

Setting Your New Authenticator

Introduction

This manual provides step-by-step instructions for users to set their new password and second factor of authentication. Following these guidelines will help ensure your account remains secure and accessible. If you encounter any issues during the process, please contact your system administrator.

What Is an Authenticator Application?

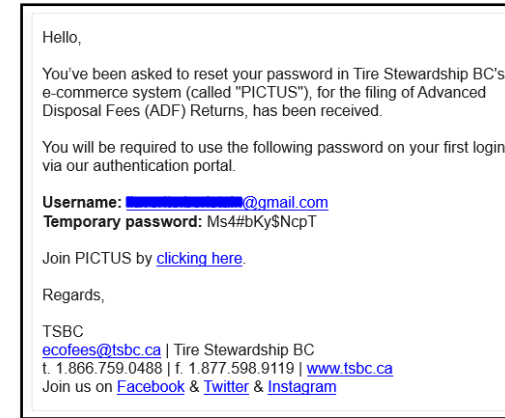
An authenticator application is a tool that generates time-based one-time passwords (OTPs) to provide an extra layer of security for online accounts through two-factor or multi-factor authentication (2FA/MFA). It is used to verify your identity when accessing the PICTUS Online platform. It helps protect your personal and organizational information from unauthorized access.

Before You Begin

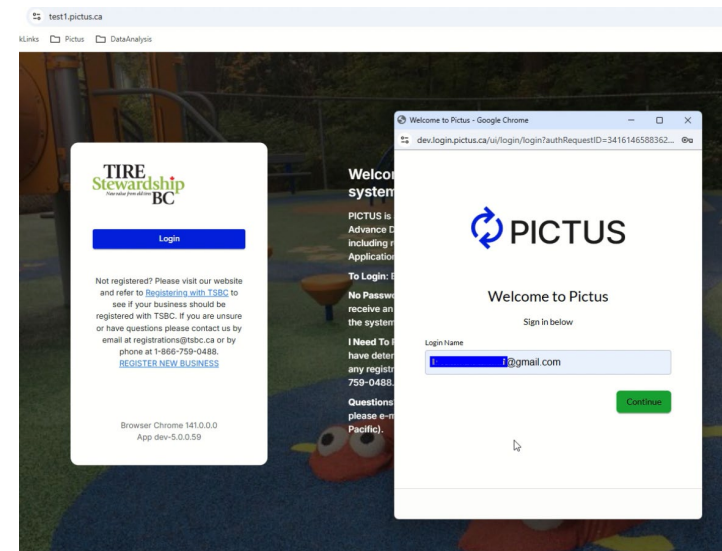
- Ensure you have access to your registered email.
- Choose a strong password that you have not used elsewhere.

Step-by-Step Guide

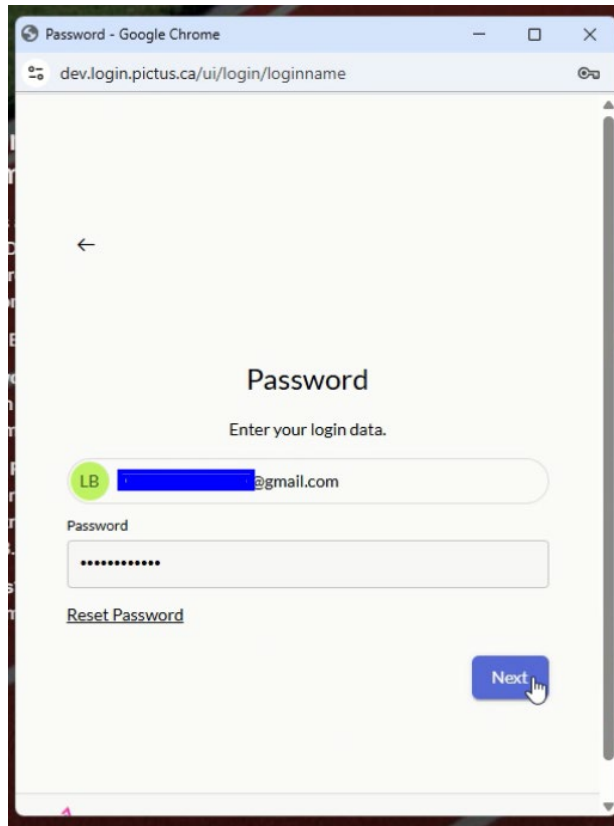
- 1) You will receive an email with subject: "Tire Stewardship BC - New authenticator password"
- 2) On the email click on the [click here](#) hyperlink.



- 3) The PICTUS Login page will be open, click on the Login blue button.
- 4) A pop-up window will open, enter your email and click on the Continue button.

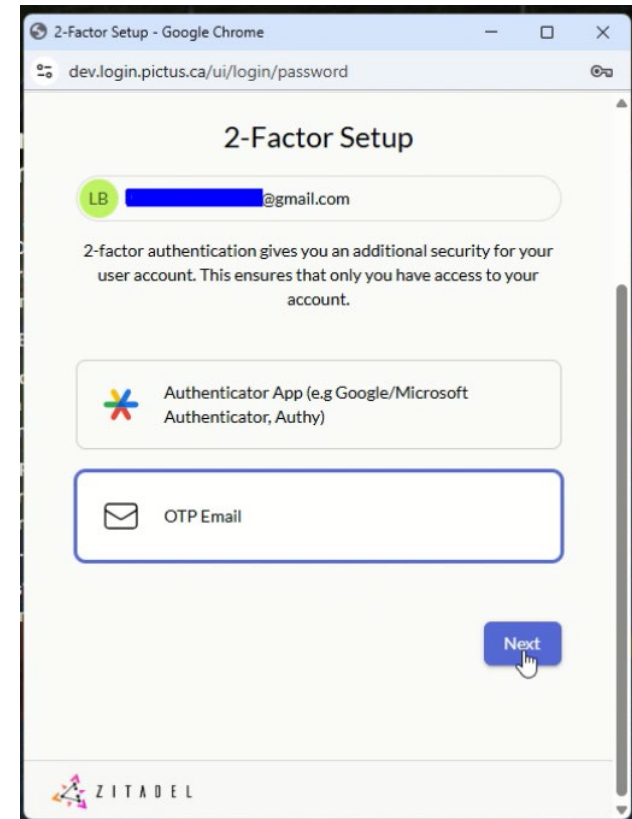


- 5) The system will request a password, copy the Temporary password on the email and paste it in the Password field.



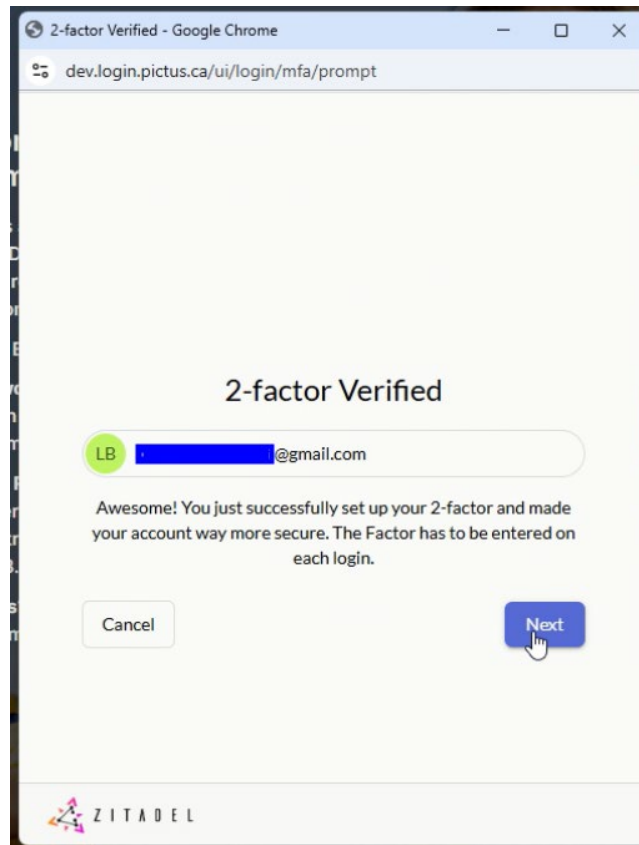
The screenshot shows a web browser window titled "Password - Google Chrome" with the URL "dev.login.pictus.ca/ui/login/loginname". The page has a light beige background. At the top left is a back arrow. The main heading is "Password" with the instruction "Enter your login data." below it. There is a text input field for the email address, which contains "LB [redacted]@gmail.com". Below this is a "Password" label and a password input field filled with dots. A link for "Reset Password" is located below the password field. A blue "Next" button is at the bottom right, with a mouse cursor hovering over it.

- 6) The system will request to select a 2-Factor of authentication. The first OTP Email option is the most common, select it and click the next button.



The screenshot shows a web browser window titled "2-Factor Setup - Google Chrome" with the URL "dev.login.pictus.ca/ui/login/password". The page has a light beige background. The heading is "2-Factor Setup". Below it is a text input field for the email address, containing "LB [redacted]@gmail.com". A paragraph explains: "2-factor authentication gives you an additional security for your user account. This ensures that only you have access to your account." There are two selection options: "Authenticator App (e.g Google/Microsoft Authenticator, Authy)" with a colorful star icon, and "OTP Email" with an envelope icon. The "OTP Email" option is highlighted with a blue border. A blue "Next" button is at the bottom right, with a mouse cursor hovering over it. The ZITADEL logo is at the bottom left.

- 7) A successful message is shown after the 2-Factor is Verified.
Click on the Next button.



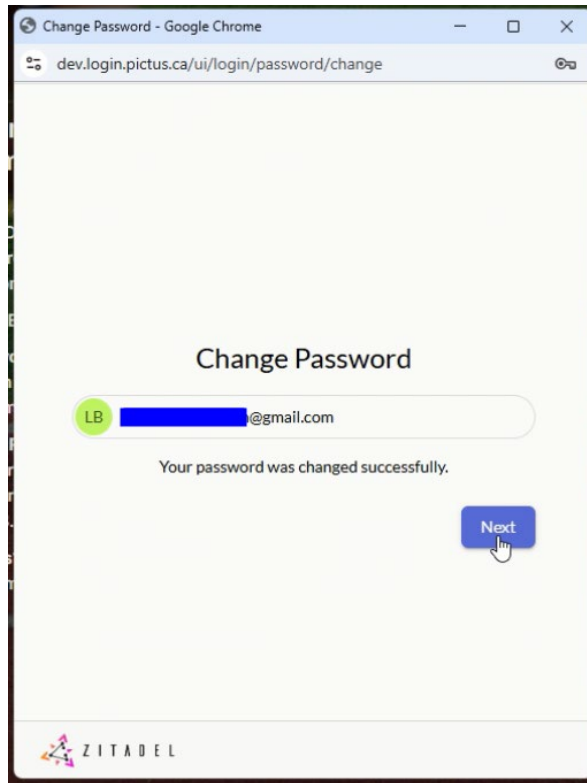
- 8) The new window will ask you for the old and new passwords.
a) The old password is the one on the email.

Username: [redacted]@gmail.com
Temporary password: Ms4#bKy\$NcpT

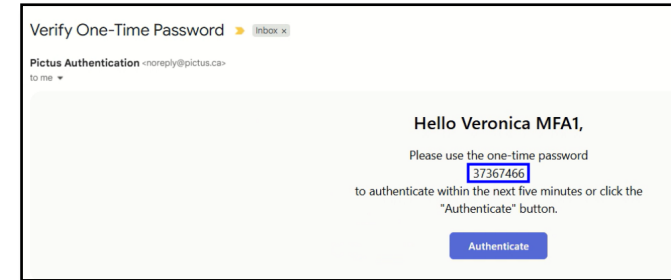
- b) Enter a new password that complies with the requirements listed on the screen.
c) Click the Next button to save the password.

A screenshot of a web browser window titled 'Change Password - Google Chrome'. The address bar shows 'dev.login.pictus.ca/ui/login/login'. The main content area has a heading 'Change Password' and a message: 'Change your password. Enter your old and new password.' Below the message are three input fields: 'Old Password', 'New Password', and 'Password confirmation'. To the right of these fields are six password requirements, each with a green checkmark: 'Must be at least 12 characters long.', 'Must be less than 70 characters long.', 'Must include an uppercase letter.', 'Must include a lowercase letter.', 'Must include a number.', and 'Must include a symbol.'. Below these requirements is a 'Next' button with a hand cursor icon. At the bottom left is a 'Cancel' button.

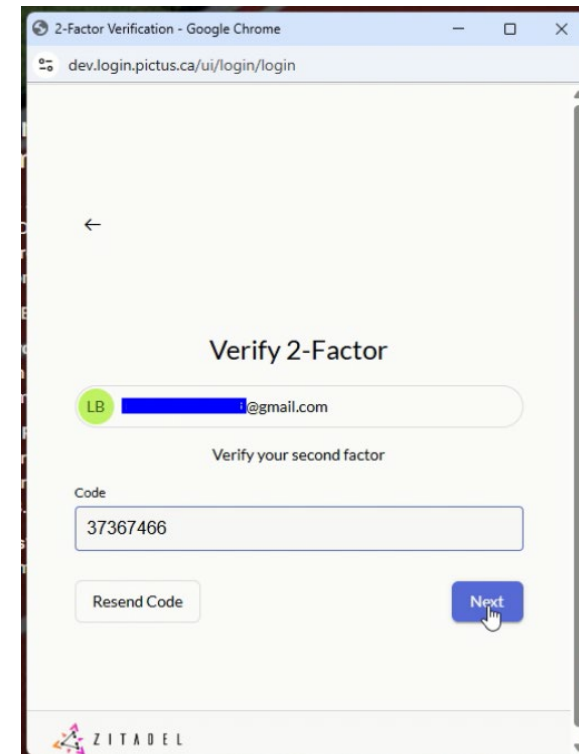
- 9) The screen will show the message: “Your password was changed successfully”.
- a) You will receive a confirmation email.
 - b) Click the Next button to log into PICTUS.



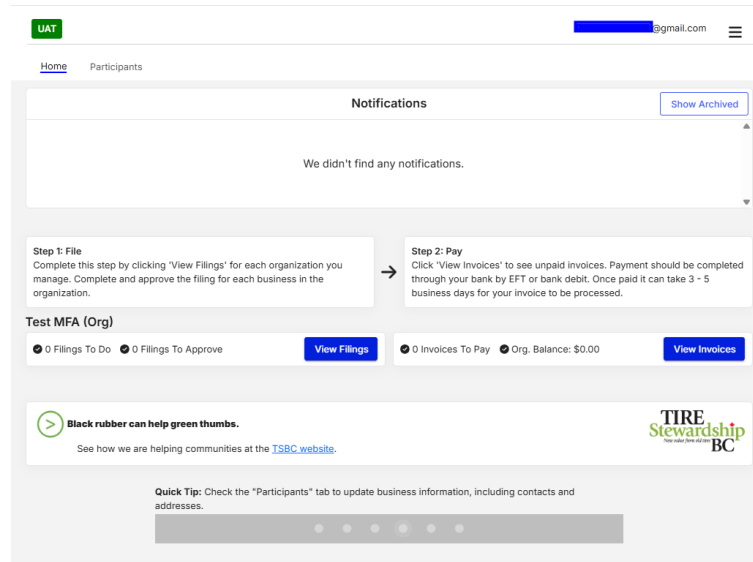
- 10) A 2-Factor of Authentication is required.
- a) Go to your email inbox, there should be a new email that contains the code.



- b) Copy the code and paste it on the pop-up window.
- c) Click on the Next button.



11) The PICTUS home page will be shown.



Troubleshooting

- If you forget your password, use the *Reset Password* feature on the login page.
- If you do not receive a verification code, check your spam folder or verify your contact information.
- Contact technical support if you experience persistent issues.

Appendix: Frequently Asked Questions (FAQ)

- **Q:** Can I use my old password as the new authenticator password?
- **A:** For security reasons, it is recommended to use a unique password that has not been used previously.
- **Q:** How often should I change my authenticator password?
- **A:** It is advisable to change your password every three to six months, or immediately if you suspect a security breach.
- **Q:** What should I do if I suspect my account has been compromised?
- **A:** Change your password immediately and contact the PICTUS support team.