kareo
a tebra company

CHECKLIST

Two-Factor Authentication (2FA) Pre-Activation

Kareo's Two-Factor Authentication (2FA) is an opt-in security measure to add another layer of protection from costly cyber attacks.

Only System Administrators can enable 2FA. It is enabled at the account level and enabled for all users for all practices under the account. We recommend System Administrators complete the following steps to prepare for the launch of 2FA in January 2023.

1 Ensure email and phone numbers are valid for System Administrators

The System Administrator is responsible for enabling/disabling 2FA and unlocking users' accounts. Having access to the platform to manage these critical functions is essential.

We highly encourage all System Administrator accounts to set up their accounts correctly so multiple admins can support and resolve any issues within the account.

Avoid a single point of failure by ensuring at least 2 System Administrators are set up correctly in the account.

Access User Settings

1. Hover over the User icon and click on Practice Settings. The Practice Settings page opens.
2. Click User Settings. The User Settings page opens.

Edit System Administrators Account

1. Click Edit to the right of the system administrator user's name. The Edit User page opens.
2. Make any necessary changes to the user's account information:

   E-mail: Enter a valid email address to allow the System Administrator to receive email notifications from Kareo.

   Phone Number: Phone Number: Enter a valid phone number that can receive SMS messages to allow the customer admin user to receive notifications from Kareo.

3. Click Save User when finished. Advise the user to log out and log back in to view changes made to their account.

Please note:

+ Once saved, the user will use the updated email address and phone number within the Kareo platform when prompted.

Ensure that all System Administrator email addresses and phone numbers are valid and that they can receive messages from the Kareo Platform when necessary

2 Create an Emergency Access Account

The Emergency Access feature allows users to request admin permissions in an emergency. We recommend your practice has multiple users authorized to request access in the event the customer admin is unavailable.

Please note:

+ This is recommended but optional. The System Administrator must authorize users to request Emergency Access to Kareo through their account settings.

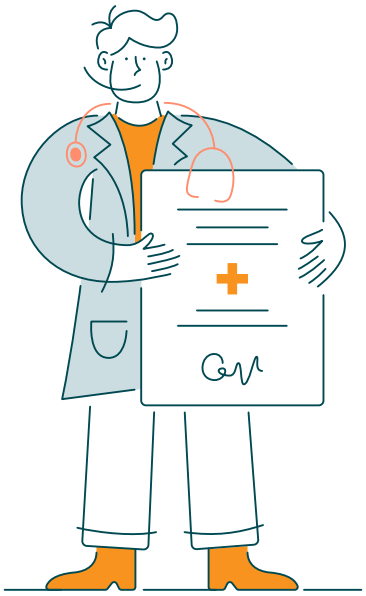
Access User Settings

1. Hover over the User icon and click on Practice Settings. The Practice Settings page opens.
2. Click User Settings. The User Settings page opens.

Edit System Administrators Account if Needed

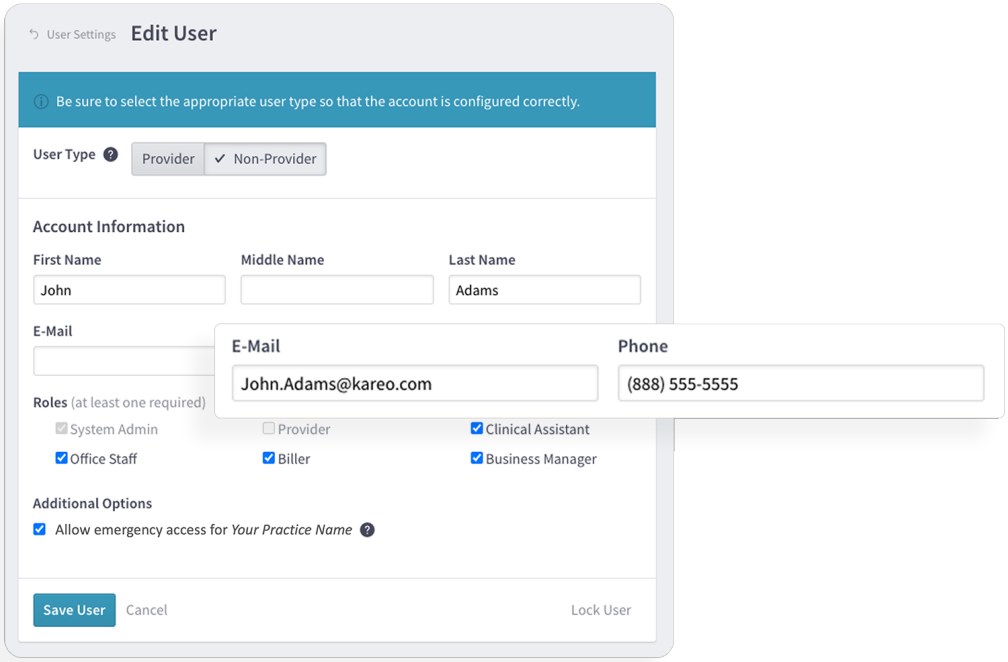
1. Click Edit to the right of the user's name. The Edit User page opens.
2. Make any necessary changes to the user's account information:
   + Navigate to additional options in the User Account edit view. Scroll down to "Additional Options". Click on the "Allow emergency access for (Practice)" box and ensure the information is correct in the fields.
3. Click Save User when finished.

Allow Emergency Access



3 Ensure all user emails and phone numbers are valid

2FA authenticates a user via SMS or email using the phone number and email address on file.
To view users' email and phone numbers on file, navigate to User Settings.
Practice settings > user settings > update all of their users
Update emails and phone numbers through the user's account on the Platform or Desktop Application (PM).



Please note:

+ For accounts with multiple practices: If a user is subscribed to a practice where the Kareo account has 2FA enabled as well as a practice where the Kareo account does not have 2FA enabled, then the user will be prompted to authenticate with 2FA when signing on to the 2FA enabled practice and will bypass the 2FA process when signing into the non-2FA enabled practice. If the user has authenticated once to a 2FA enabled practice, then they will not be required to authenticate again with 2FA when accessing a different 2FA enabled practice.
+ A user will be unable to update their email or phone number during the 2FA authentication step and risk being locked out.

System Administrator to confirm all user email and phone numbers are valid

kareo
a tebra company

Notes and Considerations

System administrators are ultimately responsible for unlocking and ensuring that their users are able to access their accounts.

Common 2FA scenarios that could result from improper set up:

+ Issues with logging in.
+ Users forget the phone number/email address that exists in their User Setting for 2FA.

Guideline:

If the user cannot access the platform, the System Administrator is responsible for unlocking the user accounts. Kareo's support team will not be able to unlock a user.

Additional Resources

Update User Email Help Article

Edit, Lock, or Unassign User Account Help Article

Web User Roles Help Article

Edit Provider User Account Help Article

Request Emergency Access Help Article

Navigate Emergency Access