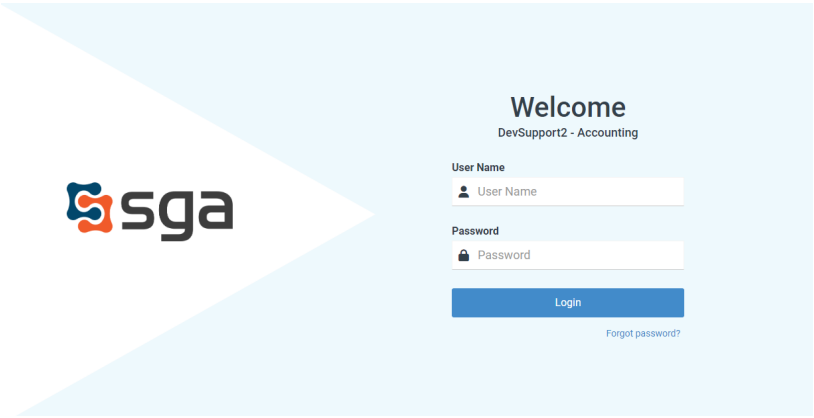
Two Factor Authentication

Last Modified on 05/18/2023 12:45 pm EDT

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 user name and password but also have access to an email account or SMS enabled phone number that is associated with their user name. SGA 2FA can also be set to authorize a device for access without requiring 2FA for a customizable period of time. 2FA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

How SGA Two Factor Authentication (2FA) Works:

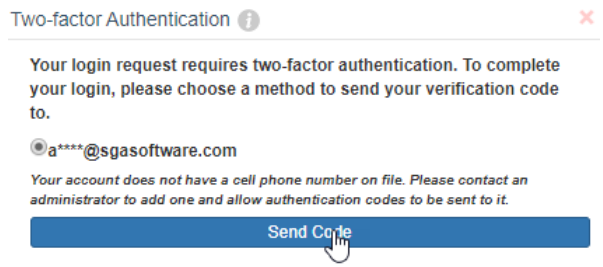
When SGA 2FA is enabled, users will log in with their user name and password.



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

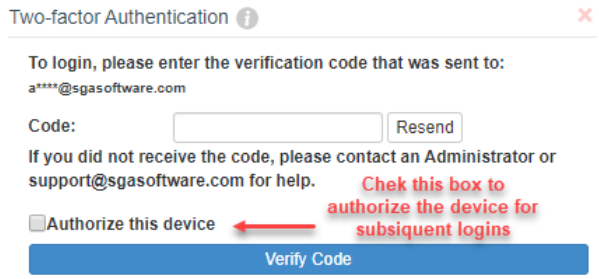
NOTE: If only one contact method is present for the user then only that method will be available.

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



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:



NOTE: The device authorization time limit is set by your organization's SGA Administrator. After the time limit is reached the user will be required to 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 will not be able to 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 be able to access SGA web accounting without requiring re-authorization via 2FA authentication. This Authorization is for one user on one device and will not carry to other devices or users.

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

Please Note:

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.