Last Modified on 10/12/2026 11:52 am EDT

General Settings

Settings > General Settings > Company Information

Company Information: This information may be used throughout the system wherever heading and address info is needed.

Time Zone: This information may be used in various places throughout the system wherever timestamps are used.

Sales System Transaction Drill Down:

Settings > General Settings > Web. This is for use with the SGA Sales system only. This identifies the system (SGA Sales), source (SL), and URL path (client-specific) for drilling down from transactions in SGA Accounting directly to the registration detail in SGA Sales.

Authentication

Settings > General Settings > Authentication

Dft password expires every x number of days: If checked, the user must change their password regularly.

Warn x number of days before password expires: Warn the user a specified number of days before their password expires.

Allow user to change password after it expires: If this is not checked and a user's password expires, an administrator will need to log in and enable their user account.

Disable user account after x login attempts: If this is checked and a user's password expires, an administrator must log in and enable the user account. This is done from *Users > System Users*. Users will receive a message on the login screen when two or more login attempts remain before the account is disabled.

Require letters: Forces a more secure password.

Require numbers: Forces a more secure password.

Require special characters: Forces a more secure password.

Minimum number of characters: Set the minimum number of characters required for a user password.

Maximum number of characters: Set the maximum number of characters required for a user password.

Strict Message: Rules for creating a password based on the settings above.

Log out after _____ minutes of inactivity: This is a security setting that logs the user out if there is no activity in the web browser for a set number of minutes. If enabled, the SGA recommends a minimum of 60 minutes or more to prevent work loss. This setting may require clearing browser cookies to take effect.

Log out every _____ days: If enabled, this security setting logs users out after a set number of days. Clearing browser cookies may be required for this setting to take effect.

Clear SGA Cookies when browser closes: If enabled, this setting will clear all authentication cookies when the web browser being used to access SGA is closed. This will also log users out and delete Two-Factor Authentication timeout tokens (if enabled). This setting may require clearing browser cookies to take effect.

Use Google Drive and OAuth2 for reports and lists: Define the settings for using Google Drive Excel connection strings on reports. When set, connections can have Google accounts applied to them, and an Excel file can be selected from the Google Drive picklist.

(Two Factor Authentication does not apply to Pulse.)

Use Two-Factor Authentication: If enabled, users must enter an authentication code sent via email or SMS message to access SGA. A valid username and password or OAuth token are still required to log in. This is an all-or-nothing setting; it can not be applied to users selectively.

Use Two Factor Authentication for Windows: This setting applies only to the Legacy SGA Windows Application and is not used by SGA Web Accounting.

Use Device Authorization Timeout: If enabled, an SGA user can save a token that enables access to SGA without entering a 2FA authorization code. This token is user-specific and will expire after the period set in the **Device Authorization Timeout** field; SGA recommends that this be set to no less than 10 hours. This token is cleared when the web browser is closed if enabled by the **Clear SGA Cookies when browser closes** feature. Contact SGA Support for more information.

OAuth2 Login Providers: Users with administrator permissions will have access to this section to maintain their credentials and configuration when using OAuth for SSO login.

Excel Settings

Settings > General Settings > Excel Settings

This is where you can specify the properties of an Excel spreadsheet when something is exported to Excel. Reports exported using a report writer have their own Excel properties defined per report.

Page orientation: This determines whether a sheet will be portrait or landscape when printed. Using auto-determine will make a sheet portrait unless it overflows horizontally. In that case, it will be landscaped instead.

Initial save folder: The initial folder when saving or exporting to Excel, though you can change it at the time you export.

Gridlines: This exports with border lines the same color as the grid's lines, using Excel's borders. If this is checked, these lines will also print when the sheet is printed.

Bold headers and totals: Bold all headers as well as total lines.

Header line: Adds a horizontal line to separate the column headers from the rest of the grid.

Colors/shades: This option exports rows the same color as those in the grid. However, these colors will also print, so if you do not use a color printer, the print will be in a relative shade.

Black and white: This determines whether color printing is enabled on all printers. If you wish to disable color printing so no one can print in color, check this.

Password-protect all workbooks: This feature protects all workbooks exported to Excel so that the data cannot be modified unless a password is supplied.

Font: The font name and size of all data exported.

Print Settings

Settings > General Settings > Print Settings

This is where you can specify the properties in which reports are printed. Reports exported using a report writer have their Print properties, which are defined per report.

Page orientation: Determines if a sheet will be portrait or landscape when printing it.

Color: This determines whether color is enabled for all printers. If you wish to turn off color so no one can print in color, set this to black and white.

Gridlines: Prints gridlines the same color as the grid's lines.

Bold headers and totals: Bold all headers as well as total lines.

Header line: Adds a horizontal line to separate the column headers from the rest of the grid.

Colors/shades: This option prints rows the same color as those in the grid. If you don't use a color printer, it will print in a relative shade.

Margins: The default margins for sheets exported to Excel.

Font: The font name and size of all data exported.

Email Settings

Settings > General Settings > Email Settings

This defines the method by which you wish to send any emails in SGA.

Email Method: Choose whether to send emails through Microsoft Outlook or SMTP. SMTP is recommended if you have access to an SMTP server. Most companies do; you have to talk to your IT staff to find out. If you use Outlook, a warning message will be displayed every time you send an email through SGA, which is a nuisance.

Outgoing mail (SMTP): If you wish to use the email capabilities of SGA software, then you must specify an SMTP server through which to send email. If using this method, you may need to use your ISP's mail router to send mail outside your domain. Most servers require authentication to send outgoing mail outside your domain. If this is the case, enter the username and password as well.

From Administrator: This is the **From** address for all emails appearing in people's inboxes. If an invalid email address is entered, you will either get an error while mailing or an email will be sent to the **from address** as undeliverable.

Troubleshooting SMTP

If you are having trouble sending mail to an address outside your domain, you may need one or both.

- Change your SMTP server to be the mail router of your ISP.
- Specify a user and password for authentication.

If you get an error message saying it can't find the server, a firewall or antivirus software may be blocking your ability to send emails. The McAfee antivirus **VirusScan Enterprise** software will prohibit email sending by default. You need to add all email-sending executables to the **processes to exclude** the list found within the **Prevent Mass Mailing Worms from Sending Mail** rule within the **Antivirus Standard Protection** category within the **Access Protection Properties** within the **VirusScan Console**. Add SGA.exe to the list of executables.

For steps on adding a New From Email, click here.

Constant Contact (API Key, Access Token): This service is used only for marketing emails by the SGA Sales member management system. Contact SGA Support for assistance in setting up and enabling this service.

Mail Chimp (API Key): The SGA sales member management system uses Mail Chimp only for marketing emails. Contact SGA Support for assistance in setting up and enabling this service.

Twilio: Twilio is used for SMS (text) messages. If enabled, two-factor authentication codes are available in SGA. Twilio also sends SMS (text) messages within the SGA Sales system. Each client must set up their own Twilio account to enable this feature. Twilio collects a per-message fee. Contact Support for assistance with setting up and allowing this service.