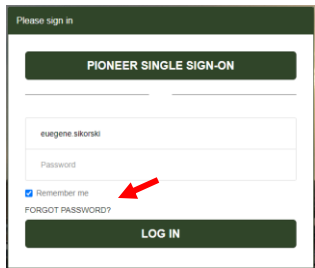


How to Reset Your Password and Setup Multifactor Authentication (MFA) for the First Time



To access information about your case, you must reset your password and set up multifactor authentication (MFA) for security purposes.

Your username is the email address on file for your account.

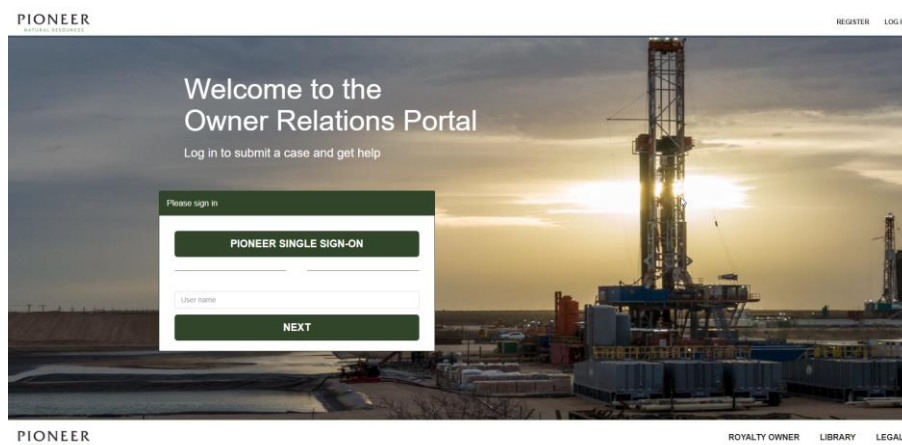
Accessing the Owner Relations Portal

The Owner Relations Portal is your one-stop shop to access your cases regarding division orders, changes of ownership, direct deposits, revenue inquiries etc. You can submit a new case, check the status on a case or update an existing case. You'll also be able to review your old cases.

Note: You must log in to the site to create or view your cases.

Try it: Access the Owner Relations portal

1. Open your internet browser and navigate to <https://ownerrelations.pxd.com>
2. The home page should appear, and you should be prompted to log in.



Resetting Your Password for the First Time

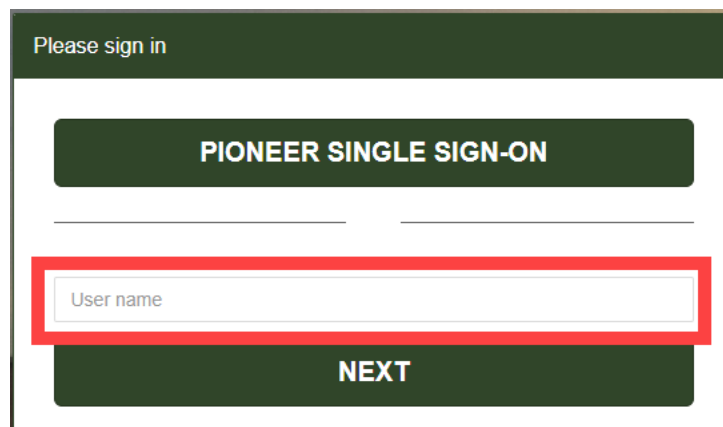
When accessing the site for the first time, you'll need to reset your password.

Your username is your email address on file. If we do not have your email address on file, please email **OwnerRelationsInquiry@pxd.com** so we can tie it to your account. This is the only way you can access your Owner Relations Portal online.

If you need help going through this document, please contact our Pioneer Help Desk at 1-877-969-3503, option 1.

Try it: Reset your password.

1. From the login page, enter your username*, which is your email address on file, and click **Next**.



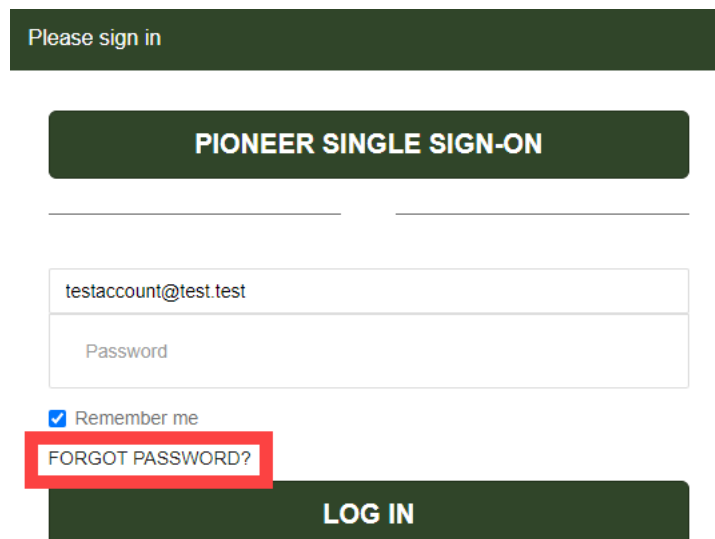
Please sign in

PIONEER SINGLE SIGN-ON

User name

NEXT

2. Click on the **FORGOT PASSWORD?** link located above the LOG IN button.



Please sign in

PIONEER SINGLE SIGN-ON

testaccount@test.test

Password

Remember me

FORGOT PASSWORD?

LOG IN

3. You will be redirected to the following page; enter your username, again, and click **Next**.

Identify Verify Reset

* Username [Next](#)

4. On the **Verify** screen, enter your email, and click **Next**.


Identify ✓ Verify Reset

Personal Data Verification

* Email [Next](#)

5. Once verified, an email will be sent containing instructions on how to reset the password.

Identify ✓ Verify ✓ Reset



An email has been sent to you providing instructions to reset your password

[Done](#)

- Click on the link in the email to access the **Reset Password** page. Follow the instructions on the screen to reset your password.

The screenshot shows a progress bar at the top with three stages: 'Identify' (checked), 'Verify' (checked), and 'Reset' (active). Below the progress bar is a 'Reset Password' form. The form includes a message 'Account is not locked', a 'New password' field with a strength indicator set to 'Great', and a list of requirements: Minimum 8 Characters, Maximum 40 Characters, At least 1 lowercase letter(s), At least 1 uppercase letter(s), At least 1 digit(s), and At least 0 Special Character(s). Below these is a 'Retype password' field with a 'Passwords must match' indicator and a 'Show passwords' checkbox. A 'Reset Password' button is located at the bottom right of the form.

- After you hit the **Reset Password** button, you will be redirected back to the Owner Relations homepage. Log in with your new password.

The screenshot shows the Pioneer Natural Resources Owner Relations Portal homepage. The page features a large background image of an oil rig at sunset. The header includes the Pioneer logo and 'NATURAL RESOURCES' on the left, and 'REGISTER' and 'LOGIN' on the right. The main content area has a large heading 'Welcome to the Owner Relations Portal' and a sub-heading 'Log in to submit a case and get help'. A sign-in form is overlaid on the page, containing a 'PIONEER SINGLE SIGN-ON' button, a text input field with 'testaccount@test.test', a password field with '*****', a 'Remember me' checkbox, a 'FORGOT PASSWORD?' link, and a 'LOG IN' button highlighted with a red border. The footer includes the Pioneer logo and 'NATURAL RESOURCES' on the left, and 'ROYALTY OWNER', 'LIBRARY', and 'LEGAL' on the right.

Setting Up Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA), also known as two-step verification, is a security requirement that users enter more than one set of credentials to access an instance. With MFA, each time you try to log in, you will be challenged for a second form of identification through a third-party authenticator application.



Or type in: FEXAMPLE ONLY#5

Try it: After resetting your password and logging in for the first time, you will be prompted to enable multi-factor authentication (MFA). Follow the instructions listed on the screen.

Enable multi-factor authentication(MFA)

[Learn more](#) [Postpone Setup](#)

Number of times MFA setup can be postponed is: 3

1. Download an authenticator app that supports Time Based One-Time Password(TOTP) on your mobile device.

[More Details](#)

2. Open the app and scan the QR code below to pair your mobile device



Or type in: FEXAMPLE ONLY#5

3. Enter the code generated by the Authenticator app below

6-digit code

Pair device and Login

1. Download a third-party authentication app that supports Time Based One-Time Password (TOTP) on your mobile device. An authenticator application is third-party software that generates temporary passcodes. You can use these passcodes along with your password to login into an instance that requires multi-factor authentication (MFA). Below are applications that are known to be compatible:

- Google Authenticator
- Microsoft Authenticator

- LastPass Authenticator
- Authy
- FreeOTP
- Duo
- Okta Verify

Note: *Other authenticators not listed might also be compatible but are not tested by ServiceNow.*

2. Open the application and scan the QR Code on the screen to pair your mobile device or type in the code that is shown under the QR code. This code is unique to your account. Do not scan the code in this document, as it is just an example.
3. The authenticator application will generate a 6-digit code. Enter this code on the screen and click on the **Pair device and Login** button.
4. MFA will then be enabled for your user account. Anytime you login, you will be prompted to enter the 6-digit code after entering your password.

Note: *You can postpone setting up MFA up to 3 times.*