Two Factor Authentication

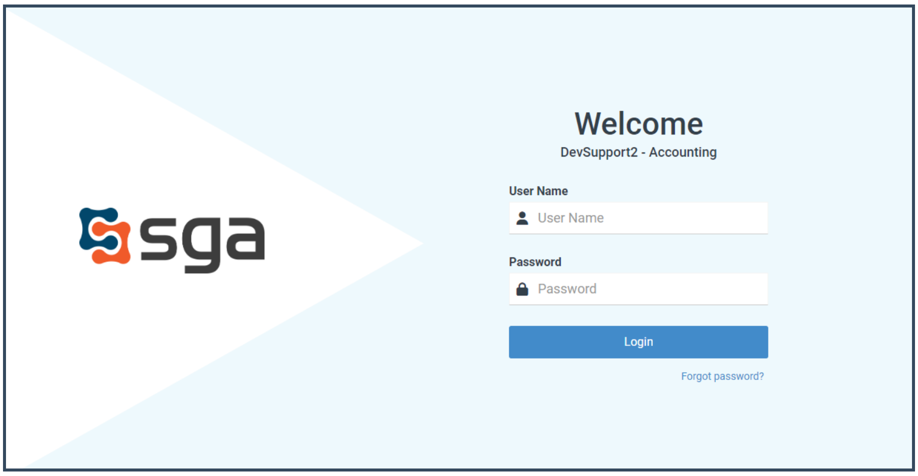
Last Modified on 01/02/2025 11:07 am EST

Two Factor Authentication

Two-Factor Authentication (2FA). SGA 2FA brings an added level of security by requiring two methods to verify identity. SGA 2FA requires that users not only know their username and password but also have access to an email account or SMS-enabled phone number associated with their username. SGA 2FA can also be set to authorize a device for access without requiring 2FA for a customizable period. 2FA protects against phishing, social engineering, and brute-force password attacks, and it secures your logins from attackers who exploit weak or stolen credentials.

How SGA Two Factor Authentication (2FA) Works:

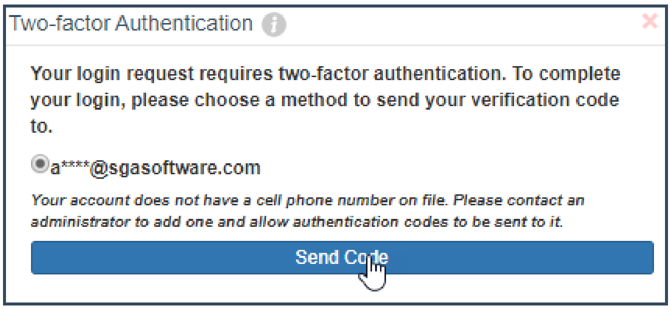
When SGA 2FA is enabled, users will log in with their username and password.



Users will then be asked how they would like to receive an authorization code by email or text.

NOTE: If only one contact method is available to the user, that method will be available.

A one-time code will be generated and sent to the location that was chosen when the user presses the “**Send Code”** button:



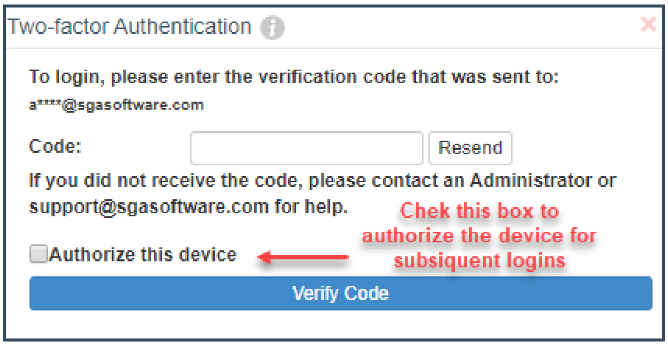
Your login request requires two-factor authentication. To complete your login, please choose a method to send your verification code to.

● a****@sgasoftware.com

Your account does not have a cell phone number on file. Please contact an administrator to add one and allow authentication codes to be sent to it.

This access code will need to be entered into the SGA dialog box.

If the user wants the device they’re currently using to be authorized for subsequent logins, they need to check the “**Authorize this Device**” box:



Two-factor Authentication

To login, please enter the verification code that was sent to:
a****@sgasoftware.com

Code:

If you did not receive the code, please contact an Administrator or support@sgasoftware.com for help.

□ Authorize this device

Chek this box to authorize the device for subsiquent logins

NOTE: *Your organization's SGA administrator sets the device authorization time limit. After reaching the time limit, the user must reauthorize the device to log in.*

SGA Two Factor (2FA) Prerequisites:

All users **MUST** have a unique email address and/or an SMS enabled (cellular, SMS enabled VOIP) associated with their user name.

Any users without an email or SMS-enabled phone number associated with their account cannot access SGA.

Setting Up 2FA:

NOTE: *This setting can only be enabled in SGA Web Accounting.*

SGA 2FA can be enabled in the ***Settings > General Settings > Authentication*** menu.

2FA Settings:

- Use Two-Factor Authentication
  - Enables Two-Factor Authentication for SGA Web
- Use Two-Factor Authentication for Windows
  - Enables Two-Factor Authentication for SGA for Windows
- Allow SMS Two-Factor Authentication

  *Enables 2FA codes via SMS **Requires Twilio Account**
- Allow Email Two-Factor authentication

  *Enables 2FA codes via Email

Use Device Authorization Timeout

- Allows setting of a number of Hours or Days to authorize a device to access SGA web accounting without requiring re-authorization via 2FA authentication. This authorization is for one user on one device and will not be carried to other devices or users.

For assistance setting up Two Factor Authentication, please contact SGA Support.

Important: These settings will apply to **ALL** users accessing SGA and can not be limited to only a subset of users.

All users **MUST** have a unique email address and/or an SMS enabled (cellular, SMS enabled VOIP) associated with their username, or they will not be able to access SGA.