RRC Access Management Process (RAMP)

Delegated Administrator Guide

Railroad Commission of Texas
Information Technology Services Division
June 2021

Table of Contents

Introduction

Overview

An RRC Access Management Process (RAMP) account allows you to have a single set of sign-in credentials for multiple RRC applications. At this time, you can only access the RRC CASES and PIPES Portal applications. In the future, other RRC applications will be accessible using RAMP.

There are two types of accounts in RAMP:

- **Delegated Administrator** - Creates and maintains Standard User accounts for those with their company who need to file forms and perform other work via applications available through RAMP. See the Becoming a Delegated Administrator section for more information.

- **Standard User** - Creates and submits filings and makes payments through applications available in the RAMP. See the RAMP User Guide for more information.
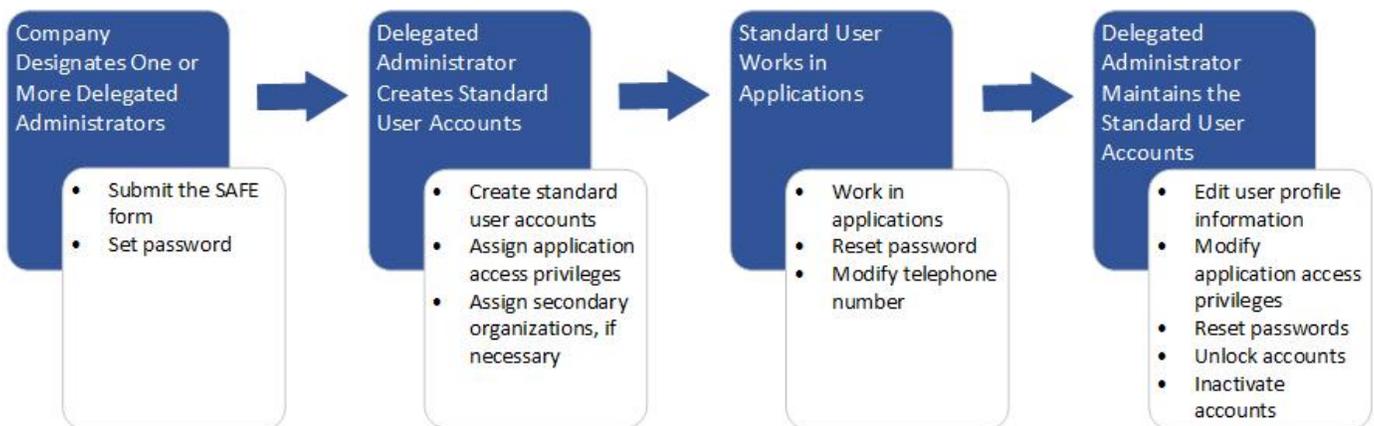
Getting an Account

Each company must have at least one Delegated Administrator. To become a Delegated Administrator, please complete the online Security Administrator Form – External (SAFE form). For more information, see the Becoming a Delegated Administrator section of this user guide.

If you need to become a Standard User, contact your company's Delegated Administrator.

NOTE: If you are not sure who is your company's Delegated Administrator, then send a request to the RRC at rrconline-security@rrc.texas.gov asking for a list of the Delegated Administrators for your company.

The graphic below shows the overall process for creating and managing RAMP accounts.

Company Designates One or More Delegated Administrators	Delegated Administrator Creates Standard User Accounts	Standard User Works in Applications	Delegated Administrator Maintains the Standard User Accounts
• Submit the SAFE form • Set password	• Create standard user accounts • Assign application access privileges • Assign secondary organizations, if necessary	• Work in applications • Reset password • Modify telephone number	• Edit user profile information • Modify application access privileges • Reset passwords • Unlock accounts • Inactivate accounts

NOTE: If you need to file on behalf of another company, contact your company's Delegated Administrator. They can assign any additional companies as secondary organizations. See the Filing on Behalf of Another Company section of this user guide.

Delegated Administrators

What is a Delegated Administrator?

Delegated Administrators manage Standard User accounts for their company. All companies must have at least one Delegated Administrator. To become a Delegated Administrator, you will need to complete and submit the online Security Administrator Form – External (SAFE form).
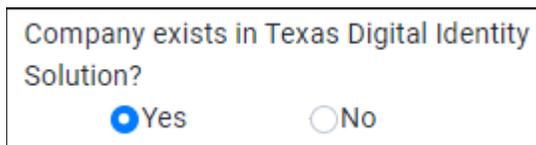
Delegated Administrators can perform the following tasks:

- Create Standard Users
- Modify Standard User Accounts
- Reset a Standard User's Password
- Unlock a Standard User's Locked Account
- Inactivate a Standard User
- Request the Promotion of a Standard User to a Delegated Administrator
- Request the Demotion of a Delegated Administrator to a Standard User
- Reset Their Own Password
- Change Their Own Phone Number
- Assign secondary organizations to Standard Users, allowing them to file on behalf of other companies.

Becoming a Delegated Administrator

You must submit the online Security Administrator Form – External (SAFE) form to request to become a Delegated Administrator for your company. You will receive an email confirmation from RRC once your request has been approved.

1. Navigate to the online SAFE form.

2. Indicate whether or not your company exists in the Texas Digital Identify Solution (RAMP).

- Select **Yes** if your company had a P5 Number on February 23, 2021, **or** already has at least one Delegated Administrator for RAMP.

- Select **No** if your company did not have a P5 Number on February 23, 2021, **or** does not have at least one Delegated Administrator for RAMP.

NOTE: If your company is an Oil & Gas, Pipeline, or Gas Utility company, your company will need to obtain a P5 number before you can become a Delegated Administrator.

3. Select the *Company Type*. You can choose from the following:

```
Select Company Type
● Oil & Gas/Pipelines/Gas Utility
○ Alternative Fuels
○ Surface Mining
○ Consultant/Lawyer
```

- Oil & Gas/Pipeline/Gas Utility

- Alternative Fuels

- Surface Mining

- Consultant/Lawyer

4. Enter the *Company Name*.

NOTE: If your company has a P5 Number, the name you enter should match the name on your P5 paperwork exactly.

5. Enter your company's *Organization Identifier*.

NOTE: The *Organization Identifier* must be six digits. Therefore, leading zeros should be included if needed.

- If your company is an Oil & Gas, Pipeline, or Gas Utility company, enter your P5 Number.

- If your company is an Alternative Fuels company, enter your AFS Company Number.

- If your company is a Surface Mining company, enter your Surface Mining Company ID.

- If you are a consultant or lawyer, enter the Identification Number previously sent to your company.

NOTE: If you are setting up your law or consultant firm for the first time in RAMP, you will not be prompted to enter an Organization Identifier. The Organization Identifier will be assigned when the Delegated Administrator request is approved. You will receive an email notification with the Organization Identifier.

6. Enter your *Email Address*. Email notifications related to signing in via RAMP, such as password reset emails, will be sent to this address.

7. Enter your *First Name*.

8. Enter your *Last Name*.

9. If applicable, enter your *Suffix*.

10. Enter your *Cell Phone Number*.

NOTE: The first time the you sign in from a device, you will be required to complete multi-factor authentication for that device. If you select text message or phone call authentication, an authentication code will be sent to this number. You will be prompted to enter the authentication code during the sign in process.

11. Read the *Certification* and select the **I agree with these restrictions** check box.

CERTIFICATION

I declare, under penalties prescribed in Sec. 91.143, Texas Natural Resources Code, that I am authorized to make this Security Administrator Designation, that it was prepared by me or under my supervision and direction, and that the information stated herein is true, correct, and complete, to the best of my knowledge and belief.

I further declare that all electronic filings made pursuant to this designation will be in the manner prescribed by the Railroad Commission of Texas and will be compatible with the software, equipment, and facilities required by the Railroad Commission of Texas. All electronic filings will comply with any required procedures for participation in electronic filing.

I further declare that any filings which I make on behalf of another party will be made only if I have been authorized by that party to file on its behalf and I acknowledge that any filings made on behalf of an operator by me as an independent third party which are subsequently determined by the Commission to be made without the operator's authorization may result in the suspension or revocation of this Security Administrator Designation and/or the right to make any filings at the Commission on behalf of other parties.

☐   I agree with these restrictions.

12. Type your name in the text box to sign.

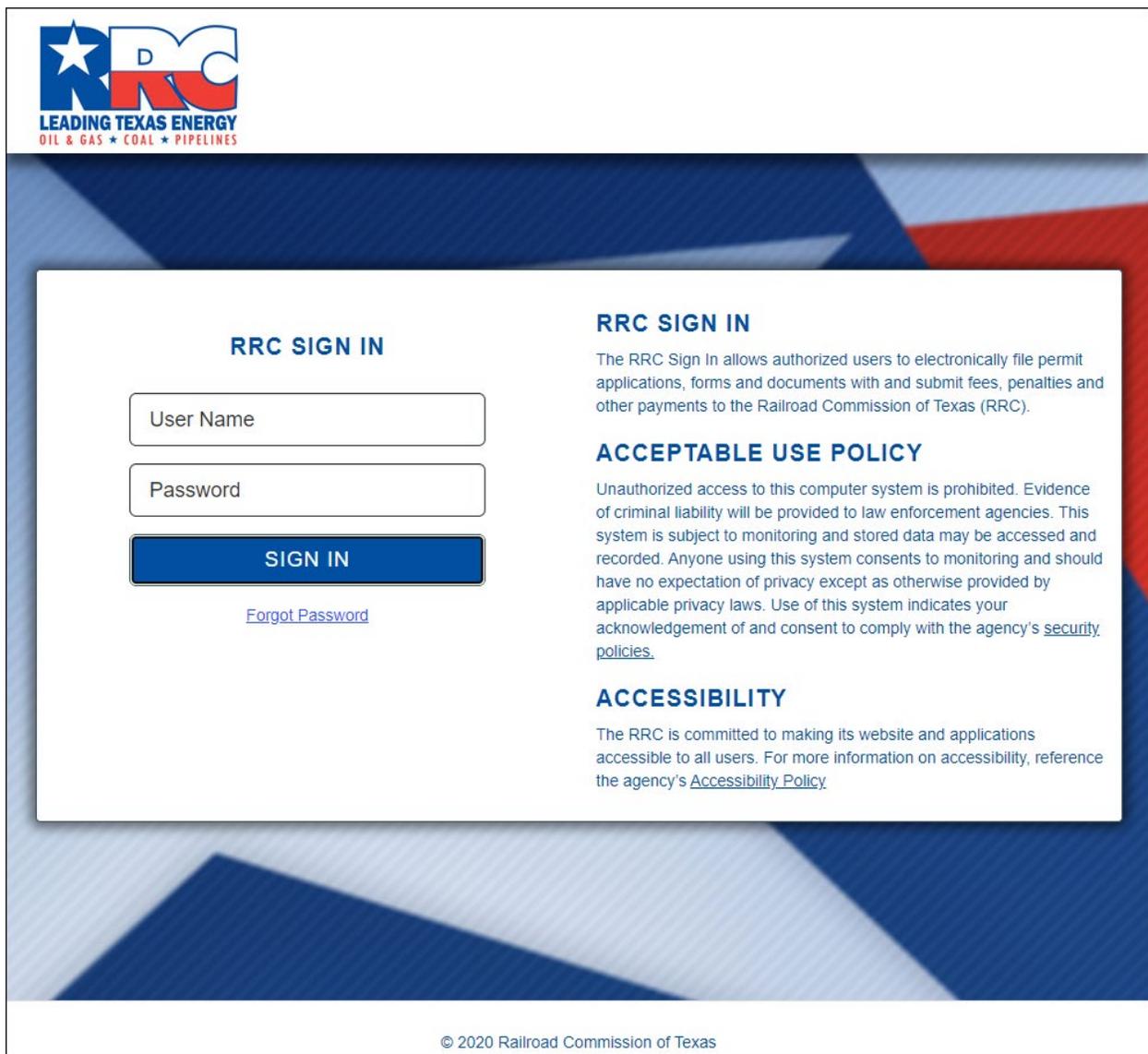Type in your name to sign

13. Click **Sign Up** [Sign Up] .

If your request is approved, you will receive a confirmation email from RRC that allows you to set your password. You can then use your email address and new password to sign into the RAMP Dashboard and applications available through RAMP.

Signing In

As a Delegated Administrator, you can sign into the RAMP Dashboard to create Standard Users and perform other tasks.

IMPORTANT: Unauthorized access to this computer system is prohibited. Evidence of criminal liability will be provided to law enforcement agencies. This system is subject to monitoring and stored data may be accessed and recorded. Anyone using this system consents to monitoring and should have no expectation of privacy except as otherwise provided by applicable privacy laws. Use of this system indicates your acknowledgement of and consent to comply with the agency's security policies.

1. Navigate to the RAMP Dashboard sign-in page.

2. Enter the email address associated to your account.

3. Enter your password.

4. Click **Sign In**.

5. If it is the first time you have signed in from your device, you will be asked to perform a multifactor authentication.

    a. Choose to receive an authentication code by text/SMS, phone call, or email.

RRC SIGN IN

Where would you like your one-time passcode sent?

◉ Text/SMS me the code at *** *** 8-5974
○ Call me at *** *** 8-5974
○ Email me the code at ***********rc@yopmail.com

SEND OTP

    b. Click **Send OTP**. An authentication code is sent by text/SMS, phone call, or email.

    c. Enter the authorization code.

RRC SIGN IN

A six-digit number has been sent to *** *** 8-5974

One Time Passcode

SUBMIT

RESEND

    d. Click **Submit.**

    e. Select **Yes** to save the device to your profile.

RRC SIGN IN

Would you like to save this device to your profile?

◉ Yes
○ No

SIGN IN

f.   Click **Sign In**.

Creating Standard Users

After receiving the confirmation email from RRC and setting your password, you can create Standard Users for your company.

1.   In the RAMP Dashboard, click the ☰ button in the top left corner and select **User** from the left pane. A list of your company's users displays.

2.   To create a standard user, click the **New User** button. The *New user* dialog box displays.
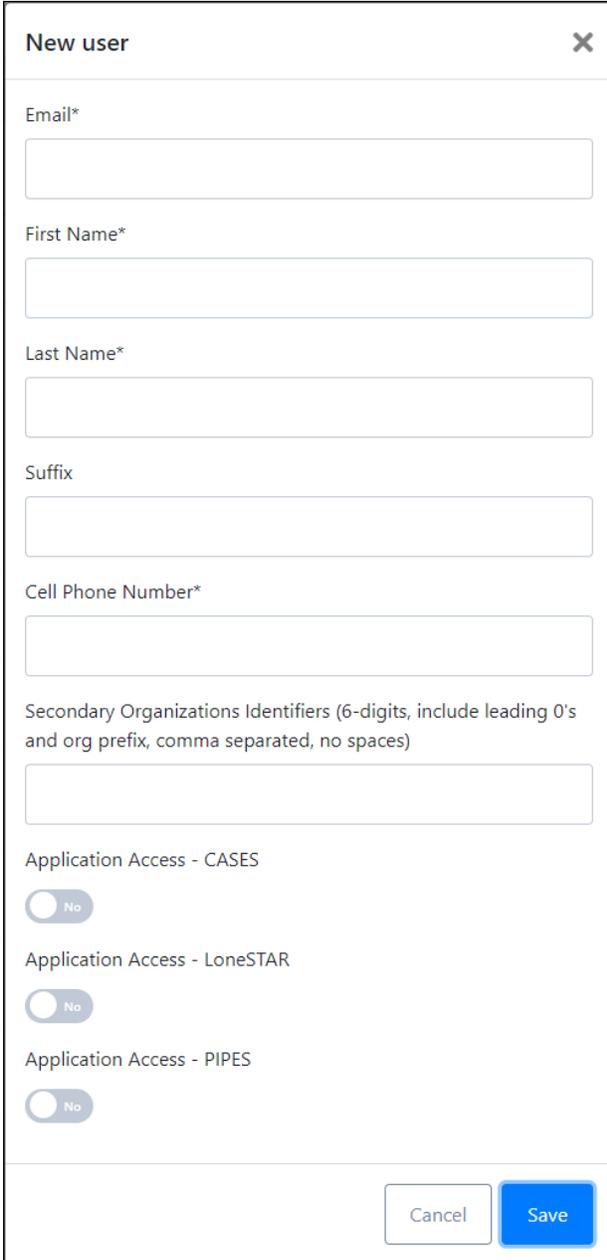
3.   Complete the following fields in the *New user* dialog box.

a. **Email:** Enter the user's email. The user will use this email to sign in. Email notifications related to signing in through RAMP, such as password reset emails, will be sent to this address

b. **First Name:** Enter the user's first name.

c. **Last Name:** Enter the user's last name.

d. **Suffix:** If applicable, enter the user's suffix.

e. **Cell Phone Number:** Enter the user's cell phone number.

> **NOTE:** The first time the user signs in from a device, they will be required to complete multi-factor authentication for that device. If they select text message or phone call authentication, an authentication code will be sent to this number. They will be prompted to enter the authentication code during the sign in process.

f. **Secondary Organizations Identifiers:** If the user will file on behalf of other companies, enter the RRC organizational identifiers, including the prefix, for those companies (e.g., P-5 Number).

> **NOTE: 1)** The Organization Identifier's prefix (i.e., RR (Oil & Gas, Gas Utility, and Pipeline companies), CL (Consultant or Law Firm), AF (Alternative Fuels companies), or SM (Surface Mining companies)) will need to be included as part of the Secondary Organization Identifier. For example, if the Organization Identifier is 111111 for an Oil & Gas company, enter RR-111111. **2)** The Organizational Identifier must be six digits. Therefore, leading zeroes should be included if needed.

g. **Application Access:** Select the toggle for each RRC application to which the user should be given access.

> **NOTE:** At this time, you can only assign access to the RRC CASES and PIPES Portal applications. In the future, other RRC applications, including LoneSTAR, will be accessible through RAMP.

4. Click **Save**. The new Standard User will receive a confirmation email that allows them to set a password.

> **NOTE:** There may be a short lag after clicking the *Save* button. Do **not** click the *Save* button twice. Wait several seconds for the request to process.

Searching for a Standard User

As a Delegated Administrator, you can search for a specific Standard User at your company.

1. In the RAMP Dashboard, click the ☰ button and select **User** from the left pane. The *User* page displays.
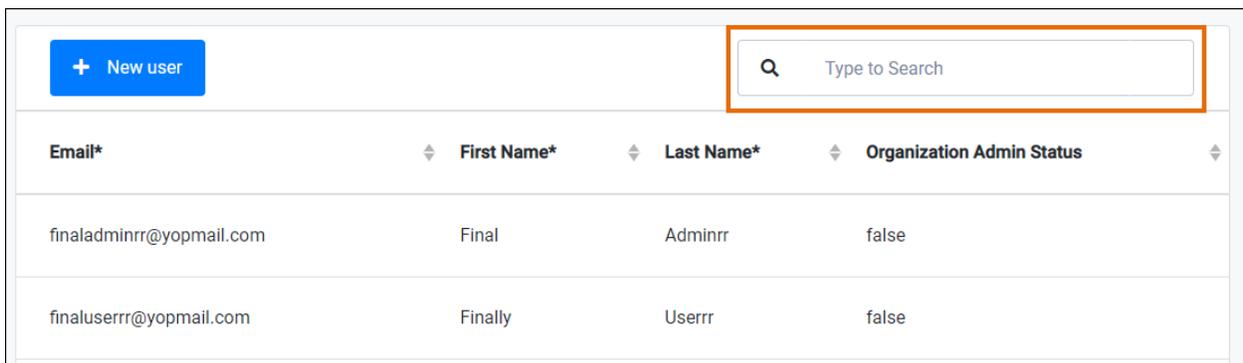
Email*	First Name*	Last Name*	Organization Admin Status
finaladminrr@yopmail.com	Final	Adminrr	false
finaluserrr@yopmail.com	Finally	Userrr	false

2. In the Search box in the upper left corner, enter one of the following for the user:

   a. Email

   b. First Name

   c. Last Name

3. Press **Enter**. Users whose email, first name, or last name begin with the specified search criteria display in the search results. Both Delegated Administrators and Standard Users with your company display in the search results.

Modifying a Standard User

As a Delegated Administrator, you can edit the profile information for Standard Users in your company and change their access privileges to the applications available through RAMP.

Modifying a Standard User's Profile

As a Delegated Administrator, you can modify a Standard User's profile information.

1. In the RAMP Dashboard, search for the user.

2. Click the row of the user you need to modify. Their user profile information displays.

3. Modify one or more of the following user attributes:

   - First Name

   - Last Name

   - Suffix

   - Email Address

   - Cell Phone Number

   - Secondary Organization Identifiers (See the Filing on Behalf of Another Company section of this user guide for more information on assigning secondary organizations.)

   - Application Roles (See the Modifying a Standard User's Access Privileges section of this user guide for more information on assigning application roles.)

   IMPORTANT: Do **not** modify the following fields on a user's account page: *Status, Account Locked Time, Admin submitting for promotion, Admins description of promotion, Remove Admin submitting for promotion, Admin Submitting for demotion, Reason for demotion, Promotion workflow flag*, and *Demotion workflow flag*.

   These fields are used by the RAMP system and should not be directly modified by a user.
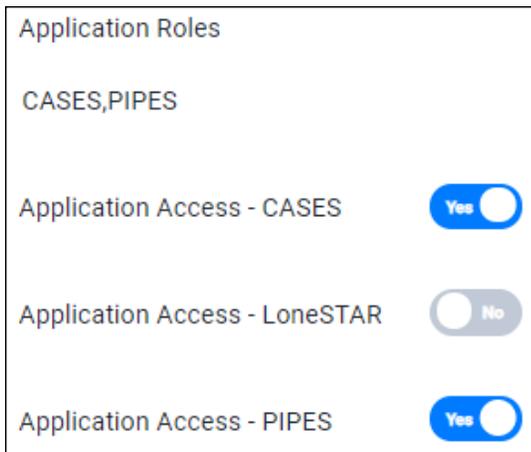
4. Click **Save**.

   NOTE: There may be a short lag after clicking the *Save* button. Do **not** click the *Save* button twice. Wait several seconds for the request to process.

Modifying a Standard User's Access Privileges

As a Delegated Administrator, you can add or remove access privileges to specific applications for a Standard User.

1. In the RAMP Dashboard, search for the user.

2. Click the row of the user you need to modify. Their user profile information displays.

3. In the *Application Roles* area, select or deselect the toggles for application access as appropriate.
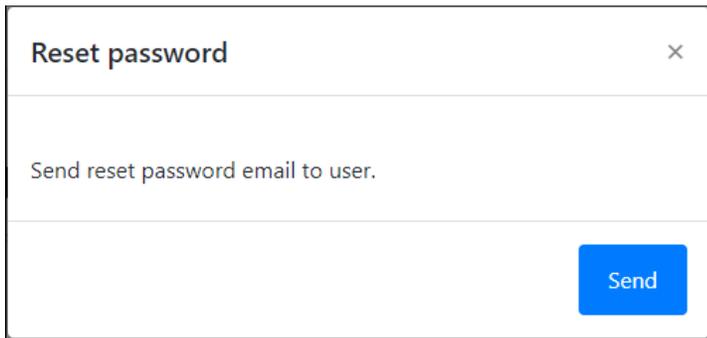
4. Click **Save**.

Resetting a User's Password

As a Delegated Administrator, you can reset the password of a Standard User and other Delegated Administrators in your company.

1. In the RAMP Dashboard, search for the user.

2. Click the row of the user whose password you need to reset. Their user profile information displays.

3. From the *Actions* drop-down list, select **Reset password**.
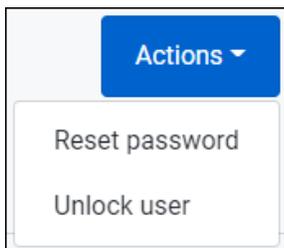
The *Reset password* dialog box displays.

4. Click **Send**. The Standard User receives a password reset email.

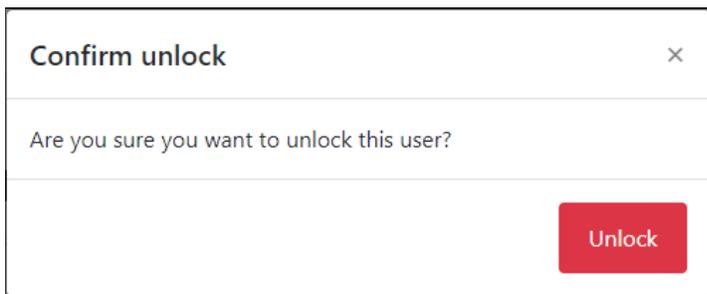## Unlocking a Standard User's Account

A user will be locked out of their account if they use incorrect sign in credentials five times in a row. As a Delegated Administrator, you can unlock the accounts of Standard Users and other Delegated Administrators in your company.

NOTE: If you need your Delegated Administrator account unlocked, contact the RRC at rrconline-security@rrc.texas.gov.

1. In the RAMP Dashboard, search for the user.

2. Click the row of the user whose account you need to unlock. Their user profile information displays. The *Account Locked Time* field will display the time when the account was locked.

3. From the *Actions* drop-down list, select **Unlock user**.
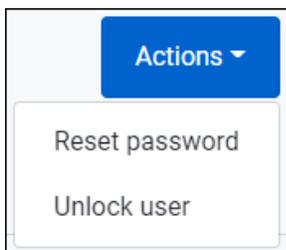
The *Confirm unlock* dialog box displays.

4. Click **Unlock**. The Standard User's account is unlocked.
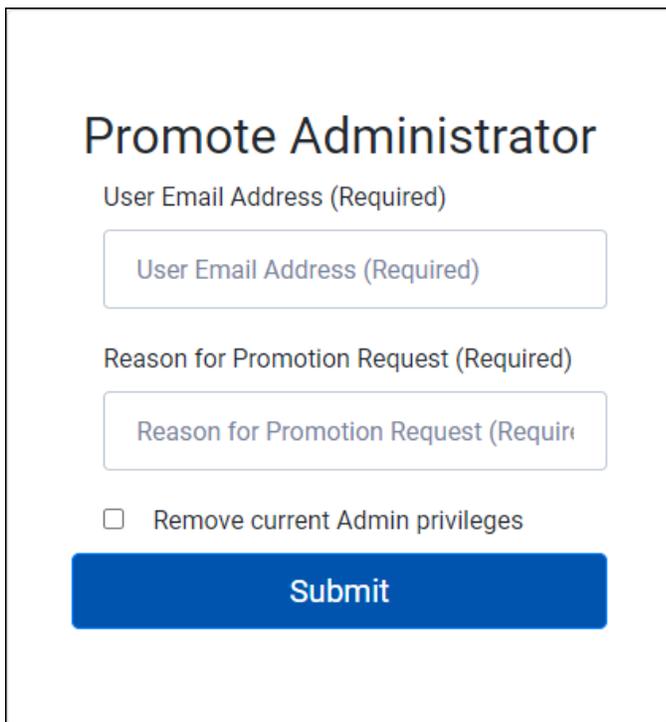
Inactivating a Standard User

As a Delegated Administrator, you may need to inactivate a Standard User's account if they leave your company or no longer need access to RRC applications. To inactivate a Standard User in your company, contact the RRC at rrconline-security@rrc.texas.gov.

The *Status* of the user should display as *inactive* after they have been inactivated.

Requesting the Promotion of a Standard User to a Delegated Administrator

As a Delegated Administrator, you can request that a Standard User in your company receive Delegated Administrator privileges.

1. In the RAMP Dashboard, click the ☰ button and select **Promote Administrator** from the left pane. The *Promote Administrator* screen displays.

> ### Promote Administrator
>
> User Email Address (Required)
>
> | User Email Address (Required) |
>
> Reason for Promotion Request (Required)
>
> | Reason for Promotion Request (Require |
>
> ☐ Remove current Admin privileges
>
> **Submit**

2. Enter the email of Standard User who needs Delegated Administrator privileges.

3. Enter the reason you are assigning the user Delegated Administrator privileges.

4. If you need Delegated Administrator privileges removed from your own account following approval of the promotion request, select the **Remove current Admin privileges** checkbox. **You can only select this option when your company already has at least one additional Delegated Administrator.**

5. Click **Submit**. A *Task created* dialog box displays.

> **NOTE:** There may be a short lag after clicking the *Submit* button. Do **not** click the *Submit* button twice. Wait several seconds for the request to process.
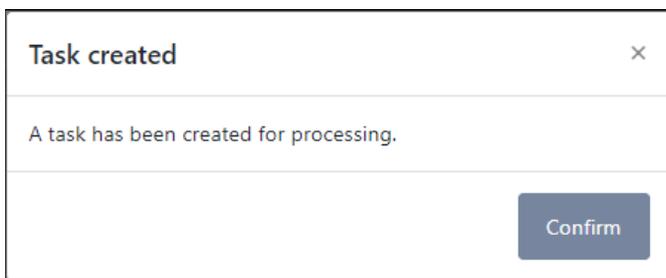
> **Task created**   ✕
>
> A task has been created for processing.
>
> **Confirm**

6. Click **Confirm**.

The user being promoted will receive a task to accept the Delegated Administrator Certification Statement. (There is one exception to this workflow. If the user has been promoted and demoted in the past, they will not receive the Delegated Administrator Certification Statement task.)

Once the user accepts the certification, the RRC will review and approve or reject the request. When the promotion request is approved, both you and the user will receive an email notification.

NOTE: If you requested that your Delegated Administrator privileges be removed, you will also receive an email notification when your privileges are removed.

Requesting the Demotion of a Delegated Administrator to a Standard User

As a Delegated Administrator, you can request that another Delegated Administrator in your company be demoted to a Standard User.

1. In the RAMP Dashboard, click the ☰ button and select **Demote Administrator** from the left pane. The *Demote Administrator* screen displays.
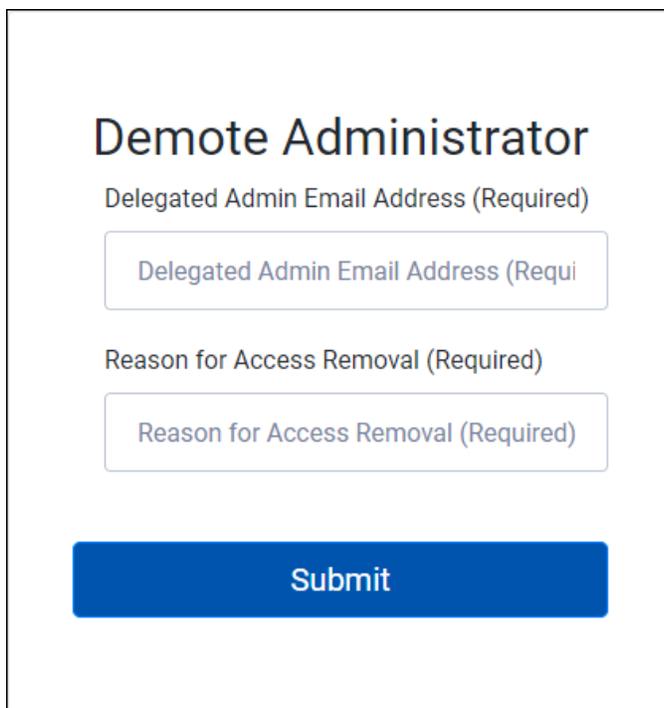
Demote Administrator

Delegated Admin Email Address (Required)

> Delegated Admin Email Address (Requi

Reason for Access Removal (Required)

> Reason for Access Removal (Required)

Submit

2. Enter the email of the Delegated Admin who needs to be demoted to a Standard User.

3. Enter the reason you are removing the user's Delegated Administrator privileges.

4. Click **Submit**. A *Task created* dialog box displays.

NOTE: There may be a short lag after clicking the *Submit* button. Do **not** click the *Submit* button twice. Wait several seconds for the request to process.

Task created   ✕

A task has been created for processing.
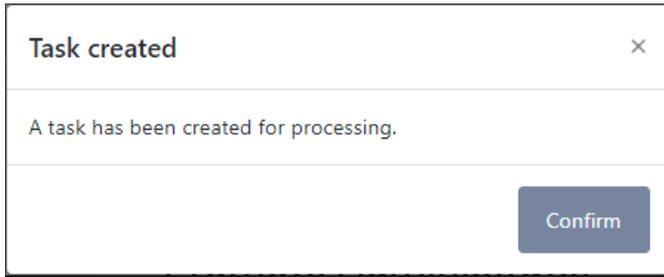
[Confirm]

5. Click **Confirm**. When the request is approved by the RRC, both you and the user will receive email notifications.
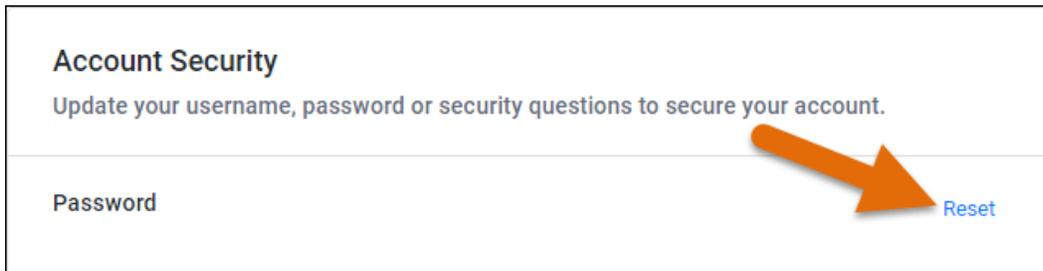
Resetting Your Password

As a Delegated Administrator, you are required to change your password at least every 90 days. You will receive an email notification before the 90-day deadline. If you do not change your password by the deadline, your account will be locked.

1. Log in to the RAMP Dashboard.

2. Click your name in the top right corner.

Jane Tester ▼

Profile

Sign Out

3. Select **Profile**.

4. In the *Account Security* area, select **Reset** in the *Password* row**.**

Account Security
Update your username, password or security questions to secure your account.

Password   Reset

The *Password* area expands.

5. Enter your *Current password*.

6. Enter your *New password*.

7. Click **Save password**.

If your account is locked because you do not change your password within the 90-day timeframe, contact the RRC at rrconline-security@rrc.texas.gov for assistance.

Changing Your Phone Number

As a Delegated Administrator, you can change your own phone number in your profile information. This phone number can be used for multi-factor authentication the first time you log in from a device.

1. Log in to the RAMP Dashboard.

2. Click the **Edit Your Profile** button.
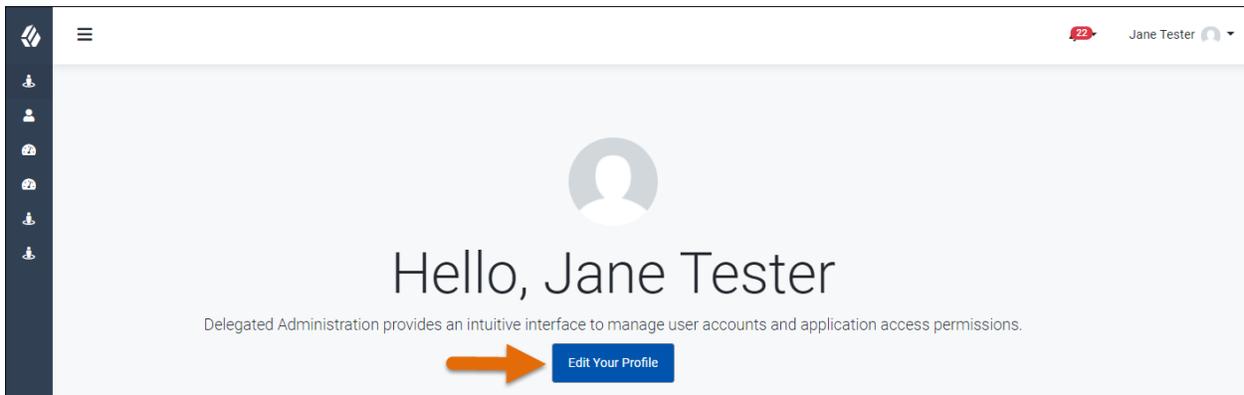
3. Enter the correct phone number in the *Cell Phone Number* field.

NOTE: The *Terms Agreed* and *Signed Certification* fields also display on this page. Do **not** modify these fields.

4. Click **Save Changes**.

Filing on Behalf of Another Company

Consultants, attorneys, and other non-operators may need to file on behalf of another company. Also, in some instances, an operator's employees may need to file on behalf of a related company, such as a subsidiary.

As a Delegated Administrator, you can add secondary organizations to your company's Standard User accounts to allow them to file on behalf of the secondary organization.

Adding a Secondary Organization for a Standard User

1. In the RAMP Dashboard, search for the user.

2. Click the row of the user you need to modify. Their user profile information displays.

3. Enter the organizational identifier for the company for which the user needs for in the *Secondary Organizations Identifiers* field. Include the prefix for the organization identifier.

16

Secondary Organizations Identifiers (6-digits, include leading 0's and org prefix, comma separated, no spaces)

- For Oil and Gas, Pipeline, or Gas Utility companies, enter the P5 Number. The prefix is "RR," so the number will be in the following format: RR-111111.

- For Alternative Fuels companies, enter the AFS company number. The prefix is "AF," so the number will be in the following format: AF-111111.

- For Surface Mining companies, enter the Surface Mining company ID. The prefix is "SM," so the number will be in the following format: SM-000111.

Enter commas between multiple organization identifiers, but do not space between commas. Multiple organizations would be in the following format: RR-111111,SM-000111.

NOTE: The Organizational Identifier must be six digits. Therefore, leading zeroes should be included if needed.

4. Click **Save**.