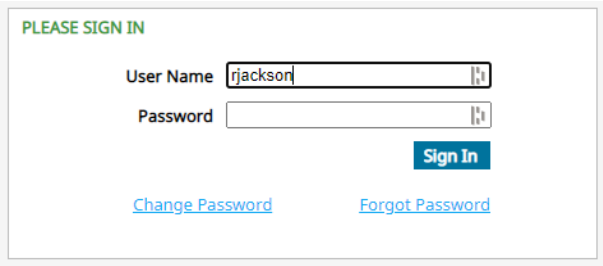
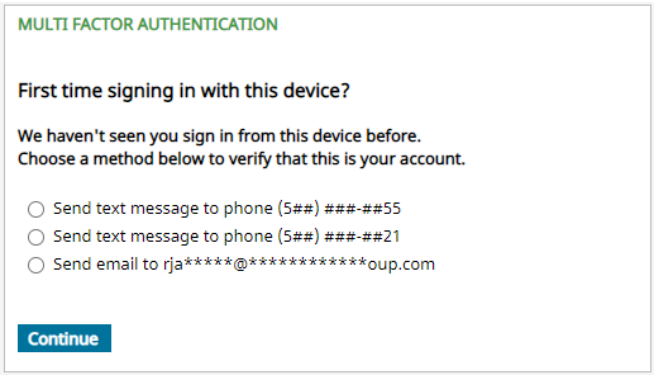
# Multi-Factor Authentication

For increased security, Rockingham has enabled Bluestone to require multi-factor authentication (also called 2-factor authentication) when users log into Bluestone. When enabled, users who access Bluestone from a new device will be required to choose a second, independent authentication method.




To authenticate, users have the option to receive their authentication code via SMS text message or email. By default, the authentication code is an alphanumeric sequence of 6 characters. For security purposes, if the authentication code is entered incorrectly 3 times in a row, the system will wait for 5 seconds before allowing the user to log in with a different code. Also, the SMS and email authentication code is only valid for 15 minutes.




On the next screen, the user must enter the authentication code received by either SMS text message or email.


Before verifying the authentication code, users have the option to select the "*Remember me on this device*" option. With this option, for the next 30 days, the user is only required to enter a password to login from this device.

If the authentication code has expired or has been lost, users that use SMS or email to receive their authentication code have the option to be sent another authentication code.