User States

and the effect of various user actions

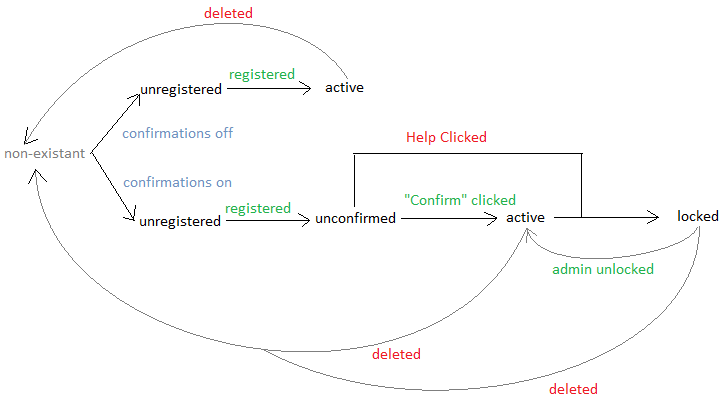
# Introduction

## User States

The user state refers to the mode that the user’s account is in. The four options are:

1. non-existent
2. unregistered
3. unconfirmed
4. active
5. locked

If the “Account Confirmations” checkbox is left unchecked on the user onboarding page, then “unconfirmed” is not a valid state



## User Actions

1. User attempts to see email content through a personalized link
2. Login attempt w/ wrong password
3. Login attempt w/ correct password
4. “Forgot my password” pressed
5. “Reset password” email link pressed.
6. “Help! – I didn’t create this account” pressed to lock account
7. “Confirm – Create Account” pressed
8. “Register Now” link pressed

# ACTION = user attempts to see email content through a personalized link

#### STATE = non-existent

Show a simple page with an error message: “The user <username> could not be found on the system.”

#### STATE = unregistered

Show the registration page. Then if confirmations are off, show the content; else if confirmations are on, show the user a message telling them to check their email for an account creation confirmation.

#### STATE = unconfirmed

Show a simple page with an error message: “*Sorry, your account is not activated. In order to confirm your identity, you must open the “Account Confirmation” email sent to* [*foo@bar.com*](mailto:foo@bar.com) *and click the “Confirm” link. I lost my confirmation email; send me another.”*

#### STATE = active

If the user is logged in, show them the content. If not, show them the login page until the log in and then show them the content.

#### STATE = locked

Show a simple page with an error message: “This account has been locked down by someone – probably you. If this account should be unlocked, contact an administrator.”

# ACTION = user attempts to see email content through a generic link

If generic links are being used, then we cannot tell which user is clicking on the link form their inbox, we can only tell which user is currently logged in. If no user is currently logged in, the person who clicked the link should be redirected to the login page in which case the “login attempt” action scenarios can be followed. The user should be redirected to the desired content after they log in assuming they have permission.

If a user *is* logged in, the result will differ based on whether or not the logged in account was a sender or recipient of the given email. If they are (if they have permission), then the email content will be rendered. If they do not have permission, then the email content will not be rendered. They will be shown a “You do not have permission to this content” message instead.

#### STATE = non-existent

See above

#### STATE = unregistered

See above

#### STATE = unconfirmed

See above

#### STATE = active

See above

#### STATE = locked

See above

# ACTION = Login attempt w/ wrong password

A login attempt with an incorrect password should never reveal information about the users that do or do not exist on the system. For example, if someone attempts to log in as an unregistered, unconfirmed, or locked user, the system should not reveal through an error message that the user is unregistered, unconfirmed, or locked out unless the person making the login attempt can actually prove they are the user they claim they are (either by typing in the password, using a private link, or having access to the user’s email account).

#### STATE = non-existent

Show the error message “Invalid Credentials”.

#### STATE = unregistered

Show the error message “Invalid Credentials”.

#### STATE = unconfirmed

Show the error message “Invalid Credentials”.

#### STATE = active

Show the error message “Invalid Credentials”.

#### STATE = locked

Show the error message “Invalid Credentials”.

# ACTION = Login attempt w/ correct password

#### STATE = non-existent

This action is impossible in this state. There is no correct password.

#### STATE = unregistered

This action is impossible in this state. There is no correct password.

#### STATE = unconfirmed

Show a simple page with an error message: “*Sorry, your account is not activated. In order to confirm your identity, you must open the “Account Confirmation” email sent to* [*foo@bar.com*](mailto:foo@bar.com) *and click the “Confirm” link. I lost my confirmation email; send me another.”*

#### STATE = active

Forward the user to their homepage (inbox or admin homepage – either way)

#### STATE = locked

Show them an error message “This account has been locked down by someone – probably you. If this account should be unlocked, contact an administrator.”

# ACTION = “forgot my password” pressed

#### STATE = non-existent

Right now the system tells the user in the browser that a user by the given username cannot be found on the system. This behavior is acceptable for now since most other sites I tested behaved this way, but in the future, we should probably change this to email the typed-in email addr whether or not we find it on the system – that way people will not be able to gather data about accounts that are not associated with one of their email addresses.

#### STATE = unregistered

User is sent a reset password link.

#### STATE = unconfirmed

User is sent a reset password link.

#### STATE = active

User is sent a reset password link.

#### STATE = locked

User is sent a reset password link.

# ACTION = “reset password” email link pressed.

#### STATE = non-existent

Show a simple page with an error message: “The user <username> could not be found on the system.”

#### STATE = unregistered

Unregistered users should not be able to get password reset emails, but they may have an email in their inbox from before their account was deleted and then re-created through by being on-boarded. If so, when they press it, it should take them to the registration page with a warning message explaining why.

#### STATE = unconfirmed

The user will not be shown the reset password page; they will be show the error message: “*Sorry, your account is not activated. In order to confirm your identity, you must open the “Account Confirmation” email sent to* [*foo@bar.com*](mailto:foo@bar.com) *and click the “Confirm” link. I lost my confirmation email; send me another.”*

#### STATE = active

After they reset their password, they will be logged in and redirected to their homepage.

#### STATE = locked

The user will not be shown the reset password page; they will be show the error message: “This account has been locked down by someone – probably you. If this account should be unlocked, contact an administrator.”

# ACTION = “Help! – I didn’t create this account” pressed to lock account

#### STATE = non-existent

Show a simple page with an error message: “The user <username> could not be found on the system.”

STATE = unregistered  
Unregistered users should not be able to get account confirmation emails, but they may have an email in their inbox from before their account was deleted and then re-created through by being onboarded. If a user clicks this link, even though the user should not be able to have it, the account should transition to the “locked” state with an appropriate success message.

STATE = unconfirmed

The account should transition to the “locked” state with an appropriate success message.

#### STATE = active

The account should transition to the “locked” state with an appropriate success message.

#### STATE = locked

The account should remain in the locked state; they will be show the warning message: “This account has already been locked.”

# ACTION = “Confirm – Create Account” pressed

#### STATE = non-existent

Show a simple page with an error message: “The user <username> could not be found on the system.”

#### STATE = unregistered

An informational message saying “You cannot confirm the activation of your account before you register” should be shown. The registration page should be shown and the registration process should be followed in the normal manner.

STATE = unconfirmed  
A success message telling them that their account is now active should be shown on the login page where their email address is pre-populated.

#### STATE = active

An informational message should appear telling the user that their account is already activated – shown on the login page with the username prepopulated if the user is logged out, else on the user’s homepage.

#### STATE = locked

The account should remain in the locked state; they will be show the error message: “This account has been locked down by someone – probably you. If this account should be unlocked, contact an administrator.”

# ACTION = “Register Now” link pressed

#### STATE = non-existent

Show a simple page with an error message: “The user <username> could not be found on the system.”

#### STATE = unregistered

The user should be taken to the registration page and allowed to register.

#### STATE = unconfirmed

The user should be shown the message “*This account has already been registered and now needs to be activated. In order to confirm your identity, you must open the “Account Confirmation” email sent to* [*foo@bar.com*](mailto:foo@bar.com) *and click the “Confirm” link. I lost my confirmation email; send me another.”*

#### STATE = active

The user should be shown the message “*This account has already been registered” on their homepage if logged in and the login page otherwise.*

#### STATE = locked

The user will not be shown the registration page; they will be show the error message: “This account has been locked down by someone – probably you. If this account should be unlocked, contact an administrator.”