- **Custom Credentials**: For users you create with the Custom Credentials login mode, the software creates a randomly generated alphanumeric string of characters to be their password. This password grants users with the appropriate Access permissions access to the GxP Admin Portal Software and the SoftMax Pro GxP Software. Both software applications require Custom Credentials login mode users to change their password upon initial login. Both software applications enable Custom Credentials login mode users to change their password as often as they want. The GxP Admin Portal Software has settings to manage password strength and password aging to require Custom Credentials login mode users to change their password at the interval you specify.
- **Windows Credentials**: For users you create with the Windows Credentials login mode, password management is maintained through the Active Directory. Windows Credentials login mode users cannot change their password in the GxP Admin Portal Software or the SoftMax Pro GxP Software. The password maintenance settings in the GxP Admin Portal Software do not affect Windows Credentials login mode users. Windows Credential login mode users with the SoftMax Pro Access permission must have a license and must be a member of at least one Project. Their activity within the SoftMax Pro GxP Software is restricted by their Role permissions. Windows Credentials login mode is available when you use the multi computer setup.

Chapter 2: Software Installation Introduction

2

The SoftMax Pro GxP Software Suite scales with the size of your laboratory environment. Depending on the size of your implementation, you can install the interdependent SoftMax Pro GxP Software Suite components on multiple networked computers. For the smallest of implementations, it is possible to install the components on a single computer. You should consult with your Molecular Devices representative and your network administrators to plan and scale your implementation according to your requirements.

SoftMax Pro GxP Software Suite components:

- **SoftMax Pro GxP Software**: The SoftMax Pro GxP Software (client) controls the microplate reader for data acquisition and statistical data analysis. These computers must have access to the dedicated server on which you install the GxP Admin Software.
- **GxP Admin Portal Software**: The GxP Admin Portal Software is the user interface that you use to interact with the GxP Admin Software. These computers must have access to the dedicated server on which you install the GxP Admin Software.
- **GxP Admin Software**: The GxP Admin Software (server) is the database and security back-end application that you install on a dedicated, centrally located server with a static IP address. This server must be accessible to all computers that run the GxP Admin Portal Software and the SoftMax Pro GxP Software.

See the following documents for installation instructions:

- *SoftMax Pro Data Acquisition and Analysis Software - GxP Edition - Installation Guide for the Multi Computer Setup*
- *SoftMax Pro Data Acquisition and Analysis Software - GxP Edition - Installation Guide for the Single Computer Setup*

Chapter 3: Getting Started

3

On the computer desktop, double-click [icon] to display either the GxP Server Hostname page or the GxP Admin Portal Software Login page.

Logging In To The GxP Admin Portal

The first time you start the GxP Admin Portal Software, the GxP Server Hostname dialog displays so you can connect the GxP Admin Portal Software to the GxP Admin Software. After the first time, users with the GxP Admin Access permission and/or the System Audit Trail Access permission use the Login page to access the GxP Admin Portal Software.
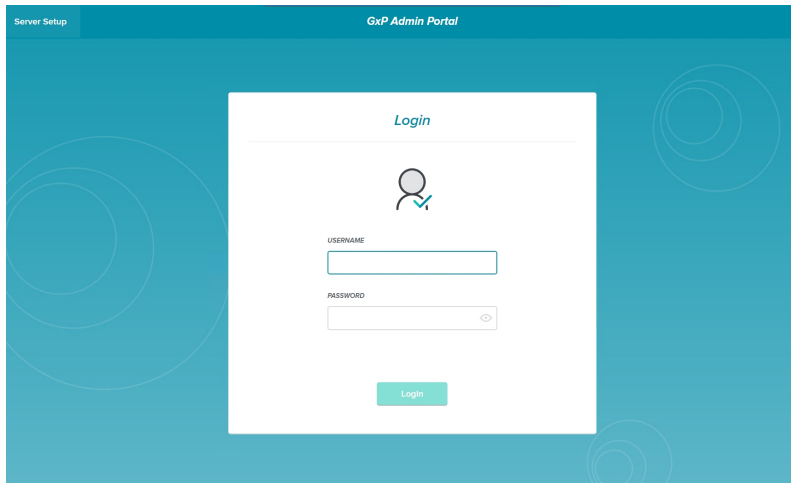
Connecting the GxP Admin Portal Software to the GxP Admin Software

The first time you use the GxP Admin Portal Software you need to connect the GxP Admin Portal Software to the GxP Admin Software. You do this one time for each computer that runs the GxP Admin Portal Software.

To connect the GxP Admin Portal Software to the GxP Admin Software:

1. If the GxP Server Hostname page does not display the first time you start the software or if the connection between the GxP Admin Portal Software and the GxP Admin Software is disrupted, on the top left of the Login page, click **Server Setup** to display the GxP Server Hostname page.
2. On the GxP Server Hostname page:
   - For the multi computer setup, in the **Server Hostname** field, enter either the hostname or IP address of the computer on which you install the GxP Admin Software and in the **Port** field, enter the port number to use for communication between the computers.

     > [icon] **Note:** The GxP Admin Software computer is NOT the external Microsoft SQL database server if you configure the GxP Admin Software to use an external Microsoft SQL database.

   - For the single computer setup, in the **Server Hostname** field, enter **localhost** and in the **Port** field, enter **8210**.
3. Click **Continue** to return to the Login page.

Logging In For The First Time

During software installation, you create the password for the first user that you use to login to the software. This user has the username *gxpadmin* and after you successfully enter the username and password in the Login page, the software forces you to change this user's password.

> **Note:** You get five attempts to log in for the first time. If you forgot the password you entered during installation, you need to reinstall the software.

The software assigns all users with the Custom Credentials login mode a randomly generated alphanumeric string as their initial password. The software prompts users with the Custom Credentials login mode to change their password upon initial login. Default password strength settings require you to create a password that contains at least ten characters, both uppercase and lowercase letters, at least one digit, and at least one special character. You can change the default password strength settings on the Maintenance page. See Maintenance Settings on page 44.

Users you create with the Windows Credentials login mode use the password associated with their Active Directory user account. Windows Credentials login mode users cannot change their password in the GxP Admin Portal Software and the software does not prompt these users to change their passwords upon initial login. Windows Credentials login mode user passwords are managed via your company's Active Directory and the password management settings in the GxP Admin Portal Software are ignored.

To login for the first time:

1. In the **Username** field, enter your username. Default first username is *gxpadmin*.
2. In the **Password** field, enter your password. For the *gxpadmin* user, you created this password during installation.
3. Click **Login**.
   For Windows Credentials login mode users, the Home page displays.
   For Custom Credentials login mode users, the Set New Password dialog displays.
4. For Custom Credentials login mode users, in the **New Password** field, enter the new password with at least ten characters, both uppercase and lowercase letters, at least one digit, and at least one special character.
5. In the **Repeat New Password** field, reenter the password.
6. Click **Change** to display the Home page. See Home on page 17.

Home - First Steps

When you login to the GxP Admin Portal Software for the first time, the Home page displays a list of tasks you should do as the first steps.
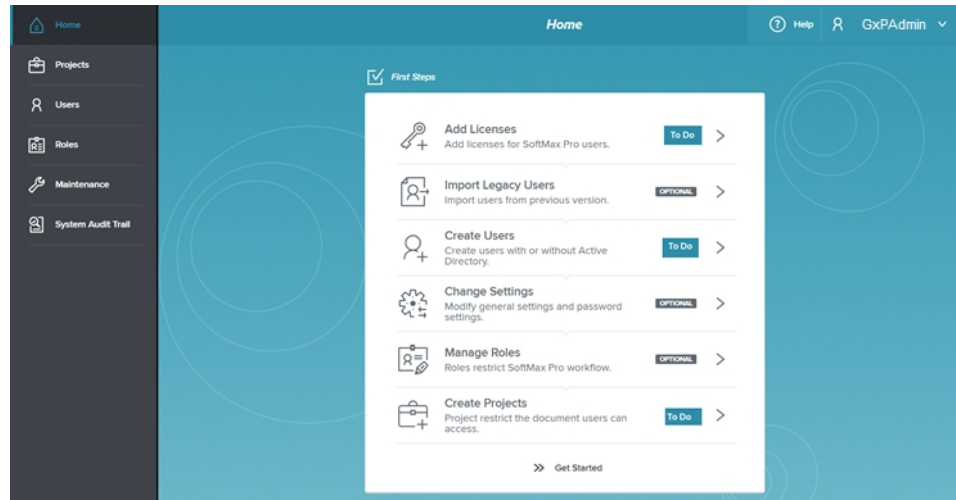
The general sequence of steps to get started follows the sequence of the items in the First Steps list.

- **Add Licenses:** Click to activate the user licenses that each user with the SoftMax Pro Access permission requires to login to the SoftMax Pro GxP Software. See Maintenance Licenses on page 46.
- **Import Legacy Users**: If you use GxP Admin Software version 2.x, use the GxP Admin EDB Converter Tool to convert the version 2.x .edb user files to version 7.2 .edbexp files and then click this to import the converted user files into GxP Admin Software database. See Maintenance User Import on page 50.
- **Create Users**: Click to create the users for both the GxP Admin Portal Software and the SoftMax Pro GxP Software. See Users on page 23.
- **Change Settings**: Click to define settings for password strength and administrator contact information. See Maintenance Settings on page 44.
- **Manage Roles**: Click to manage the Roles that restrict the actions users with the SoftMax Pro Access permission can do in the SoftMax Pro GxP Software. See Roles on page 29.
- **Create Projects**: Click to manage the Projects that restrict the documents users with the SoftMax Pro Access permission can access in the SoftMax Pro GxP Software. See Projects on page 35.

To permanently remove the First Steps check list, click **>> Get Started**.

> **Note:** After you click Get Started you cannot display the First Steps check list again.

Chapter 4: Home

4

The Home page displays when you login and provides shortcuts to most workflows along with other useful information. The top right of most pages displays the Help icon and the name of the user that logged in. The left side of most pages displays the navigation icons with a black background.
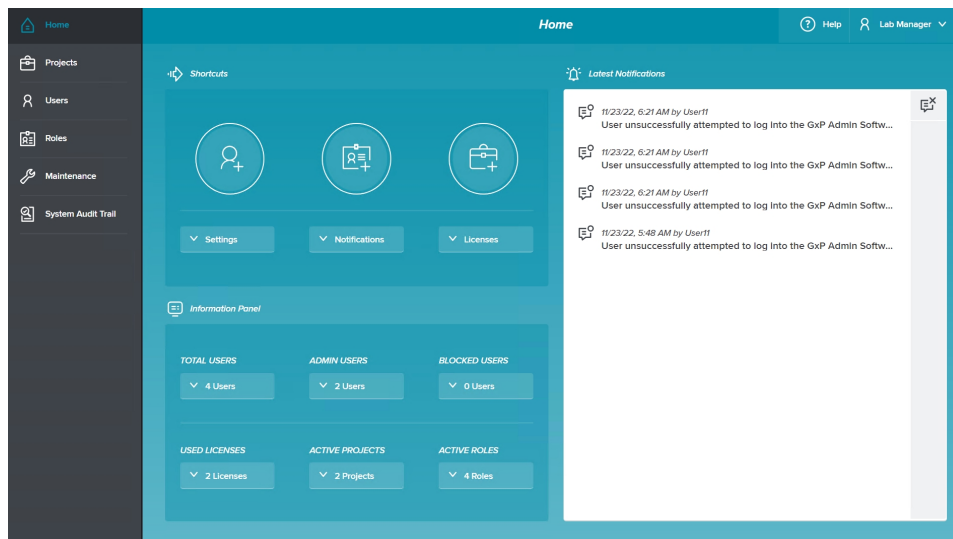
User Actions

On the top right, click ∨ next to your username:

- Select **Change Date/Time Format** to display the Change Date/Time Format dialog where you can change the format of the date and time display. The database uses the UTC time zone. See Change Date/Time Format on page 21.
- Select **Change Password** to display the Change Password dialog. This option is available for users with the Custom Credentials login mode. See Change Password on page 20.
- Select **Logout** to log out of the GxP Admin Portal Software.

Navigation Icons

On the left, the navigation icons display with a black background and provide access to the following workflows.

- Click **Home** to return to the Home page when you navigate away from the Home page.
- Click **Projects** to display the Project Administration page to manage Projects. Each user with the SoftMax Pro Access permission must be a member of at least one Project. After you add users with the SoftMax Pro Access permission and you define Roles, you assign each user to a Project with a Role. A user can have one Role in each Project and can be a member of multiple Projects. You can assign a user to a different Role in each Project. See Projects on page 35.
- Click **Users** to display the User Administration page to manage users. You grant each user Access permissions. The GxP Admin Access permission grants access to the GxP Admin Portal Software as an administrator. The System Audit Trail Access permission grants access to the GxP Admin Portal Software to view the System Audit Trail. The SoftMax Pro Access permission grants access to the SoftMax Pro GxP Software. See Users on page 23.

- Click **Roles** to display the Role Administration page to manage Roles. Use Roles to restrict the responsibilities of the users within the SoftMax Pro GxP Software. Each user with the SoftMax Pro Access permission can be a member of multiple Projects. A user can have one Role in each Project which allows you to assign the same user a different Role with a unique set of permissions in each different Project. See Roles on page 29.
- Click **Maintenance** to display the Maintenance page. The Maintenance page has four tabs.
  - **Settings**: Use to define auto lock settings, password strength settings, and the administrator contact information. See Maintenance Settings on page 44.
  - **Notifications**: Use to select which events should trigger the notifications that display on the Home page. All events are recorded to the System Audit Trail. See Maintenance Notifications on page 45.
  - **Licenses**: Use manage the licenses you assign to users with the SoftMax Pro Access permission. See Maintenance Licenses on page 46.
  - **User Import**: Use to import users from the GxP Admin Software version 2.x into the SoftMax Pro GxP Software Suite version 7.2 database. See Maintenance User Import on page 50.
- Click **System Audit Trail** to display the System Audit Trail page. Use the System Audit Trail to view a list of the events that user actions trigger. When a user has the System Audit Trail Access permission, they can see only the System Audit Trail page. Users with the GxP Admin Access permission automatically receive the System Audit Trail Access permission. See System Audit Trail on page 53.

After you complete the First Steps check list and click Get Started, the Home page displays shortcuts, notifications, and additional information.

Shortcuts

The upper left side of the Home page provides shortcuts to:

- New Users on page 24
- New Roles on page 30
- New Projects on page 36
- Maintenance Settings on page 44
- Maintenance Notifications on page 45
- Maintenance Licenses on page 46

Information Panel

The lower left side of the Home page displays statistics. Each statistic is a link to the workflow where you act on the information.

- Click **Total Users** to display the User Administration page with no filters applied. See Users on page 23.
- Click **Admin Users** to display the User Administration page with filters to display only users with the GxP Admin Access permission.
- Click **Blocked Users** to display the User Administration page with filters to display only users whose software access has been blocked due to too many false login attempts.
- Click **Used Licenses** to display the Maintenance page with the Licenses tab selected where you manage the licenses you assign to users with the SoftMax Pro Access permission. See Maintenance Licenses on page 46.
- Click **Active Projects** to display the Project Administration page with filters to display only active Projects. See Projects on page 35.
- Click **Active Roles** to display the Role Administration page with filters to display only active Roles. See Roles on page 29.

Latest Notifications

The right side of the Home page displays notifications for the events you choose to display. These notifications are similar to your smart phone notifications. When a user triggers an event, the software includes the details in the System Audit Trail.

Use the Notifications tab on the Maintenance page to select which events display as a notification on the Home page. See Maintenance Notifications on page 45.

Note: You cannot change the audit trail. The software permanently records all events in the System Audit Trail even if they do not display as a notification on the Home page.

On the Home page:

- Click on a notification to go to the System Audit Trail page to view additional details.
- Click ![icon] next to a notification to dismiss the notification from the Home page display.
- Click ![icon] on the right to dismiss all notifications from the Home page display.

Change Password

Users with the Custom Credentials login mode use the Change Password dialog to change their password.

> **Note:** Users with the Windows Credentials login mode use the password that is managed via the Windows Active Directory and cannot change their password in the GxP Admin Portal Software.

Change Password

OLD PASSWORD

NEW PASSWORD

REPEAT NEW PASSWORD

ⓘ *Please enter your existing password before setting a new one.*

Cancel   Change

To change your password:

1. On the top right, click ⌄ next to your username and select **Change Password** to display the Change Password dialog.
2. In the **Old Password** field, enter your current password.
3. In the **New Password** field, enter your new password.
4. In the **Repeat New Password** field, enter your new password a second time to confirm that you enter the password correctly.
5. Click **Change**.

Change Date/Time Format

Use the Change Date/Time Format dialog to define how you want to display the date and time. The database uses the UTC time zone. Your date/time format settings affect the display of the dates on the System Audit Trail page.
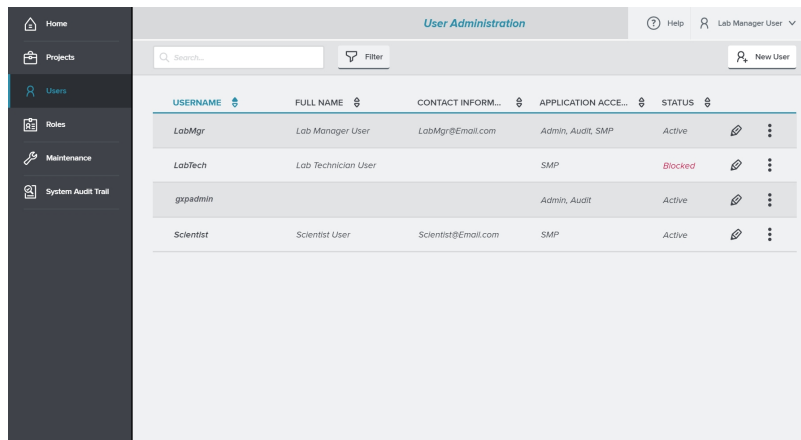
The Preview area at the bottom of the dialog displays the result of each of the following selections.

To change the date and time format:

1. On the top right, click ⌄ next to your username and select **Change Date/Time Format** to display the Change Date/Time Format dialog.
2. Click the **Region** drop-down and select a regional date/time format.
3. Click the **Format** drop-down:
   - Select **Short** to display the date and time in the regional format you select.
   - Select **Short + GMT** to display the date and time in the regional format you select plus the offset to the Greenwich Mean Time.
4. Click the **UTC Time** [OFF] to display [ON] to have the time display in the regional format you select using the Greenwich Mean Time zone.
5. Click **Apply**.

5

The User Administration page displays the list of users and allows you to manage users.

To manage users:

1. Click **Users** on the left to display the User Administration page.
2. Click **New User** to display the New User page. See New Users on page 24.
3. Next to a user, click ⬚ to display the Edit User page. See Edit Users on page 27.
4. Next to a user, click ⋮ :
   - Select **Reset Password** to reset the user's password. This displays for users with the Custom Credentials login mode. See below.
   - Select **Deactivate User** to make an active user inactive or select **Activate User** to make an inactive user active.

     > **Note:** When you deactivate a user, the software removes all Access permissions and releases the license from a user that had the SoftMax Pro Access permission. You cannot re-activate the user for 30 days.

   - Select **User Information** to display user information. See User Information on page 28.

Reset Password

When a user with the Custom Credentials login mode forgets their password, the Reset Password option generates a new alphanumeric string password for the user. The software requires the user to change the system generated password the first time they login.

To reset passwords:

1. On the User Administration page, next to a user, click ⋮ and select **Reset Password**.
2. A message displays to confirm your request. You cannot undo this. Click **OK**.

3. The User Information dialog displays.

- Click to copy the user information including the new password to the computer clipboard. Then paste the user information into an email or into a text editor software file and save the file in a location that the user can access.

- Click to print the new user information including the new system generated password.

New Users

Use the New User page to add users.

Select the Login Mode

The first time you click New User, the New User page allows you to select the user's login mode. The next time you click New User, the New User page displays the settings for the login mode you selected for the previous user you added and contains a Change Login Mode button that you use to add a user with the alternate login mode.
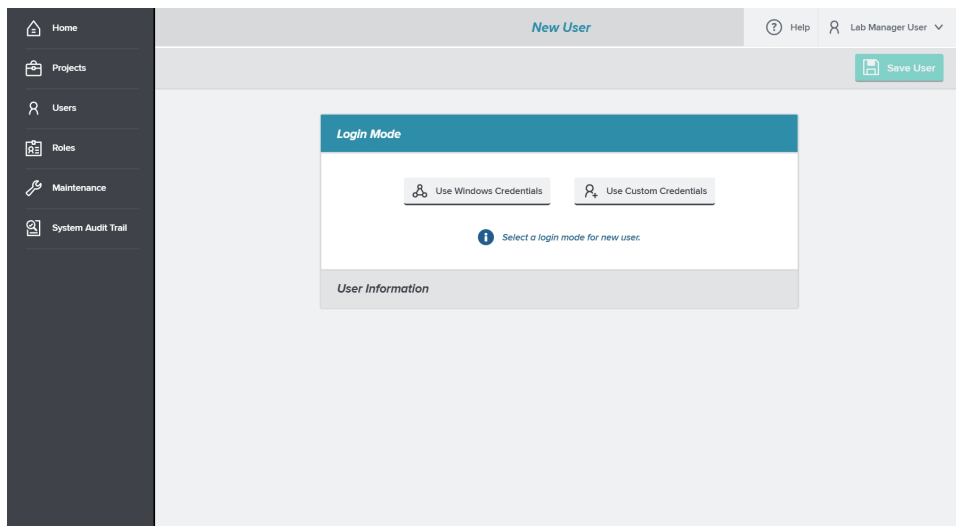
To select a login mode:

1. Click **Users** on the left to display the User Administration page.
2. Click **New User** to display the New User page.
   - Click **Use Windows Credentials** to display fields that you use to add a user account that uses your company's Active Directory database for "single sign on" and password management.

     > **Note:** Windows Credentials login mode is available for the multi computer setup only.

   - Click **Use Custom Credentials** to display fields that you use to add a user account that uses the username and password restrictions you define from the GxP Admin Portal Software.

Windows Credentials Login Mode Users

Windows Credentials login mode users use the username and password settings from your company's Windows Active Directory database.

> **Note:** You must install the SoftMax Pro GxP Software Suite using the multi computer setup to use the Windows Credentials login mode. The computer running the GxP Admin Software must have access to the computer that contains your company's Active Directory database.

To add users with the Windows Credentials login mode:

1. Click **Users** on the left to display the Users page.
2. Click **New User** to display the New User page.
3. Click **Use Windows Credentials** to display fields that you use to add a user with the Windows Credentials login mode, if needed.

> **Note:** If you previously added Custom Credential users, click **Change Login Mode** and then click **Use Windows Credentials**.

4. In the **Username** field, enter the user's Windows Active Directory username.
5. Click **Verify** to link the user's Active Directory account to the GxP Admin Software. The Username field becomes inactive and you cannot edit the Username field.
6. The **Full Name** field can display the user's full name from Active Directory or you can enter the full name.
7. The **Contact Information** field can display the user's contact information from Active Directory or you can enter the user's contact information. (optional)
8. Select **Application Access** options.
   - Select the **GxP Admin** check box to grant the user Access to the GxP Admin Portal Software with permission to maintain user information, password strength settings, and Access to the System Audit Trail.
   - Select the **System Audit Trail** check box to grant the user Access to the GxP Admin Portal Software with permission to view the System Audit Trail.
9. Click the **SoftMax Pro Access** - **No Access** ⌄ and select a license to grant the user access to the SoftMax Pro GxP Software. Each user with the SoftMax Pro Access permission requires a license and must be a member of a Project. See Maintenance Licenses on page 46 and Projects on page 35.
10. Click **Save User**.

Custom Credentials Login Mode Users

Custom Credentials login mode users use the username and password settings you define from the GxP Admin Portal Software.

To add users with the Custom Credentials login mode:

1. Click **Users** on the left to display the Users page.
2. Click **New User** to display the New User page.
3. Click **Use Custom Credentials** to display fields that you use to add a user with the Custom Credentials login mode, if needed.

> **Note:** If you previously added Windows Credential users, click **Change Login Mode** and then click **Use Custom Credentials**.

4. In the **Username** field, enter the username.
5. In the **Full Name** field, enter the full name.
6. In the **Contact Information** field, enter the user's contact information. (optional)
7. Select **Application Access** options.
   - Select the **GxP Admin** check box to grant the user Access to the GxP Admin Portal Software with permission to maintain user information, password strength settings, and Access to the System Audit Trail.
   - Select the **System Audit Trail** check box to grant the user Access to the GxP Admin Portal Software with permission to view the System Audit Trail.
8. Click the **SoftMax Pro Access** - **No Access** ⌄ and select a license to grant the user access to the SoftMax Pro GxP Software. Each user with the SoftMax Pro Access permission requires a license and must be a member of a Project.
9. Click **Save User**.
10. The User Information dialog displays. See User Information on page 28.
    - Click 🗗 to copy the user information including the new password to the computer clipboard. Then paste the user information into an email or into a text editor software file and save the file in a location that the user can access.
    - Click 🖨 to print the new user information including the new system generated password.

Edit Users

Use the Edit User page to edit users.

To edit users:

1. Click **Users** on the left to display the User Administration page.

2. Next to a user, click ✎ to display the Edit User page.

3. To change a Custom Credentials login mode user to a Windows Credentials login mode user or to change a Windows Credentials login mode user to a Custom Credentials login mode user, click **Change Login Mode** and then click either **Use Windows Credentials** or click **Use Custom Credentials**.

4. In the **Username** field, enter the username. You cannot change the username for a Windows Credentials login mode user.

5. In the **Full Name** field, enter the full name.

6. In the **Contact Information** field enter the user's contact information.

7. Select **Application Access** options.
   - Select the **GxP Admin** check box to grant the user Access to the GxP Admin Portal Software with permission to maintain user information, password strength settings, and Access to the System Audit Trail.
   - Select the **System Audit Trail** check box to grant the user Access to the GxP Admin Portal Software with permission to view the System Audit Trail.

8. Click the **SoftMax Pro Access - No Access** ⌄ and select a license to grant the user access to the SoftMax Pro GxP Software. Each user with the SoftMax Pro Access permission requires a license and must be a member of a Project. See Maintenance Licenses on page 46 and Projects on page 35.

9. Click **Save User**.

User Information

The User Information dialog displays user information.
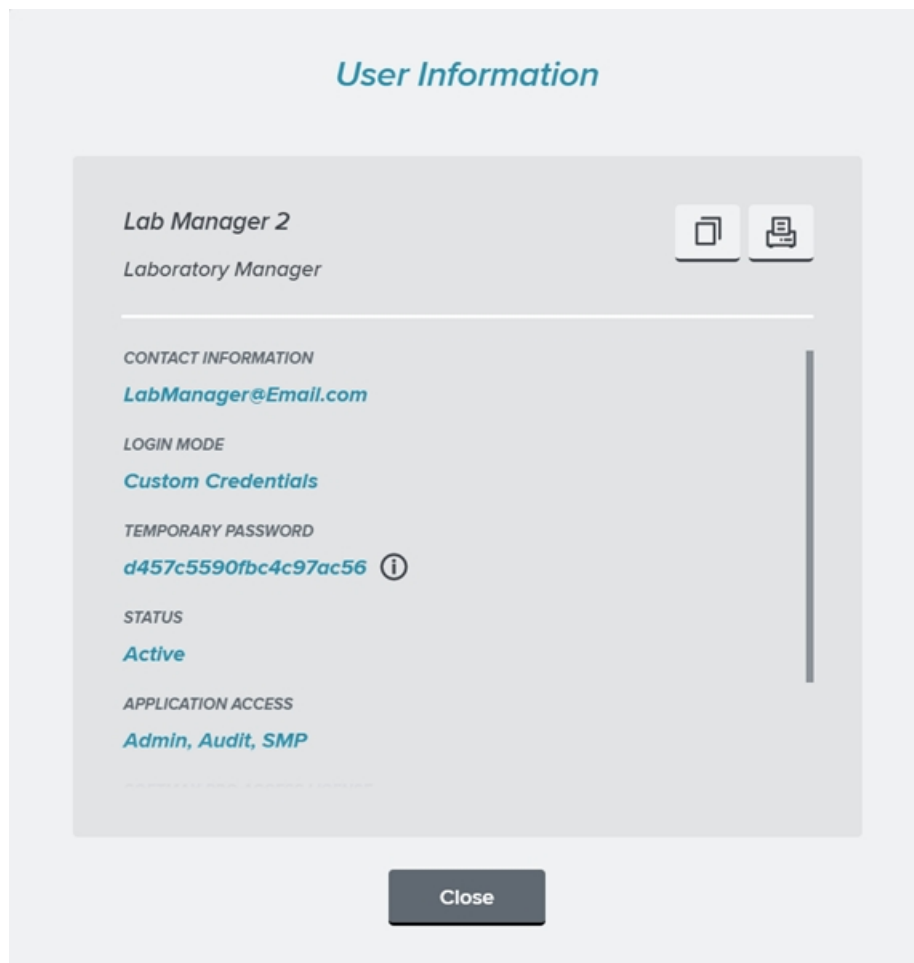
To view user information:

1. Click **Users** on the left to display the User Administration page.

2. Next to a user, click ⋮ and select **User Information** to display the User Information dialog.

3. Click ⧉ to copy the user information to the computer clipboard from where you can paste the information into an email or text file.

4. Click 🖨 to print the user information.

Chapter 6: Roles

6

The Role Administration page displays the list of Roles and allows you to manage Roles. Use Roles to define the list of permissions that grant a user access to the workflows in the SoftMax Pro GxP Software. You assign a Role to a user when you manage Projects from the Project Administration page. See Projects on page 35.

Each user with the SoftMax Pro Access permission can be a member of multiple Projects. The user has one Role in each Project. This allows you to assign the same user a different Role with a unique set of permissions in each Project.

The software installation includes three default Roles. You can edit the default Roles or copy the default Roles to create your own similar Roles. See Default Roles on page 61.

	Role Administration					
ROLE NAME	DESCRIPTION	PERMISSIONS	PROJECTS	STATUS		
Lab Manager	Standard Workflow	26	0	Active		
Lab Technician	Standard Workflow	12	0	Active		
Scientist	Standard Workflow	42	0	Active		

To manage Roles:

1. Click **Roles** on the left to display the Role Administration page.
2. Click **New Role** to add a new Role. See New Roles on page 30.
3. Next to a Role, click ![edit icon] to display the Edit Role page. See Edit Roles on page 30.
4. Next to a Role, click ![menu icon] :
   - Select **Copy Role** to display the Copy Role page. See Copy Roles on page 31.
   - Select **Deactivate Role** to make an active Role inactive or **Activate Role** to make an inactive Role active.
   - Select **Assigned Permissions** to display the Assigned Permission dialog that displays the permission that are granted to users with the Role. See Assigned Permissions on page 31.
   - Select **Assigned Projects** to display the Assigned Projects dialog that displays the list of Projects that include users with the Role. See Project Information on page 41.
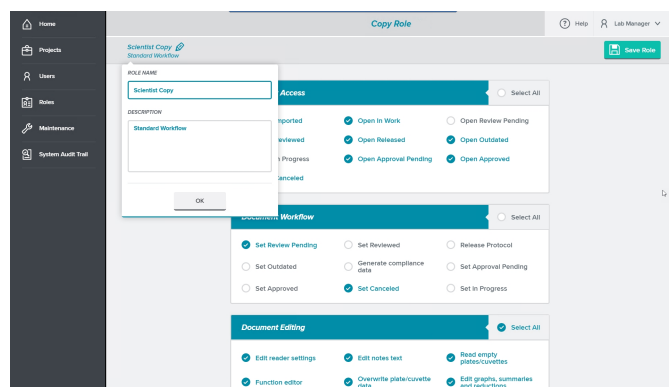
New Roles

Use the New Role page to add Roles.
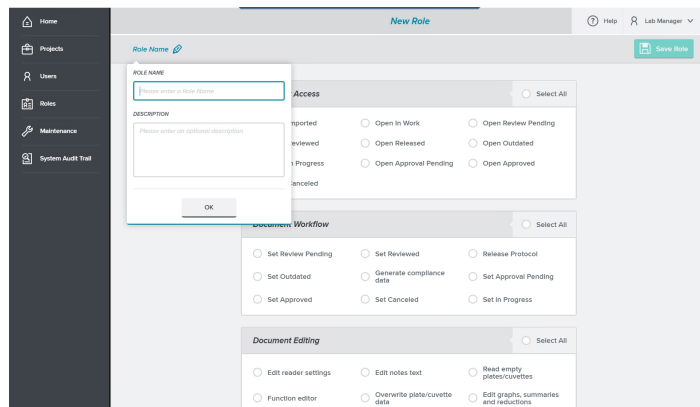
To add Roles:

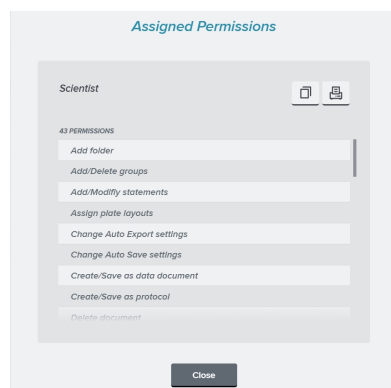1. Click **Roles** on the left to display the Role Administration page.
2. Click **New Role** to display the New Role page.
3. In the **Role Name** field, enter the Role name.
4. In the **Description** field, enter the Role description and click **OK**.
5. Select the check box for each permission to grant to the users you assign to the Role. See Role Permissions on page 33.
6. Click **Save Role**.

Edit Roles

Use the Edit Role page to edit Roles.
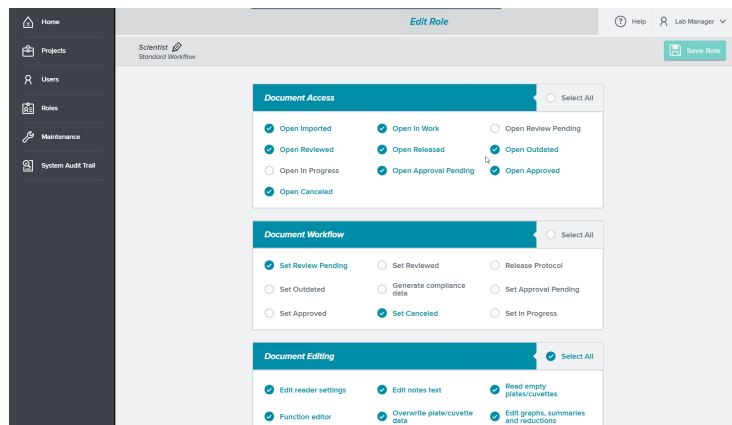
To edit Roles:

1. Click **Roles** on the left to display the Role Administration page.
2. Next to a Role, click [icon] to display the Edit Role page.
3. On the top left, click [icon] to edit the **Role Name** and **Description**.
4. Select the check box for each permission to grant to the users you assign to the Role. See Role Permissions on page 33.
5. Click **Save Role**.

Copy Roles

Use the Copy Role page to create a copy of a Role to expedite the creation of similar Roles.

To copy Roles:

1. Click **Roles** on the left to display the Role Administration page.
2. Next to a Role, click ⋮ and select **Copy Role** to display the Copy Role page.
3. In the **Role Name** field, enter the Role name.
4. In the **Description** field, enter the Role description and click **OK**.
5. Select the check box for each permission to grant to the users you assign to the Role. See Role Permissions on page 33.
6. Click **Save Role**.

Assigned Permissions

The Assigned Permissions dialog displays the permissions you assign to a Role.

To view assigned permissions:

1. Click **Roles** on the left to display the Role Administration page.
2. Next to a Role, click ⋮ and select **Assigned Permissions** to display the Assigned Permissions dialog.
3. Click to copy the permissions to the computer clipboard from where you can paste the information into an email or text file.
4. Click to print the permissions.

Assigned Projects

The Assigned Projects dialog displays the list of Projects that use the Role and the number of users in the Role for each Project.
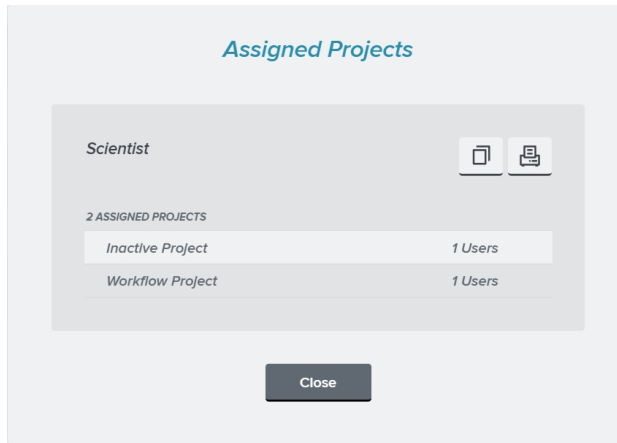
To view assigned Projects:

1. Click **Roles** on the left to display the Role Administration page.

2. Next to a Role, click ⋮ and select **Assigned Projects** to display the Assigned Projects dialog.

3. Click ⧉ to copy the assigned Projects list to the computer clipboard from where you can paste the information into an email or text file.

4. Click 🖨 to print the assigned Projects list.

Role Permissions

In the GxP Admin Portal Software, you assign permissions to a Role. When you assign users to a Project, you select each user's Role in the Project. For each Project, the user can have one Role that permits the user to perform their required tasks, and no more. You can assign each user to multiple Projects and the user can have a different Role in each Project. This provides extensive and highly granular administrative control over the user's activities in the SoftMax Pro GxP Software.

Document Access Permissions

Use Document Access permissions to manage what users can do with documents.

- **Open Imported** - Allows users to open documents with the status: Imported.
- **Open In Work** - Allows users to open documents with the status: In Work.
- **Open Review Pending** - Allows users to open documents with the status: Review Pending.
- **Open Reviewed** - Allows users to open documents with the status: Reviewed.
- **Open Released** - Allows users to open documents with the status: Released.
- **Open Outdated** - Allows users to open documents that have the status: Outdated.
- **Open In Progress** - Allows users to open documents with the status: In Progress.
- **Open Approval Pending** - Allows users to open documents with the status: Approval Pending.
- **Open Approved** - Allows users to open documents with the status: Approved.
- **Open Canceled** - Allows users to open documents with the status: Canceled.

Document Workflow Permissions

Use Document Workflow permissions to manage what users can do in the document workflow.

- **Set Review Pending** - Allows users to set documents to the status: Review Pending.
- **Set Reviewed** - Allows users to set documents to the status: Reviewed.
- **Release Protocol** - Allows users to release a document as a protocol which sets the document status to Released.
- **Set Outdated** - Allows users to set documents to the status: Outdated.
- **Generate Compliance Data** - Allows users to generate compliance data. For example, (using the system default Roles) this user would be the Lab Technician who can open a protocol document with the status Released. The software prompts the user to save the document as a data document and assigns the document the status In Progress. The user then runs the assay to generate compliance data.
- **Set Approval Pending** - Allows users to set documents to the status: Approval Pending.
- **Set Approved** - Allows users to set documents to the status: Approved.
- **Set Canceled** - Allows users to set documents to the status: Canceled.
- **Set In Progress** - Allows users to set an Approved document back to the status: In Progress

Document Editing Permissions

Use Document Editing permissions to manage what users can do with documents.

- **Edit Reader Settings** - Allows users to define microplate reader acquisition settings.
- **Edit Notes Text** - Allows users to edit Note sections in the experiments in documents.
- **Read Empty Plates/Cuvettes** - Allows users to read empty Plate sections and empty Cuvette Set sections.
- **Function Editor** - Allows users to create custom curve fit functions.
- **Overwrite Plate/Cuvette Data** - Allows users to overwrite the data in Plate sections and Cuvette Set sections.

- **Edit Graphs, Summaries, and Reductions** - Allows users to edit Graph sections and the corresponding Summary formulas, Reduction formulas, and curve fits.
- **Assign Plate Layouts** - Allows users to assign plate layouts.
- **Edit Sample and Group Information** - Allows users to edit sample and Group section information.
- **Add/Delete Groups** - Allows users to add and delete Group sections from the experiments in documents.
- **Edit Formulas** - Allows users to edit formulas in documents.
- **Edit Print Options** - Allows users to edit the print options.
- **Lock/Unlock Sections** - Allows users to lock and unlock sections in the experiments in documents.
- **Mask/Unmask Wells** - Allows users to mask and unmask wells.
- **Create/Save As Data Document** - Allows users to save data documents to the database.
- **Create/Save As Protocol** - Allows users to save protocol documents to the database.
- **Change Auto Save Settings** - Allows users to change Auto Save settings.
- **Change Auto Export Settings** - Allows users to change Auto Export settings.

Statements & Signatures Permissions

Use Statement and Signatures permissions to manage what users can do with statements.

- **Add/Modify Statements** - Allows users to edit statements.
- **Sign Statements** - Allows users to sign statements.
- **Revoke Own Signature** - Allows users to remove only their own signatures from statements.
- **Revoke Any Signature** - Allows users to remove any signature from statements.

Document Management Permissions

Use Document Management permissions to manage what users can do with the documents.

- **Rename Document** - Allows users to rename documents.
- **Move Document** - Allows users to move documents to different folders in the database.
- **Delete Document** - Allows users to delete documents from the database.
- **Unlock Document** - Allows users to unlock documents.
- **Import Documents** - Allows users to import documents into the database.
- **Export Documents** - Allows users to export documents out of the database.

Folder Management Permissions

Use Folder Access permissions to manage what users can do with document storage folders.

- **Add Folder** - Allows users to create new folders in the database.
- **Rename Folder** - Allows users to rename folders in the database.
- **Move Folder** - Allows users to move folders in the database.
- **Delete Empty Folder** - Allows users to delete empty folders from the database.
- **Hide/Unhide Folder** - Allows users to hide and unhide folders and to use hidden folders in the database.
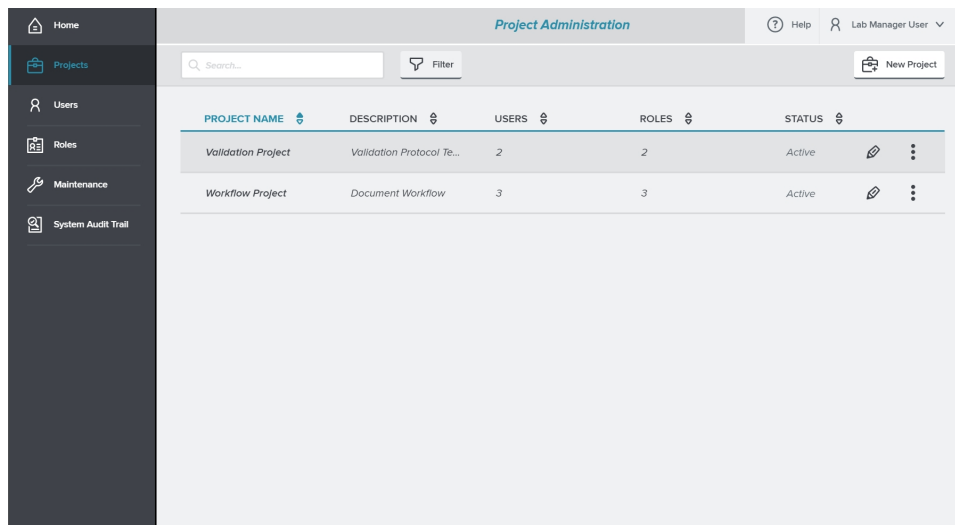
Instrument Permissions

Use Instrument permissions to manage what users can do with the microplate reader.

- **Lock/Unlock Instrument** - Allows users of the SpectraMax® iD3 Multi-Mode Microplate Reader and the SpectraMax® iD5 Multi-Mode Microplate Reader to lock and unlock the instrument touchscreen.
- **Instrument Simulator** - Allows users to simulate the connection between the SoftMax Pro GxP Software and an instrument.

The Project Administration page displays the list of Projects and allows you to manage Projects. Each user with the SoftMax Pro Access permission must be a member of at least one Project before they can login to the SoftMax Pro GxP Software. Each user with the SoftMax Pro access permission can be a member of multiple Projects and the user can have a different Role in each Project.

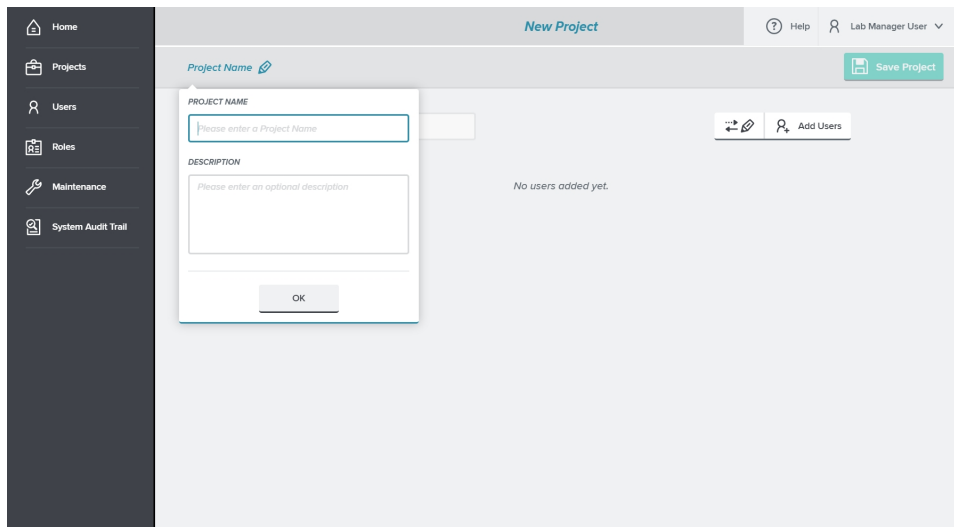> **Note:** Prerequisites: You must define users and Roles before you create Projects.

To manage Projects:

1. Click **Projects** on the left to display the Project Administration page.
2. Click **New Project** to display the New Projects page. See New Projects on page 36.
3. Next to a Project, click to display the Edit Project page. See Edit Projects on page 37.
4. Next to a Project, click :
   - Select **Copy Project** to display the Copy Project page. See Copy Projects on page 38.
   - Select **Deactivate Project** to make an active Project inactive or select **Activate Project** to make an inactive Project active.
   - Select **Project Information** to display the Project Information dialog. See Project Information on page 41.

New Projects

Use the New Project page to add Projects.

To add Projects:

1. Click **Projects** on the left to display the Project Administration page.
2. Click **New Project** to display the New Project page.
3. In the **Project Name** field, enter the Project name.
4. In the **Description** field, enter the Project description and then click **OK**.
5. Click **Add Users** to display the Assign Users to Project Role dialog where you add users to the Project and assign users to a Role in the Project. See .
6. After you add users, click **Save Project** to save the project.

## Edit Projects

Use the Edit Project page to edit Projects.
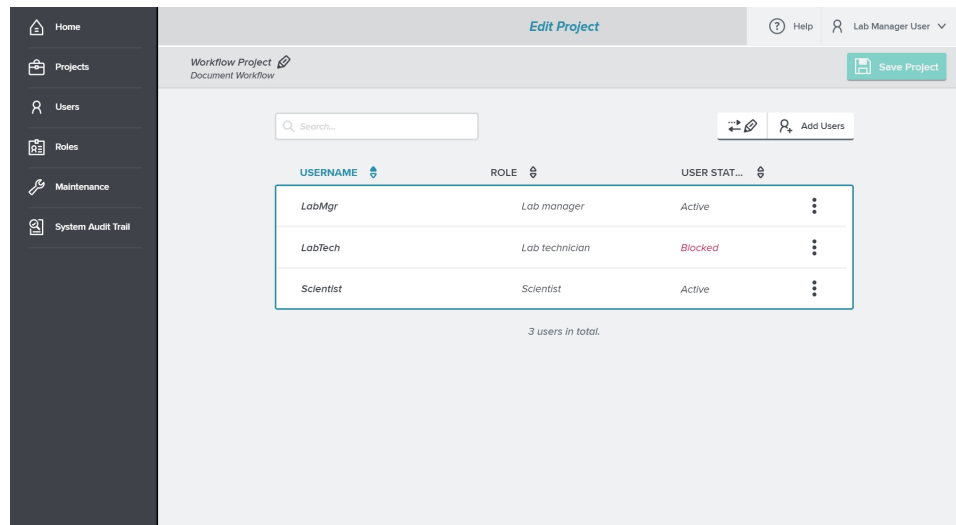
To edit Projects:

1. Click **Projects** on the left to display the Project Administration page.

2. Next to a Project, click ✎ to display the Edit Project page.

    -   On the top left, click ✎ to edit the **Project Name** and **Description**.
    -   Click **Add Users** to display the Assign Users to Project Role dialog where you add users to the Project and assign users to a Role in the Project. See Assign Users to Project Roles on page 39.
    -   Click ⇄✎ next to the Add User button to display a check box next to each username.

        Select the check box for each user to remove from the Project and then click 🗑 to remove the users you select from the Project.

1. Next to a username, click ⋮ :
    -   Select **Change Role** to display the Change Role dialog where you change the user's Role in the Project. See Change Role on page 40.
    -   Select **Remove User** to remove the user from the Project.
2. Click **Save Project**.

Copy Projects

Use the Copy Project page to copy Projects.
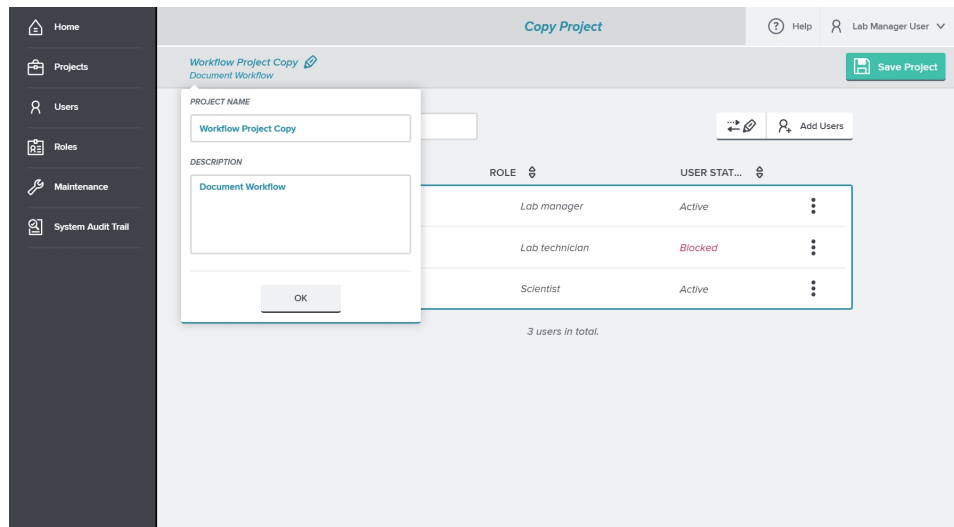
To copy Projects:

1. Click **Projects** on the left to display the Projects page.
2. Next to a Project, click ⋮ and select **Copy Project** to display the Copy Project page.
3. In the **Project Name** field, enter the Project name.
4. In the **Description** field, enter the Project description and click **OK**.
5. Click **Add Users** to display the Assign Users to Project Role page where you add users to the Project and assign users to a Role in the Project. See Assign Users to Project Roles on page 39.
6. Next to a username, click ⋮ :
   - Select **Change Role** to display the Change Role dialog where you change the user's Role in the Project. Change Role on page 40.
   - Select **Remove User** to remove the user from the Project.
7. Click ⇆⬚ next to the Add User button to display a check box next to each username.

   Select the check box for each user to remove from the Project and then click 🗑 to remove the users you select from the Project.
8. Click **Save Project**.

Assign Users to Project Roles

Use the Assign Users to Project Role dialog to add users to the Project and to assign users to a Role in the Project. You must define Users and Roles before you can assign users to a Project.
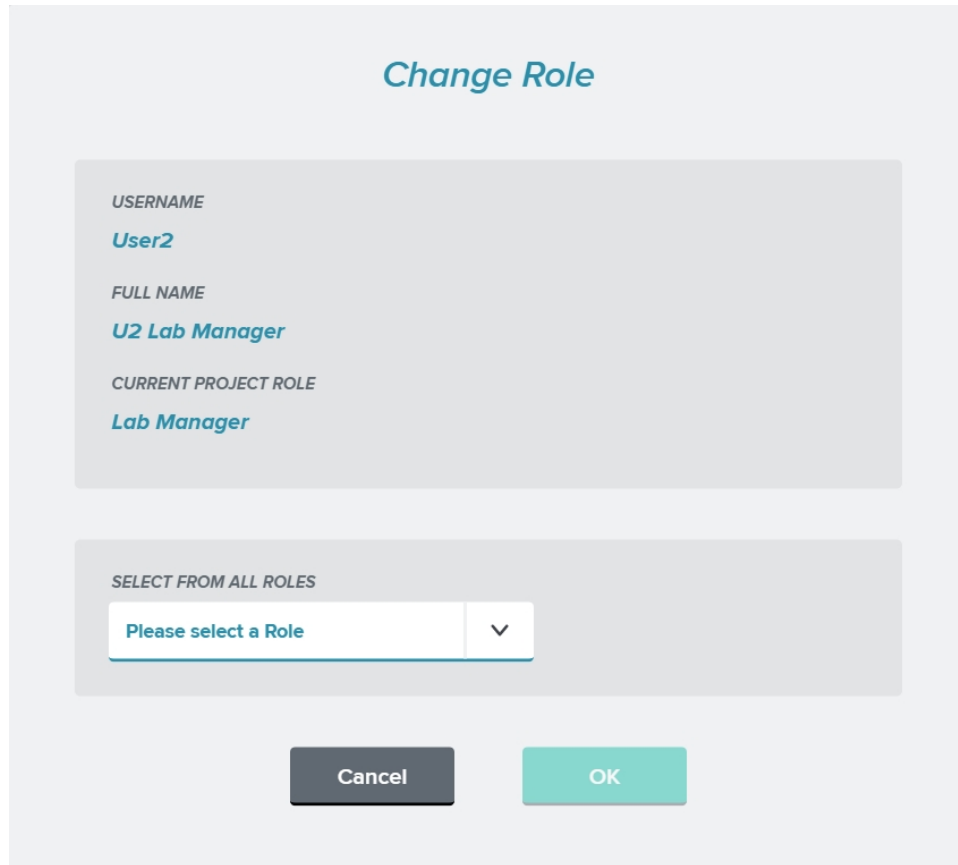
Note: Each user can have one Role in each Project.

To add users to a Project and assign users a Role in the Project:

1. Click **Projects** on the left to display the Project Administration page.

2. Click **New Project** to display the Add Projects page or click next to a Project to display the Edit Projects page. See New Projects on page 36 and Edit Projects on page 37.

3. Click **Add Users** to display the Assign Users to Project Role dialog.

4. In the **Select From All Users List**, next to each user to assign to the first Role, click to move the name to the Selected Users column.

5. Click the **Please Select A Role** and select a Role for the users.

6. Click **Assign**.

7. Click **Add Users** and repeat steps 4-6 to add additional users to a second Role in the Project, and so on for additional Roles, as needed.

Change Role

Use the Change Role dialog to change the user's Role in a Project.

To change a user's Role in a Project:

1. Click **Projects** on the left to display the Project Administration page.

2. Click **New Project** to display the Add Projects page or click ✐ next to a Project to display the Edit Project page. See New Projects on page 36 and Edit Projects on page 37.

3. Next to a username, click ⋮ and select **Change Role** to display the Change Role dialog.

4. Click the **Please Select A Role** ⌄ and select a Role for the user.

5. Click **OK**.

Project Information

The Project Information dialog displays the list of users and their Role assignment in the Project.
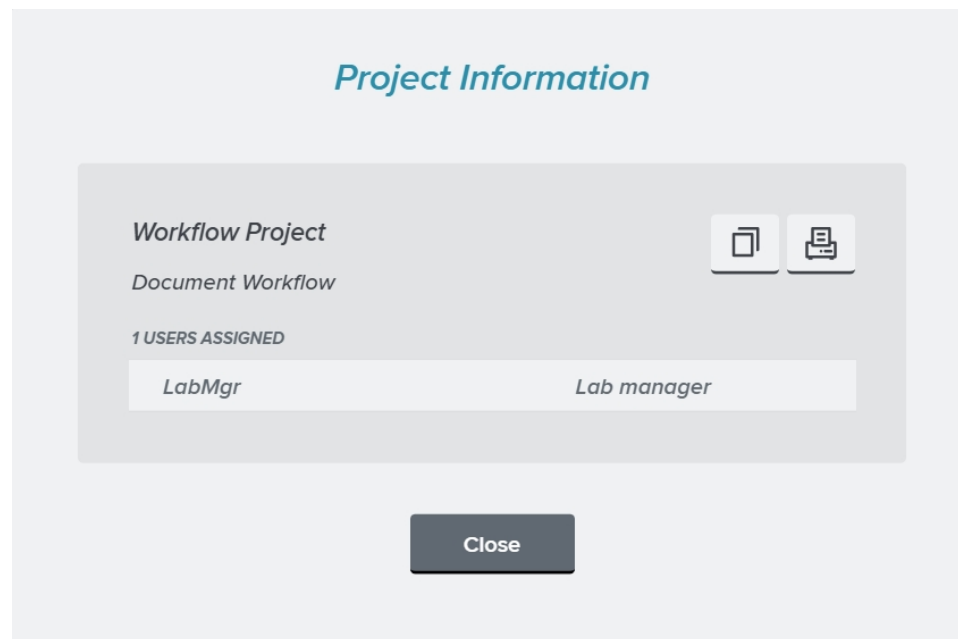
To display assigned projects:

1. Click **Projects** on the left to display the Project Administration page.

2. Next to a Project, click ⋮ and select **Project Information** to display the Project Information dialog.

3. Click 🗗 to copy the information to the computer clipboard from where you can paste the information into an email or a text file.

4. Click 🖶 to print the information.

Chapter 8: Maintenance

8

Use the Maintenance page to define password strength settings, to define which events display a notification on the Home page, to manage the licenses you assign to users with the SoftMax Pro Access permission, and to import legacy usernames.
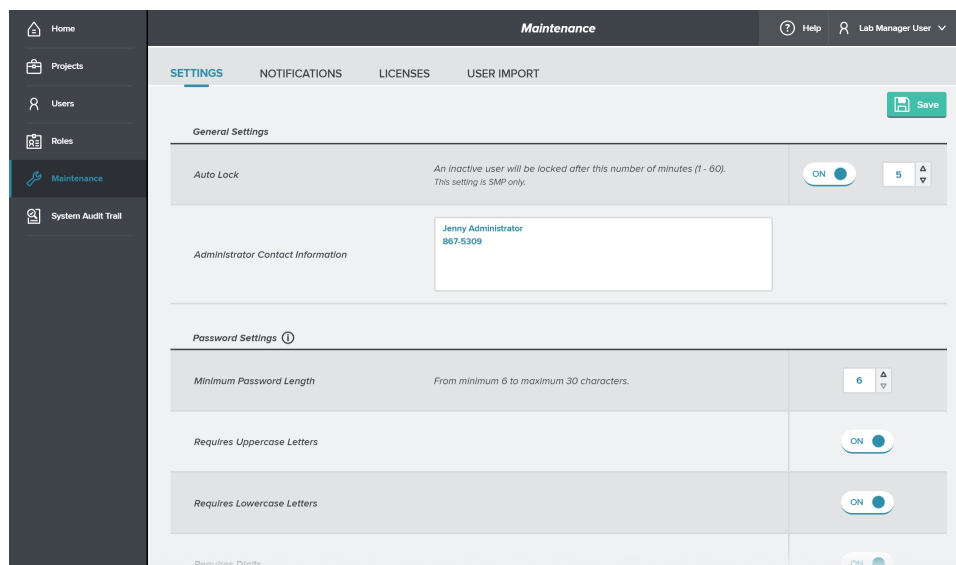
The Maintenance page has four tabs.

- Select the **Settings** tab to enter administrator contact information, define auto lock settings, and define password strength options. See .
- Select the **Notifications** tab to define which events should trigger a notification to appear on the Home page. See .
- Select the **Licenses** tab to manage the licenses you assign to users with the SoftMax Pro Access permission. See .
- Select the **User Import** tab to import GxP Admin Software version 2.x usernames into the GxP Admin Software version 7.2 database. See .

> **Note:** Windows Credentials login mode users use your company's Active Directory password settings.

Maintenance Settings

Use the Settings tab on the Maintenance page to define auto lock settings for the SoftMax Pro GxP Software, administrator contact information, and password strength options. The default password strength settings require Custom Credentials login mode user passwords to contain at least 10 characters, both uppercase and lowercase letters, at least one digit, and at least one special character.

To manage maintenance settings:

1. Click **Maintenance** on the left to display the Maintenance page with the **Settings** tab selected by default.

2. Click the **Auto Lock** to display . Enter a duration between 1 and 60 minutes to disable a user's session if they are inactive in the SoftMax Pro GxP Software for the duration you set. This does not affect the GxP Admin Portal Software.

3. In the **Administrator Contact Information** field, enter the name and contact information for the person who can reset a user's password and can unblock a user account when the user enters too many failed login attempts.

4. In the Password Settings section, set each of the following to to activate the feature:

   - Use the **Minimum Password Length** field to define the minimum number of characters for user passwords. Enter between 6 and 30 characters.
   - Use the **Requires Uppercase Letters** setting to require users to include upper case letters in their password.
   - Use the **Requires Lowercase Letters** setting to require users to include lower case letters in their password.
   - Use the **Requires Digits** setting to require users to include numbers in their password.
   - Use the **Special Characters** setting to require users to include special characters in their password.
   - Use the **Password Has To Differ From Username** setting to prevent users from using their username as their password.
   - Use the **Password Aging** setting to force users to change their password every x number of days. Enter the number of days that can elapse before the user must change their password, between 30 and 365 days.
   - Use the **Password History** setting to prevent users from reusing their previous x number of passwords. Enter the number of passwords that cannot be repeated, between 2 and 20.
   - Use the **Max. Number of False Login Attempts** setting to have the system block a user account after a number of incorrect password entries. Enter the number of allowable attempts between 3 and 10.

Note: Windows Credentials login mode users do not use the password settings you define here.

Maintenance Notifications

Use the Notifications tab on the Maintenance page to select which events display a notification on the Home page each time a user triggers the event. There are over 140 events that the software records to the System Audit Trail. You can activate Home page notifications for a subset of these events. See Audit Events on page 65.
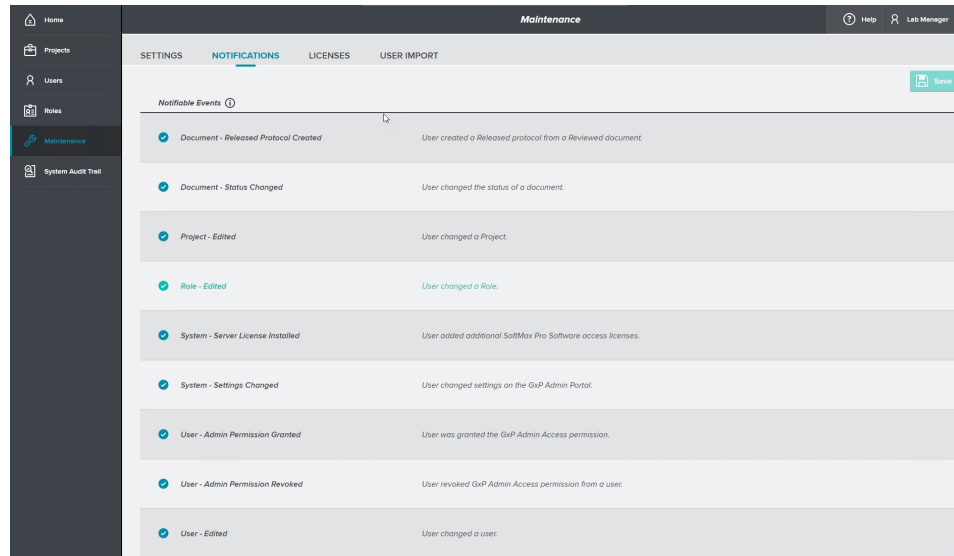
To select the events to display notifications:

1. On the Maintenance page, select the **Notifications** tab.
2. Select the check box for each event that you want to display a notification on the Home page.
3. Click **Save**.

Maintenance Licenses

Use the Licenses tab on the Maintenance page to activate the licenses for users with the SoftMax Pro Access permission.

Each user to whom you grant the SoftMax Pro Access permission requires a license.
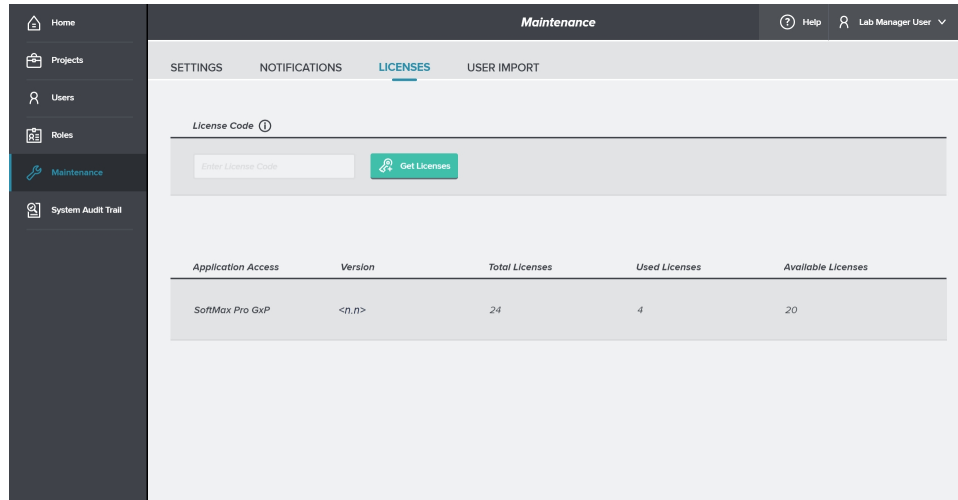
When you use upgrade licenses for multiple software versions of the GxP Admin Software and you end up with more users than licenses, use the License Upgrade dialog to assign applicable licenses to users. See License Upgrade on page 49.

Computer Has Internet Access

To activate licenses on a computer with Internet Access:

1. On the Maintenance page, select the **Licenses** tab.
2. In the **License Code** field, enter the license code.
3. Click **Get Licenses**.

Computer Does Not Have Internet Access

If the computer does not have Internet access:

1. In the **License Code** field, enter the license code.
2. Click **Get Licenses**.
3. Click **Export** and save the file that the system creates to a USB drive (offlineClaim.json).
4. Take the USB drive to a computer that has Internet Access and go to https://smplicensing.moleculardevices.com/gxpreg.
5. On the Offline License Management: Home page, click **Get License**.
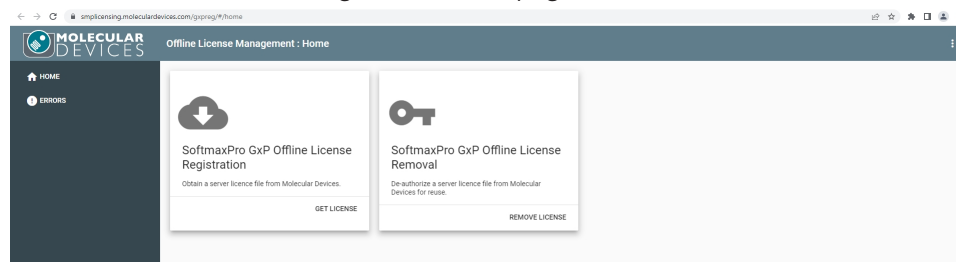
6. Next to the **Filename** field, click ✏ and navigate to the **offlineClaim.json** file.
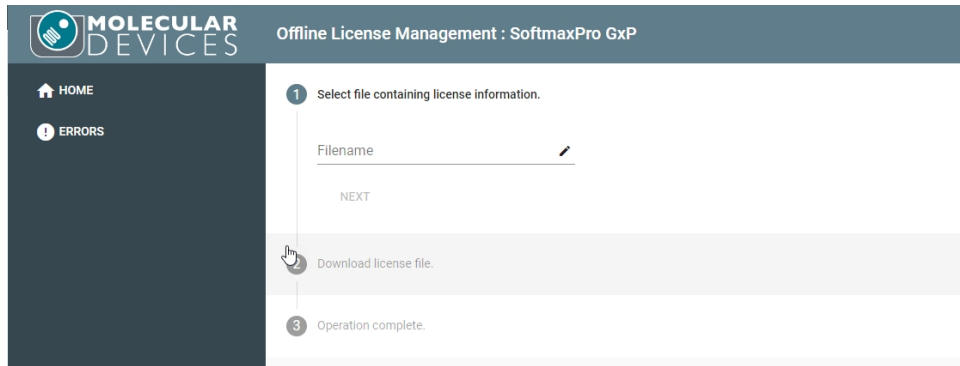
7. Click **Next**.
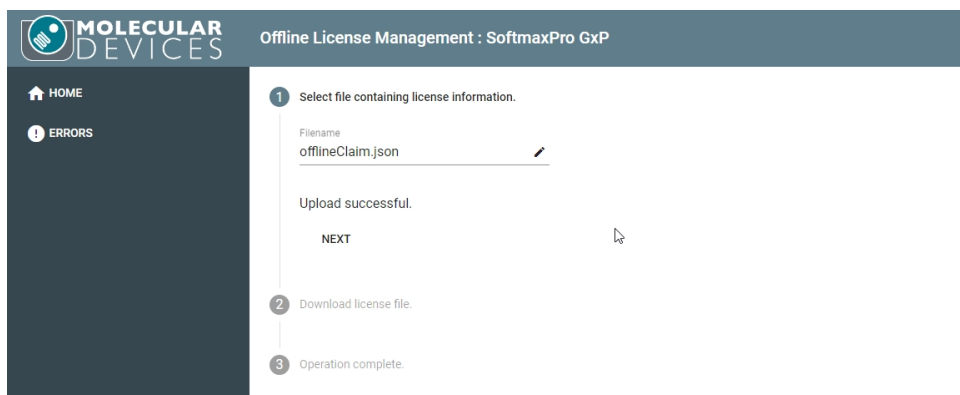
8. Click **Download License File** and save the **gxp-license-nnn.json** file to the USB.

9. Click **Done**.
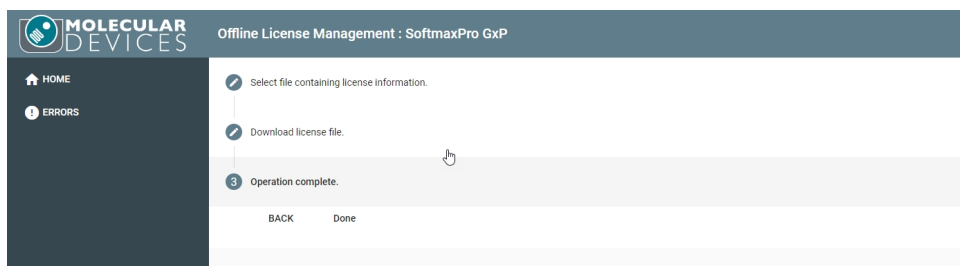
10. Take the USB drive back to the computer running the GxP Admin Portal Software and click **Import**.
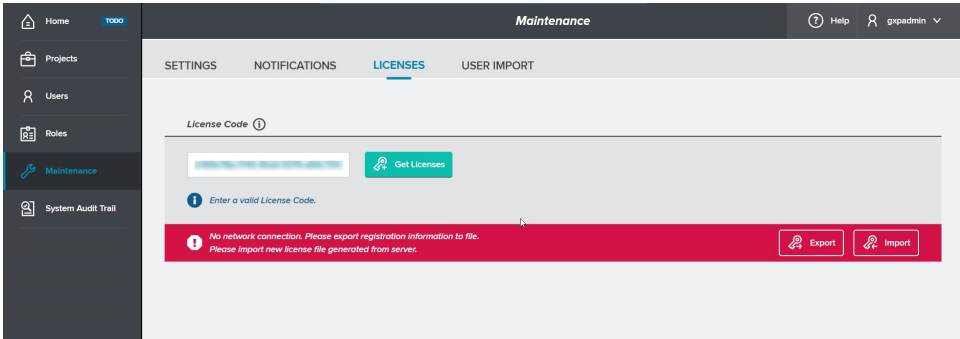
License Upgrade

When you use upgrade licenses for multiple versions of the SoftMax Pro GxP Software and you end up with more users than available licenses, use the Licenses Upgrade dialog to resolve license issues. Each user with the SoftMax Pro Access permission requires a license.
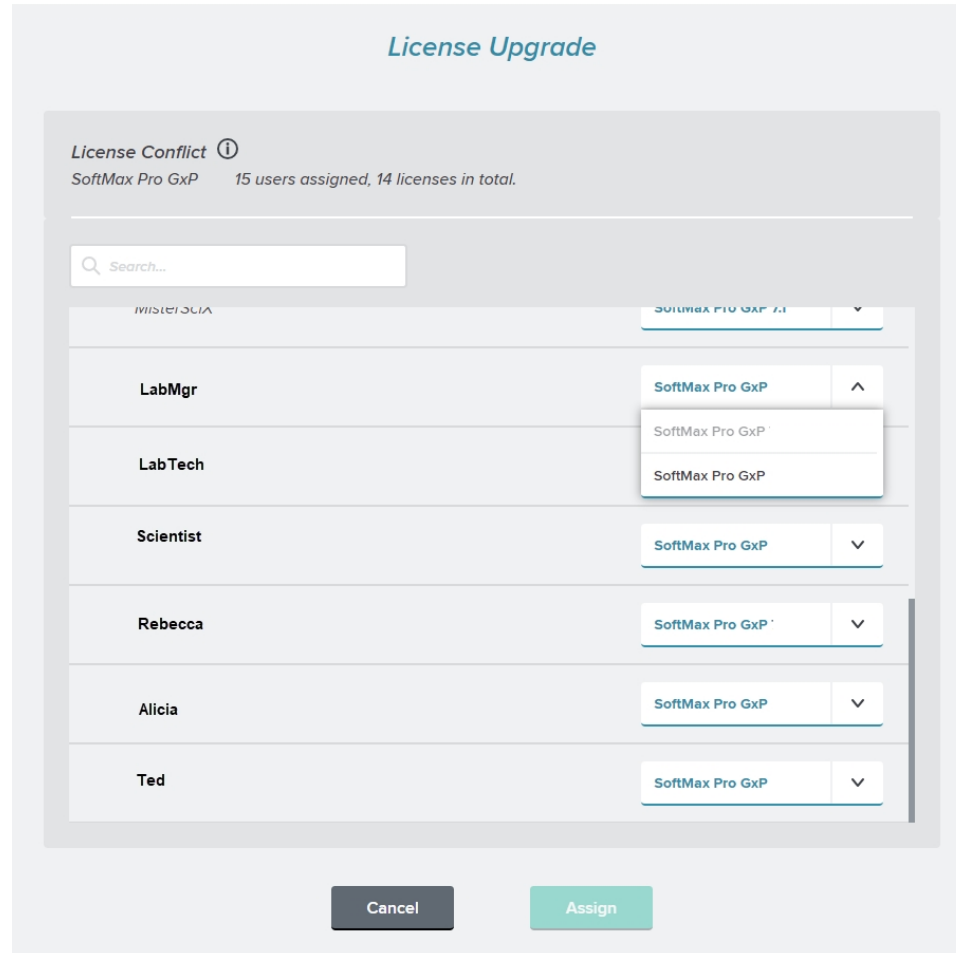
To resolve license issues:

1. Next to each user, click the **SoftMax Pro GxP** ⌄ and select a license.
2. Click **Assign**.

Maintenance User Import

Use the User Import tab on the Maintenance page to import the names of the users you created in GxP Admin Software version 2.x into the GxP Admin Software version 7.2 database. Use the GxP Admin EDB Converter Tool to convert the version 2.x *.edb files to the version 7.2 *.edbexp files before you import usernames into the 7.2 database. See Converting Legacy User Files on page 70.

Note: This process imports usernames, passwords, and the GxP Admin Access permission, when applicable.

After you complete the import, you must assign each user with the SoftMax Pro Access permission a license and to at least one Project.
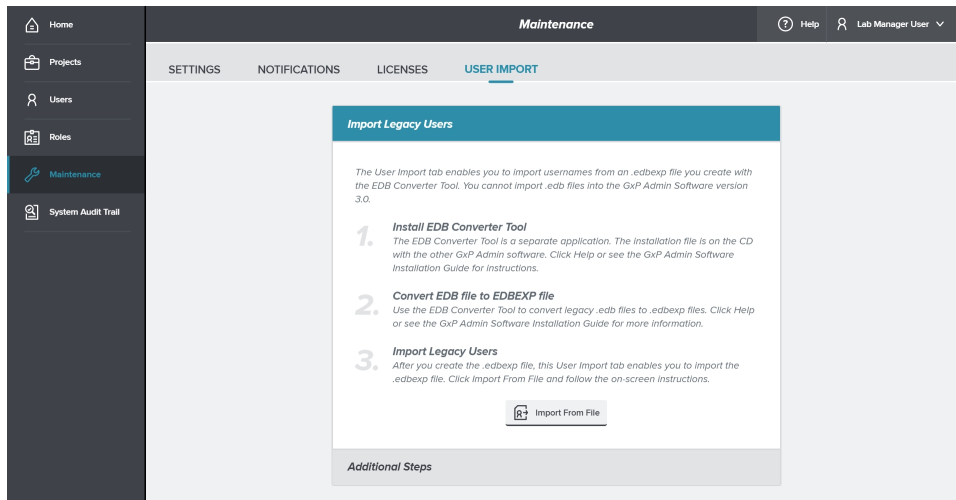
You repeat the following steps for each .edbexp file you create with the GxP Admin EDB Converter Tool.

To import users:

1. On the Maintenance page, select the **User Import** tab.
2. Click **Import From File** to display the Open dialog.
3. Navigate the folder hierarchy and select an .edbexp file to import.
4. Click **Open** to display the Import Legacy Users dialog.

Select Users to Import

Use the Import Legacy Users dialog to select the users to import into the GxP Admin Software version 7.2 database.
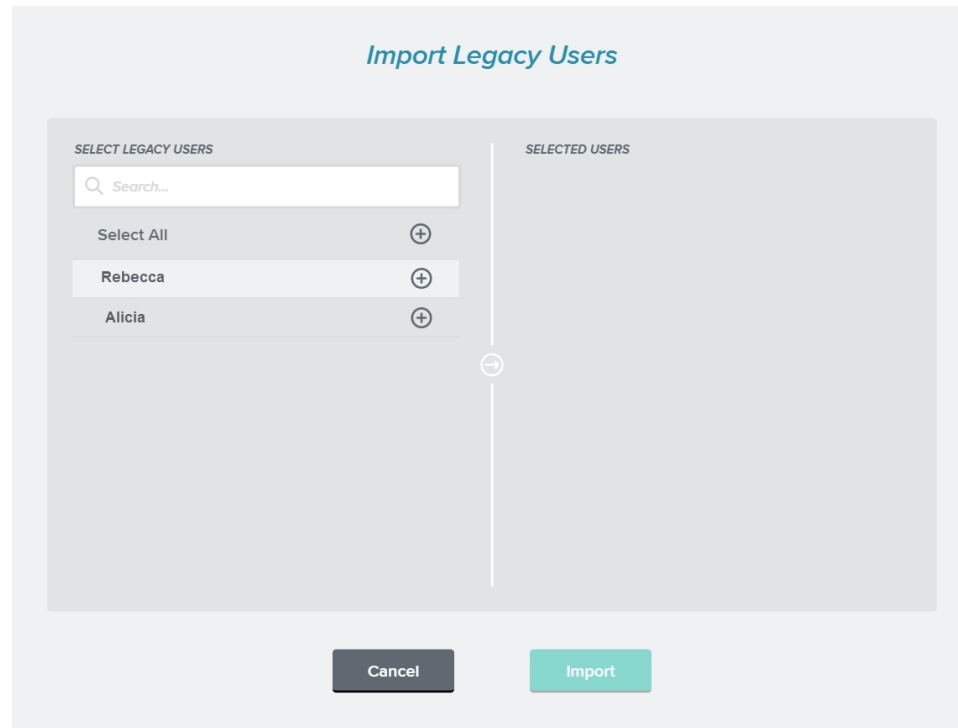
To select the users to import:

1. In the Select Legacy Users column, next to each user to import, click ⊕ to move the name to the Selected Users column.
2. Click **Import**.

Chapter 9: System Audit Trail

Use the System Audit Trail page to view the events that user actions trigger. You cannot edit or delete System Audit Trail entries. You can change the display of the page and you can filter the list of events to hide events from the display. The database uses the UTC time zone. Your date/time format settings affect the display of the dates on the System Audit Trail page. See Change Date/Time Format on page 21.

Click **System Audit Trail** on the left to display the System Audit Trail page.

- Click **Layout** to display the Custom Layout dialog where you define which columns of data display. See System Audit Trail Layout on page 54.
- Click **Refresh** to update the display.
- Click **Add Note** to display the Add Note To System Audit Trail dialog where you add a note. See System Audit Trail Notes on page 56.
- Click **Create Report** to display the Create Report dialog where you create a report. See System Audit Trail Report on page 57.
- Click **Filter Settings** to filter the list of events that display. See System Audit Trail Filters on page 55.
- Click **< Home** to return to the Home page. The Home button does not appear when the user does not have the GxP Admin Access permission. See Home on page 17.

System Audit Trail Layout

Use the Custom Layout dialog to define which columns of data display in the System Audit Trail page.
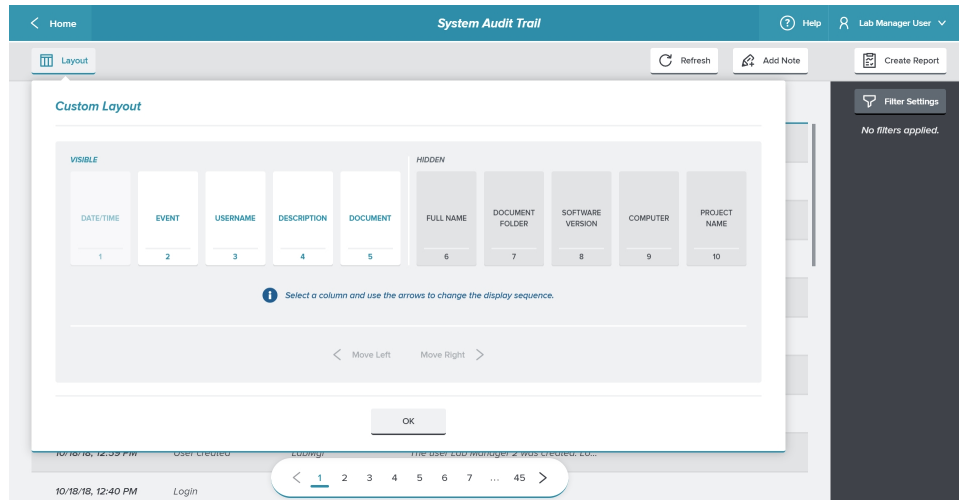
The System Audit Trail can display six columns of data. The Data/Time column must remain visible and must be located in the far left column.

1. Click **System Audit Trail** on the left to display the System Audit Trail page.
2. Click **Layout** to display the Custom Layout dialog.
   - The **Visible** area on the left displays the data columns that display in the System Audit Trail page. Each visible column has a light background and appears in the sequence in which they display.
   - The **Hidden** area on the right displays the data columns that do not display in the System Audit Trail page. Each hidden column has a shaded background.
3. Click on a column to display a blue border around the column, then click **Move Left** or click **Move Right** to change the column sequence and to move columns to the Visible area or to the Hidden area. Columns in the Visible area display in the System Audit Trail page in the sequence that displays in the Custom Layout dialog.
4. Click **OK** to display the System Audit Trail page.

System Audit Trail Filters

Use the Filter Settings dialog to limit the events that display in the System Audit Trail page. The Filter Settings dialog has four tabs and you can set up to five filters per tab.

To filter the list of events that display on the System Audit Trail page:

1. Click **System Audit Trail** on the left to display the System Audit Trail page.
2. Click **Filter Settings** to display the Filter Settings dialog.
3. The Filter Settings dialog has four tabs. After you select the tab, select up to five check boxes on the left. The fields on the right display the list of filters you select.
   - Use the **Username** tab to select up to five users to limit the list of events that display on the System Audit Trail page to only events triggered by the users you select.
   - Use the **Events** tab to select up to five events to limit the list of events that display on the System Audit Trail page to only the events you select. See Audit Events on page 65.
   - Use the **Documents** tab to select up to five documents to limit the list of events that display on the System Audit Trail page to only the events related to the documents you select.
   - Use the **Date** tab to select up to five dates to limit the list of events that display on the System Audit Trail page to only events that occurred on the dates you select.
4. Click **Apply** to display the System Audit Trail page with the list of events filtered to display only the events that meet your filter criteria.
5. Click **Remove Filter** to remove all filters.

System Audit Trail Notes

Use the Add Note To System Audit Trail dialog to add a note to the System Audit Trail.

To add a note to the System Audit Trail:

1. On the left, click **System Audit Trail** to display the System Audit Trail page.
2. Click **Add Note** to display the Add Note To System Audit Trail dialog.
3. In the **Enter Text For Note** field, enter the note text.
4. Click **Add** to add the note to the audit trail.

System Audit Trail Report

Use the Create Report dialog to create a System Audit Trail report file that you can save with a .pdf file format or a .csv file format.
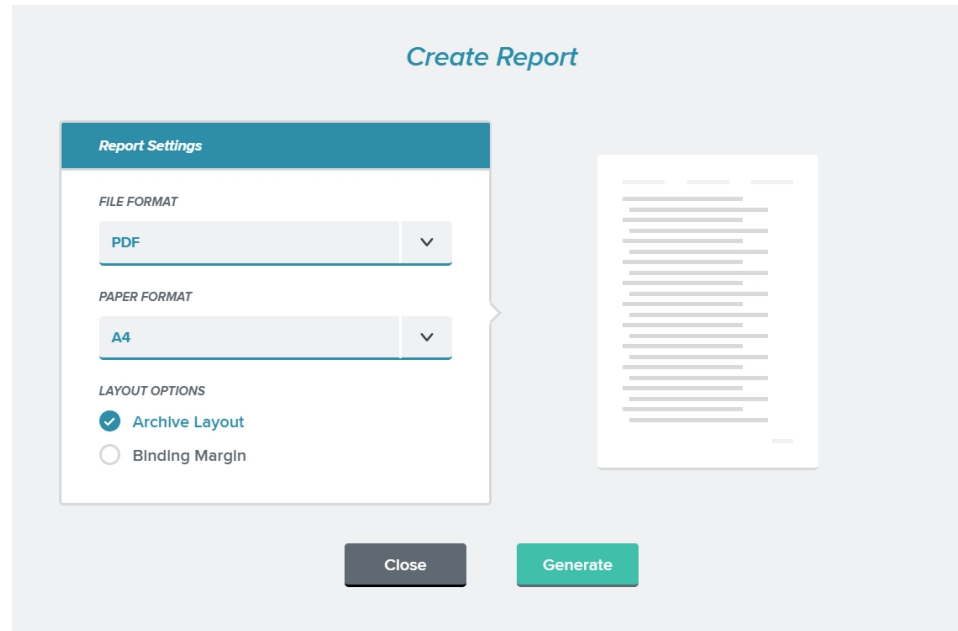
To create a System Audit Trail report:

1. On the left, click **System Audit Trail** to display the System Audit Trail page.
2. Click **Create Report** to display the Create Report dialog.
3. To create a report with the .pdf file extension, click the **File Format** ⌄ and select **PDF**:
   a. Click the **Paper Format** ⌄ and select the paper format.
   b. Select the **Archive Layout** check box to create a report in a list format. Leave this check box clear to create a report in a table format.
   c. Select the **Binding Margin** check box to justify the text to accommodate a binding. Leave this check box clear to center the report on the page.
4. To create a report with the .csv file extension, click the **File Format** and select **CSV**. The **Delimiter** field displays **CSV**.
5. Click **Generate**, the report generates and the Open dialog displays.
6. Navigate to where you want to save the report file and click **Save**.

The SoftMax Pro GxP Log On dialog displays when you start the SoftMax Pro GxP Software.
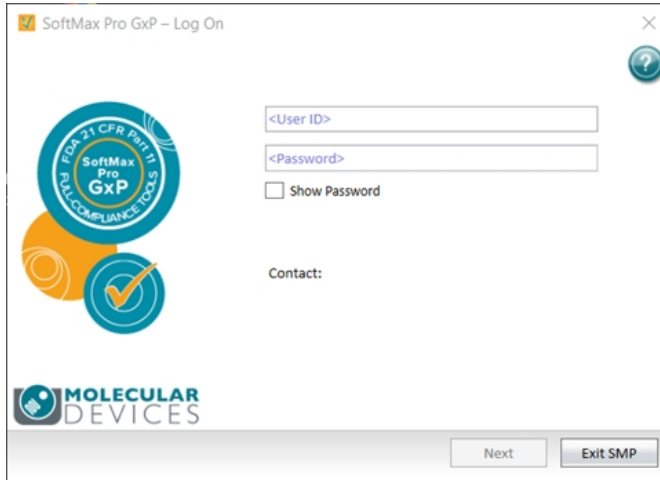
To log on to the SoftMax Pro GxP Software:

1. In the **<User ID>** field, enter your username.
2. In the **<Password>** field, enter your password (case sensitive).
3. Click **Next** to display the Please Select a Project dialog.
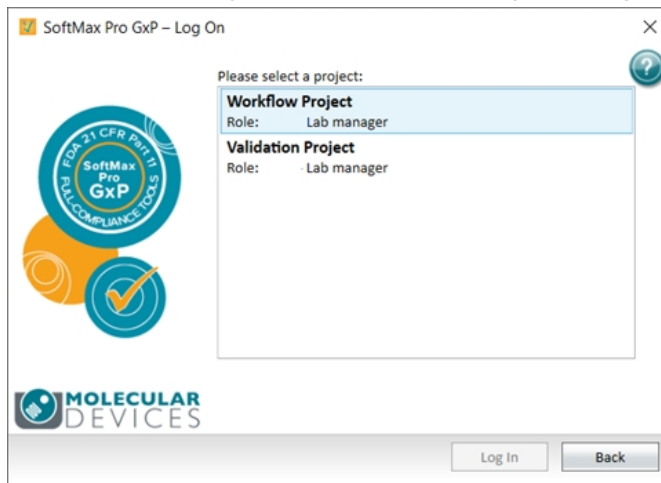
4. Select a Project and click **Log In**.

Logging In From Within the Software

In the Ribbon, on the GxP tab, use the icons to log out of the software and then log on to a different Project or as a different user.

1. In the Ribbon, select the **GxP** tab.
2. Click **User Log Off** to log off. The SoftMax Pro GxP Log On dialog displays.
3. Follow the steps above to log on.

SpectraMax iD3 and SpectraMax iD5 Considerations

- Click **GxP Mode On** to lock the instrument touchscreen and operate the instrument from the computer running the SoftMax Pro Software in GxP mode. This locks the instrument touchscreen for all users and you must operate the instrument from a computer running the SoftMax Pro Software - GxP edition.

- Click **GxP Mode Off** to release the lock from the instrument touchscreen and allow users to use the instrument touchscreen to run experiments.

 Note: The instrument remains locked until the user with the Lock/Unlock Instrument permission clicks **GxP Mode Off** to stop the GxP mode. You cannot use the Instrument Connection dialog to disconnect from an instrument that is locked in GxP mode.

Appendix A: Default Roles

A

Use the GxP Admin Software default Roles to assign users permissions to perform the tasks that correspond to each document status. You can create your own Roles and you can edit the default Roles.

Default Role Permissions

Permission Group	Permission Name	Lab Mgr	Lab Tech	Scientist
Document Access	Open Imported			✔
	Open In Work			✔
	Open Review Pending	✔		
	Open Reviewed	✔		✔
	Open Released	✔	✔	✔
	Open Outdated	✔		✔
	Open In Progress		✔	
	Open Approval Pending	✔		✔
	Open Approved	✔		✔
	Open Canceled	✔		✔
Document Workflow	Set Review Pending			✔
	Set Reviewed	✔		
	Release Protocol	✔		
	Set Outdated	✔		
	Generate Compliance Data		✔	
	Set Approval Pending		✔	
	Set Approved	✔		
	Set Canceled	✔	✔	✔
	Set In Progress	✔		

Default Role Permissions (continued)

Permission Group	Permission Name	Lab Mgr	Lab Tech	Scientist
Document Editing	Edit Reader Settings			✓
	Edit Notes Text		✓	✓
	Read Empty Plates/Cuvettes		✓	✓
	Function Editor			✓
	Overwrite Plate/Cuvette Data			✓
	Edit Graphs, Summaries, and Reductions			✓
	Assign Plate Layouts		✓	✓
	Edit Sample and Group Information		✓	✓
	Add/Delete Groups			✓
	Edit Formulas			✓
	Edit Print Options			✓
	Lock/Unlock Sections			✓
	Mask/Unmask Wells		✓	✓
	Create/Save As Data Document	✓		✓
	Create/Save As Protocol			✓
	Change Auto Save Settings			✓
	Change Auto Export Settings			✓
Statements Signatures	Add/Modify Statements			✓
	Sign Statements	✓	✓	✓
	Revoke Own Signature	✓	✓	✓
	Revoke Any Signature			
Document Management	Rename Document	✓		✓
	Move Document	✓		✓
	Delete Document	✓		✓
	Unlock Document	✓		
	Import Documents			✓
	Export Documents	✓	✓	✓

Default Role Permissions (continued)

Permission Group	Permission Name	Lab Mgr	Lab Tech	Scientist
Folder Management	Add Folder	✔		✔
	Rename Folder	✔		✔
	Move Folder	✔		✔
	Delete Empty Folder	✔		✔
	Hide/Unhide Folder	✔		✔
Instrument	Lock/Unlock Instrument	✔		✔
	Instrument Simulator			✔

Appendix B: Audit Events

B

The GxP Admin Software and the SoftMax Pro GxP Software generate audit trails that record the events that user actions trigger. For each event instance, the audit trail records the date and time, the username of the person who was logged on, and the event action. Users cannot alter the audit trail, nor can they edit or delete audit trail entries.

> **Note:** StakMax specific commands and scripts you use in the StakMax Software are not tracked in the audit trail and do not have user permission settings. Please implement standard work as required by your organization.

The following events trigger a System Audit Trail entry:

- **Application - Close on Lock**: Application closed while in locked state.
- **Auto Export - Failed**: Auto Export to location failed.
- **Auto Export - Settings Edited**: User changed Auto Export settings.
- **Auto Export - Started**: Auto Export started to export to a single location.
- **Auto Export - Started with Multiple Locations**: Auto Export started to export to multiple locations.
- **Auto Read - Settings Confirmed**: User confirmed Auto Read settings.
- **Auto Save - Settings Edited**: User changed Auto Save settings.
- **Cuvette Set Section - Added**: User added a Cuvette Set section to an experiment.
- **Cuvette Set Section - Appended Data**: User appended data to a Cuvette Set section.
- **Cuvette Set Section - Data Pasted**: User pasted data into a Cuvette Set section.
- **Cuvette Set Section - Data Replaced**: User replaced data in a Cuvette Set section.
- **Cuvette Set Section - Reference Read**: User started a Cuvette Set reference read.
- **Data Section - Data Deleted**: User deleted data from a Plate section or a Cuvette Set section.
- **Data Section - Data Pasted Over Existing**: User pasted data over existing data in a Plate section or a Cuvette Set section.
- **Document - Unlocked**: User unlocked a document.
- **Document - Altered, Modified, or Tampered**: Document has been changed, modified, or tampered with outside of the SoftMax Pro Software.
- **Document - Audit Trail Import Error**: An error occurred importing a document audit trail.
- **Document - Audit Trail Note Added**: User added a not to the audit trail.
- **Document - Changes Discarded**: User did not save changes in the document.
- **Document - Closed**: User closed a document.
- **Document - Created**: User created a new document.
- **Document - Created from Non-Compliant**: Document was created from a non-compliant document.
- **Document - Deleted**: User deleted a document from the database.
- **Document - Exported**: User exported a document in SoftMax Pro format.
- **Document - Legacy Audit Trail Imported**: The audit trail from an imported document was successfully imported to the database.
- **Document - Legacy Imported**: Documents were successfully imported into the database.
- **Document - Moved**: User moved a document to a different location in the database.
- **Document - Open Failed**: An error occurred when a user attempted to open a document.
- **Document - Opened**: User opened a document.

- **Document - Print Canceled**: User canceled the print of a document.
- **Document - Printed**: User printed a document.
- **Document - Protocol Created**: User created a new protocol.
- ***Document - Released Protocol Created**: User created a Released protocol from a Reviewed document.
- **Document - Renamed**: User changed the name of a document.
- **Document - Save**: User saved a document using Save or Save As.
- **Document - Save As PDF**: User saved a document in a .pdf format.
- **Document - Save Failed**: An error occurred when a user attempted to save a document.
- **Document - Selected Sections Exported**: User exported selected sections.
- ***Document - Status Changed**: User changed the status of a document.
- **Document - Unlocked**: User unlocked a document.
- **Document - Workflow Activity**: Workflow activity in a document captured.
- **Experiment - Added**: User added an experiment to a document.
- **Experiment - Deleted**: User deleted an experiment from a document.
- **Experiment - Duplicated**: User duplicated an experiment in a document.
- **Experiment - Read Started**: User started a read.
- **Experiment - Renamed**: User changed the name of an experiment in a document.
- **Experiment - Section Deleted**: User deleted a section from an experiment.
- **Experiment - Section Duplicated**: User duplicated a section in an experiment.
- **Experiment - Section Locked**: User locked a section in an experiment.
- **Experiment - Section Print Disabled**: User marked a section as not printable.
- **Experiment - Section Print Enabled**: User marked a section as printable.
- **Experiment - Section Renamed**: User changed the name of a section in an experiment.
- **Experiment - Section Unlocked**: User unlocked a section in an experiment.
- **Experiment - Summary Formula Added or Edited**: User added or edited a Summary formula in a Group section or a Note section.
- **Experiment - Summary Formula Deleted**: User deleted a Summary formula from a Note section or a Group section.
- **Experiment - Summary Formula Pasted**: User pasted a Summary formula into a section in an experiment.
- **Folder - Added**: User added a folder to the database.
- **Folder - Deleted**: User deleted a folder from the database.
- **Folder - Hidden**: User hid a folder in the database.
- **Folder - Moved**: User moved a folder to a new location in the database.
- **Folder - Renamed**: User changed the name of a folder in the database.
- **Folder - Unhidden**: User unhid a folder in the database.
- **Graph Section - Added**: User added a Graph section to an experiment.
- **Graph Section - Curve Fit Changed**: User changed the curve fit in a Graph section.
- **Graph Section - Settings Edited**: User changed the settings in a Graph section.
- **Group Section - Column Formula Added or Edited**: User added or edited a Column formula in a Group section.
- **Group Section - Column Pasted**: User pasted a column into a Group section.
- **Group Section - Cut or Deleted Column**: User removed a column from a Group section.
- **Group Section - Settings Edited**: User changed the settings in a Group section.
- **Instrument - Calibrated**: User calibrated an instrument.

- **Instrument - Locked**: User locked the touchscreen on a SpectraMax iD3 or a SpectraMax iD5.
- **Instrument - Selected**: User selected an instrument to acquire data.
- **Instrument - Temperature Turned Off**: User turned the instrument temperature control off.
- **Instrument - Temperature Turned On**: User turned the instrument temperature control on.
- **Note Section - Added**: User added a Note section to an experiment.
- **Plate Section - Added**: User added a Plate section to an experiment.
- **Plate Section - Append Read**: User started a read to append data.
- **Plate Section - Append Data**: User appended data to a Plate section.
- **Plate Section - Clone Added**: User cloned a plate in a Plate section.
- **Plate Section - Clone Delete Confirmed**: User confirmed the deletion of a plate clone.
- **Plate Section - Clone Deleted**: User deleted a plate clone from a Plate section.
- **Plate Section - Data Import Failed**: Data import into a Plate section failed.
- **Plate Section - Data Import Notification**: Data imported into a Plate section contains saturated or invalid values.
- **Plate Section - Data Imported**: Data was imported into a Plate section.
- **Plate Section - Data Pasted**: User pasted data into a Plate section.
- **Plate Section - Data Replaced**: User replaced data in a Plate section.
- **Plate Section - Read**: User started a read.
- **Plate Section - Read Canceled**: User canceled a read.
- **Plate Section - Read Finished**: Read finished.
- **Plate Section - Read Interrupted**: User interrupted a read.
- **Plate Section - Reduction Changes Accepted**: User confirmed changes made to reduction settings.
- **Plate Section - Settings Edited**: User changed the settings for a Plate section.
- **Plate Section - Template Edited**: User changed a plate template.
- **Plate Section - Template Imported**: User imported a template into a Plate section.
- **Plate Section - Template Pasted**: User pasted a template into a Plate section.
- **Plate Section - Wells Masked**: User masked wells in a Plate section.
- **Plate Section - Wells Unmasked**: User unmasked wells in a Plate section.
- **Print Options Edited**: User changed print options.
- **Project - Activated**: User activated a Project.
- **Project - Added**: User added a Project.
- **Project - Deactivated**: User deactivated a Project.
- ***Project - Edited**: User changed a Project.
- **Role - Activated**: User activated a Role.
- **Role - Added**: User added a new Role.
- **Role - Deactivated**: User deactivated a Role.
- ***Role - Edited**: User changed a Role.
- **Statement - Added**: User added a statement to a document.
- **Statement - All Signatures Removed**: All signatures removed when a new document was created by Save As.
- **Statement - Deleted**: User deleted a statement from a document.
- **Statement - Edited**: User edited a statement.
- **Statement - Pasted**: User pasted a statement into a document.
- **Statement - Revoke Signature Canceled**: User did not enter their password when revoking a signature from a statement and the signature was not revoked.

- **Statement - Signed**: User signed a statement.
- **Statement - Signed Statement Canceled**: User did not enter their password when adding a signature to a statement and the statement was not signed.
- **Statement - Signed Statement Removed**: Signed statement removed in the process of creating a new document from a released protocol.
- **Statement - Single Signature Revoked**: User revoked a single signature from a statement.
- **System - Database Restored**: User restored the database.
- **System - EDB File Imported**: User imported a file that contains the usernames of users from legacy GxP Admin Software.
- **System - Offline Data Sync Ended**: The SoftMax Pro Software finished synchronizing offline data.
- **System - Offline Status**: The SoftMax Pro software went into offline status.
- ***System - Server License Installed**: User added additional SoftMax Pro Software access licenses.
- ***System - Settings Changed**: User changed settings in the GxP Admin Portal.
- **User - Activated**: User activated a user.
- **User - Added**: User added a new user.
- ***User - Admin Permission Granted**: User was granted the GxP Admin Access permission.
- ***User - Admin Permission Revoked**: User revoked the GxP Admin Access permission from a user.
- **User - Blocked**: User blocked due to too many incorrect login attempts.
- **User - Change Password Attempted**: User attempted to change their password.
- **User - Change Password Canceled**: User started to change their password but did not complete the process.
- **User - Change Password Successful**: User successfully changed their password.
- **User - Deactivated**: User deactivated a user.
- ***User - Edited**: User changed a user.
- **User - License Assigned**: User was assigned a license to access the SoftMax Pro software.
- **User License Unassigned**: User removed a SoftMax Pro access license from a user.
- **User - Logged In**: User has logged into the GxP Admin Portal or the SoftMax Pro Software.
- **User - Logged Out**: User has logged out.
- **User - Logon Attempted**: User tried to log into the software.
- ***User - Logon Failed**: User unsuccessfully attempted to log into the GxP Admin Portal or the SoftMax Pro Software.
- **User - Logon Successful**: User successfully logged into the software.
- **User - Password Changed**: User changed their password.
- **User - Software Unlock Failed**: An error occurred when a user attempted to unlock the software.
- **User - Software Unlocked**: User unlocked the software.

* Can trigger a notification for the Home page.

Appendix C: Converting Legacy Users

The GxP Admin Software version 3.x and higher is significantly different from the previous versions. The database structure is different and additional security permissions have been implemented. Therefore, if you want to use the users from GxP Admin Software version 2.x, you must convert legacy user files to an updated format and then import the legacy users into the GxP Admin Software database.

> **Note:** If you use the multi computer setup and you intend have users use your company's Active Directory database you will use the GxP Admin Portal Software to create new Windows Credentials login mode users. GxP Admin Software version 2.x did not support Windows Active Directory and users you convert are created as Custom Credential users in the GxP Admin Software. The single computer setup does not support the Windows Credentials login mode.

The GxP Admin EDB Converter Tool is a separate software application that converts the GxP Admin Software version 2.x user files that have an .edb file extension to user files that have an .edbexp file extension.

After you convert the user files, you use the GxP Admin Portal Software to import the files with the .edbexp file extensions into the GxP Admin Software database. These users will appear in the GxP Admin Portal Software, will use their previous password for their initial login, and will have the GxP Admin Access permission if they had administrative permission in the 2.x software version. You must then use the GxP Admin Portal Software to assign applicable users the SoftMax Pro Access permission a user license and also assign them to a Project before they can use the SoftMax Pro GxP Software.

To prepare to convert GxP Admin Software version 2.x user files:

- You can run the GxP Admin EDB Converter Tool on the computer on which you install the SoftMax Pro GxP Software Suite if the computer has a network connection to the computers that contain the .edb files.
- You can use a USB drive to copy the .edb files to the computer on which you install the GxP Admin Portal Software and the GxP Admin EDB Converter Tool.
- You can use a USB drive to move the folder in which you install the GxP Admin EDB Converter Tool to the computer on which the .edb files are located.

## Install the GxP Admin EDB Converter Tool

To install the GxP Admin EDB Converter Tool:

1. Navigate to the SoftMax Pro GxP Software Suite installations files you downloaded or insert the GxP Admin Software USB in the computer USB drive. Locate and double-click EDBConverter<n.n.n>Setup.exe file to start the install.
2. On the Welcome page, click **Next**.
3. On the License Agreement page, select the **I Accept the Agreement** check box and then click **Next**.
4. On the Destination Folder page and the pages that follow, click **Next** to accept the default settings or you can read the instructions and do a custom installation until the Installation Complete page displays.
5. On the Installation Complete page, click **Finish**.

The GxP Admin EDB Converter Tool icon appears on the computer desktop.

Converting Legacy User Files

The GxP Admin Software version 2.x user files have an .edb file extension and the SoftMax Pro GxP Software Suite version 7.2 user files have an .edbexp file extension.
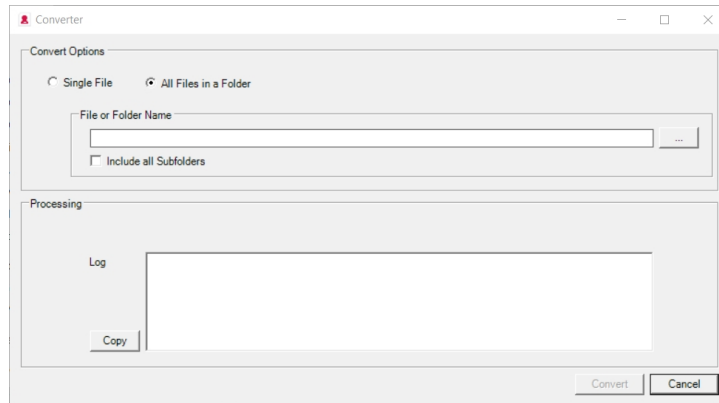
Converting a Single File

To convert one .edb file to an .edbexp file:

1. On the computer desktop, double-click or locate and double-click **ConverterTool.exe** to display the Converter dialog.
2. Select the **Single File** Convert Option.
3. To the right of the **File or Folder Name** field, click to display the Open dialog.
4. Navigate to the .edb file and click **Open** to display the path to the file in the File or Folder Name field. Note this location because the software places the new .edbexp file here.
5. Click **Convert**. The Log field displays the progress of the conversion. The software places the .edbexp file in the same folder as the .edb file.
6. Copy the .edbexp file to a USB drive or a location that is accessible to the computer running the GxP Admin Portal Software. See .

Converting Multiple Files

To convert multiple .edb files to .edbexp files:

1. On the computer desktop, double-click or locate and double-click **ConverterTool.exe** to display the Converter dialog.
2. Select the **All Files In a Folder** Convert Option.
3. To the right of the **File or Folder Name** field, click to display the Browse For Folder dialog.
4. Navigate to the folder that contains the .edb files and click **OK** to display the path to the folder in the File or Folder Name field.
5. Select the **Include All Subfolders** check box to convert all .edb files in the subfolders of the folder you select.
6. Click **Convert**. The Log field displays the progress of the conversion. The software places the .edbexp files in the same folders as the .edb files.
7. Copy the .edbexp files to a USB drive or to a location that is accessible to the computer running the GxP Admin Portal Software. See .

# Appendix D: Backing Up the GxP Admin Software Database

D

For the single computer setup, the SoftMax Pro 7.2 GxP Single Computer Setup Installation Wizard allows you to install the GxP Admin Backup Tool. If you do not have standard Microsoft SQL backup tools, you can use this tool to schedule recurring database backups and to do a backup on an as needed basis.

Note: The GxP Admin Backup Tool is not applicable for the multi computer setup because it is assumed that your network has standard backup procedures in place.

If a backup occurs while the system is in use, there is the possibility that the backup audit trail information could be inconsistent. For example, if a user is actively creating new plates when the backup starts, the backup may save the audit trail entry before the changes to the document are saved. The user continues to work, and the active database is fully consistent. However, the backup contains the audit trail information for the new plates and does not contain the document version with the latest plate added. This is only relevant if you restore the database from such a backup.
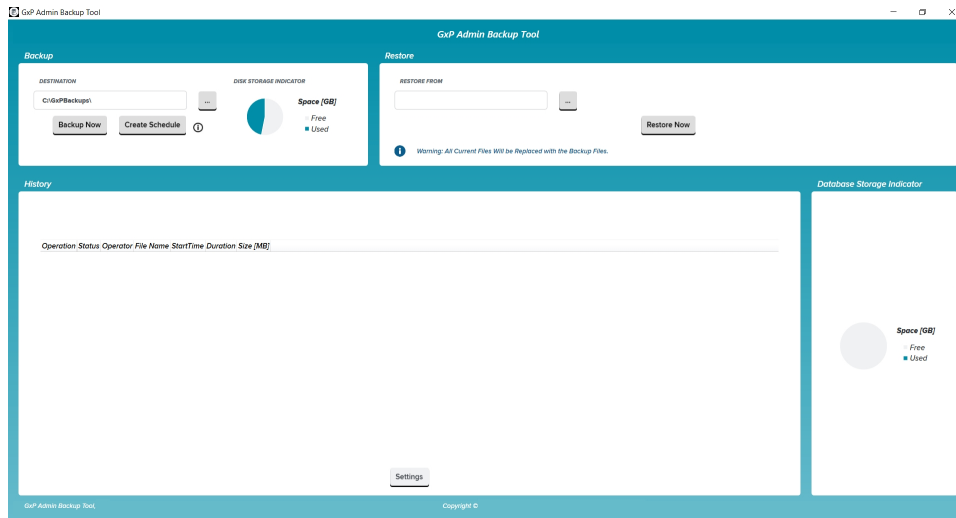
Note: The GxP Admin Backup Tool places the backup files in the following location on the local computer:
C:\users\public

Backing Up The Database

The GxP Admin Backup Tool creates a report that documents the relevant information. This report is saved to the same folder that you designate as the destination folder for the backup files.

To back up the GxP Admin Software database:

1. On the computer desktop, double-click [icon] or locate and double-click **GxPAdminBackupTool.exe** to display the GxP Admin Backup Tool dialog.
2. The Backup Destination must be the following location on the local computer: C:\users\public
3. In the Browse for Folder dialog, select the destination location and click **OK**.
4. Click **Backup Now**.

> [icon] **Note:** If you logged into the Windows operating system as a user that has administrator privileges to the computer, the GxP Admin Backup Tool displays *Could not backup database* if you attempt to back up to a folder other than C:\users\public.

5. The **History** area displays the operation, status, operator, file name (file name is the date and time the backup is created and includes the path to the file), start time, duration, and size of the backup file. The GxP Admin Backup Tool creates a ReportDocx.pdf file in the backup folder for compliance purposes.
6. To manage the backups that display in the History area, click **Settings** to display the Keep Backups dialog.
7. In the **Keep the Last __ Backups** field, enter the number of backups to save and click **OK**.

Creating a Backup Schedule

Use the GxP Admin Backup Tool and Windows Scheduler to schedule regular database backups.

To create a database backup schedule:

1. On the computer desktop, double-click [icon] or locate and double-click **GxPAdminBackupTool.exe** to display the GxP Admin Backup Tool dialog.
2. In the **Backup** area, click **Create Schedule** to display the Create Schedule Information dialog.
3. Click **Open Windows Scheduler** to display the Task Scheduler dialog.
4. On the left, select **Task Scheduler Library**.
5. In the **Task Scheduler Library**, select the **GxPDatabaseBackupTask**.
6. On the right in the **Actions** area, click **Properties** to display the Properties dialog.
7. Select the **Triggers** tab.
8. Use the **New**, **Edit**, and **Delete** buttons to define when to schedule the backup task to trigger.
9. In the Properties dialog, select the **General** tab.
10. In the **Security Options** area, note the name that appears under When Running The Task, Use The Following User Account. Click **Change User or Group** to select a different user account, if needed.

11. Choose an option:
    - Select **Run Only When User Is Logged On** to have the backup schedule task run when a user is logged on.
    - Select **Run Whether User Is Logged On Or Not** (recommended) to have the backup schedule task run without the need for the user to log on. The user you select in the previous step needs to have the LocalSecurityPolicy assignment "Log on as batch job" Windows permission.
12. In the Properties dialog, click **OK**. If you select Run Whether User Is Logged On or Not, enter the user's password.
13. Close the Task Scheduler dialog.

Restoring From Backup

> **Note:** When you restore the database from a backup, the backup files replace all the files in the GxP Admin Software database.

To restore the GxP Admin Software database from a backup:

1. On the computer desktop, double-click or locate and double-click **GxPAdminBackupTool.exe** to display the GxP Admin Backup Tool dialog.
2. In the **Restore** area, in the **Restore From** field, either enter the path to the location of the backup file or click to display the Browse For Folder dialog.
3. In the Browse For Folder dialog, select the backup file and click **OK**.
4. Click **Restore Now**.
5. Confirm that no other user is logged into the GxP Admin Portal Software or the SoftMax Pro GxP Software.

   > **Note:** Whenever you restore the database, you must confirm that no users are using the SoftMax Pro GxP Software or the GxP Admin Portal Software. Restoring while users are logged in may lead to inconsistent data.

6. Click **OK** in the message dialog. The History area displays the operation, status, operator, file name, start time, duration, and size of the backup file.
7. After a restore operation, check the recent audit entries for inconsistencies and make sure to document any inconsistencies accordingly.

Obtaining Support

Molecular Devices is a leading worldwide manufacturer and distributor of analytical instrumentation, software, and reagents. We are committed to the quality of our products and to fully supporting our customers with the highest level of technical service.

Our Support website, support.moleculardevices.com, has a link to the Knowledge Base, which contains technical notes, software upgrades, safety data sheets, and other resources. If you still need assistance after consulting the Knowledge Base, you can submit a request to Molecular Devices Technical Support.

You can contact your local representative or Molecular Devices Technical Support at 800-635-5577 x 1815 (North America only) or +1 408-747-1700.
In Europe call +44 (0) 118 944 8000.

To find regional support contact information, visit www.moleculardevices.com/contact.