Lockbox

R360+ Member Setup Admin User Guide

Use this guide to learn more about **Receivables 360+ Member Setup.**

For questions about this guide, please reach out to your Fifth Third relationship team or contact our Commercial Support Center at 866-475-0729, Monday through Friday, 7 a.m. to 10 p.m., ET.

August 2026

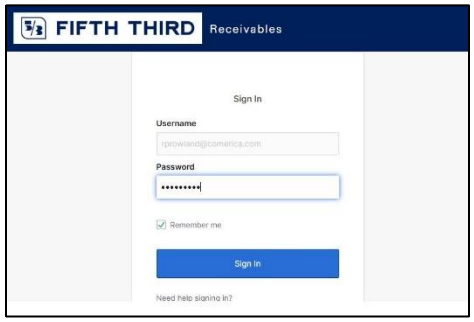
Member Setup

Receivables360+ (R360+®) is the archive made available to you for the Wholesale Lockbox image search and reporting capabilities during the migration period. It is accessed through a secure URL website. This guide covers the customer admin (user add, deletes and modifications) functions so you and your team can access the lockbox data and images.

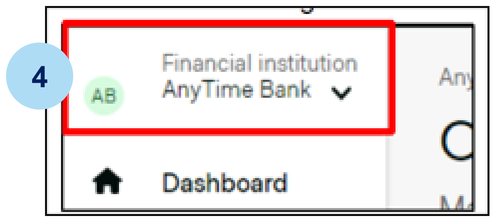
New members (users) can be set up by anyone that has access to the Members tab of Admin setup. The current company admin will be set up by Fifth Third Bank and that person can set up individual users within your company. Users should be created at the highest level of the Organization as needed, which will give them access to all lower levels of the organization. Organizations with multiple lockboxes will be able to see each individual lockbox underneath the corporation level. Care should be taken when creating users and assigning which lockboxes they have access to. There is a parent / child relationship for all lockbox accounts. Users can be set at the parent level meaning they will have access to all lockboxes or users can be set up for only specific lockboxes at the child level. Your company admin can add, modify or delete users. To add or remove a company admin, please contact the Commercial Support Center at 866-475-0729.

NOTE: Application-level access is provided by the administrator of the organization.

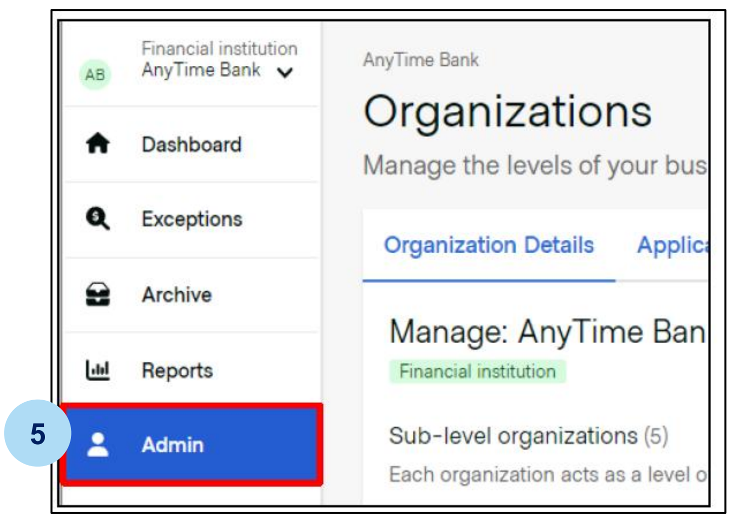
1. As a company admin, the bank will set up the account and send an email notification to activate the account. Clicking on the link within that email will prompt set up multi-factor authentication and establish a unique password for the account. Follow the on-screen prompts (see appendix).
2. As the admin for your business, open your browser, and navigate to https://payments.deluxe.com/receivables?brandingID=FifthThird
3. Enter email address, password and authenticate as the screen prompts.



4. Select the organization level where this user should be created from the navigation menu on the left side of the screen.

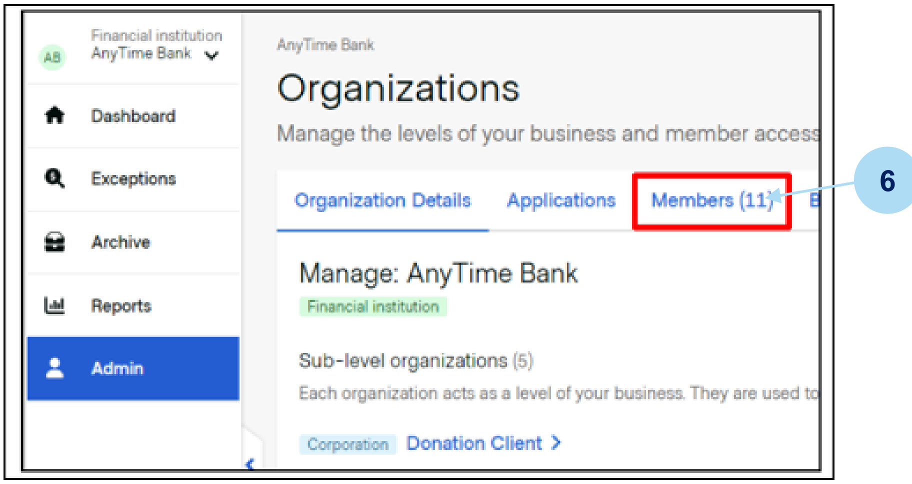


5. Select the **Admin** menu. The **Organization details tab** displays.

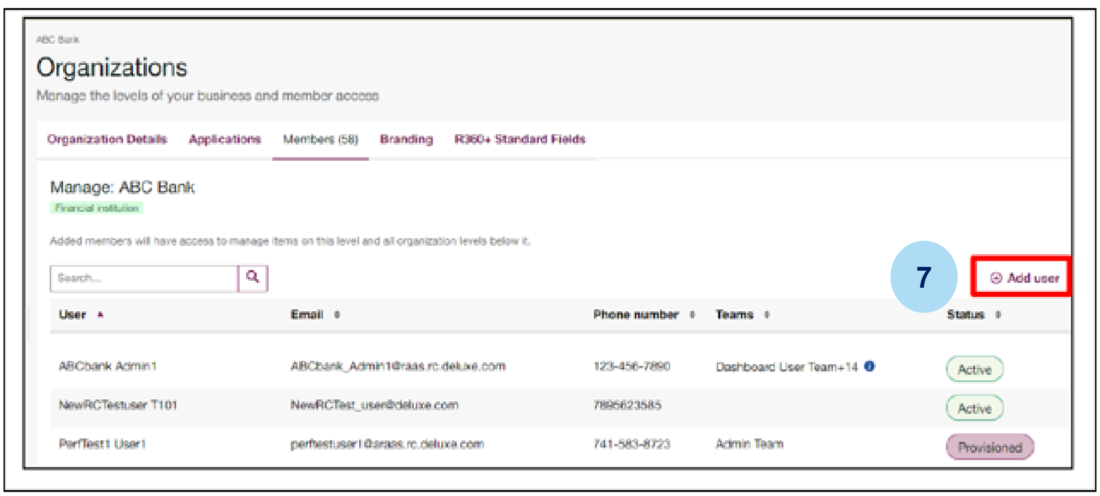


6. Select the **Members** tab.

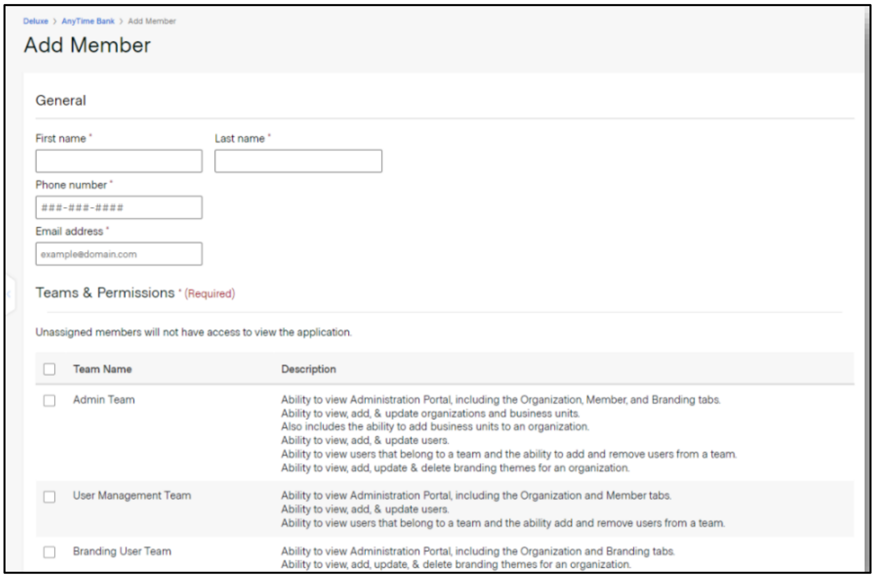
NOTE: The number next to Members in the **Members** tab reflects the number of members in the selected organization.



7. Click **Add user**.

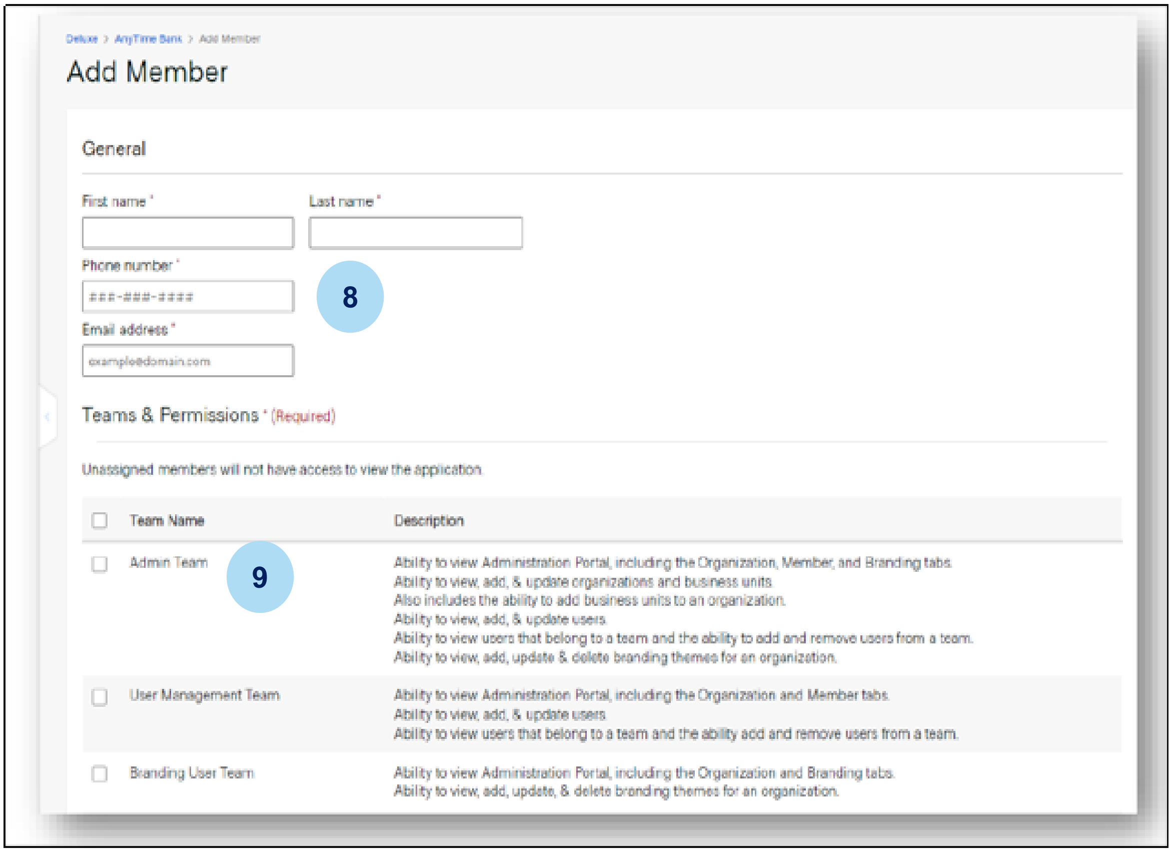


The **General member information** screen displays.



8. Enter the user's:
   a. First Name
   b. Last Name
   c. Phone number (required for multi-factor authentication (MFA))

      NOTE: MFA can be configured for an organization where requested.
   d. Email address (this will serve as the username and is the unique member identifier). An email address can only be used once in the entire R360+ environment. Group emails or email distribution group addresses cannot be used for multiple users.



IMPORTANT: Verify the user is being configured at the highest level needed as the user cannot be moved from a lower organization level to a higher organization level.

9. Select the **Teams** that the user should have access to. More than one team can be selected.

NOTE: Application-level access is provided by the administrator of the organization. This access determines the **Teams** available to the **Member**. Not all **Teams** below may be available to this organization if they are not subscribed to the corresponding application.

Application-Level Access	
Field	**Details**
User Management Team	Provides access to the Members tab of the **Admin | Organization** section.
Archive User Team	Provides access to the **Archive** section, including the ability to search and view transactions.
rDrive User Team	Provides access to the rDrive section which allows a user to view scheduled reports.
Report User Team	Provides access to the Reports section.

Application-Level Access	
Field	**Details**
Dashboard User Team	Provides access to the **Dashboard** page and the ability to interact with the **Dashboard** page and the use of the org selector and title bar functions.
Notifications User Team	Provides access to the Notification section.

NOTE: If the new user is not assigned to a team, the user will receive the following message upon login '"Your account is active but does not have permission to view or manage pages. Contact your administrator for details."

10. Click **Add member**.

A new user is created, and an email will be sent to complete the user account activation process. The user will be sent an activation email to complete the setup of their account. This email will expire in 7 days. To review details of this process, reference the Appendix of this document.

Search for a Member

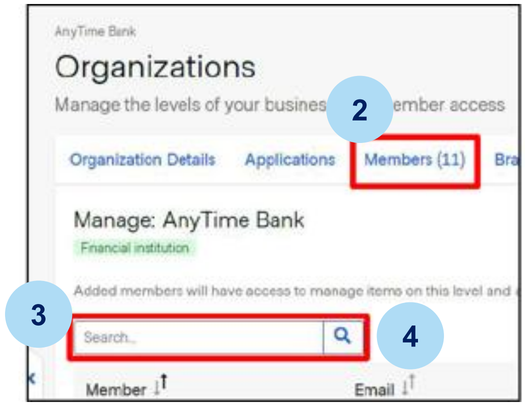
Users can search for members based on the currently selected organization. The search will only take place at the selected level, and not for members of organizations below this selected level.

1. Select the organization level where the user search will occur.
2. Select the **Members** tab under **Admin**.
3. Use the search field to search for either a member's first name, last name, email, phone number, or status.

NOTE: Currently only the first OR last name can be searched in the **Member** field; searching both first and last name will not find the member.

NOTE: The search box does not search the **Team** column.

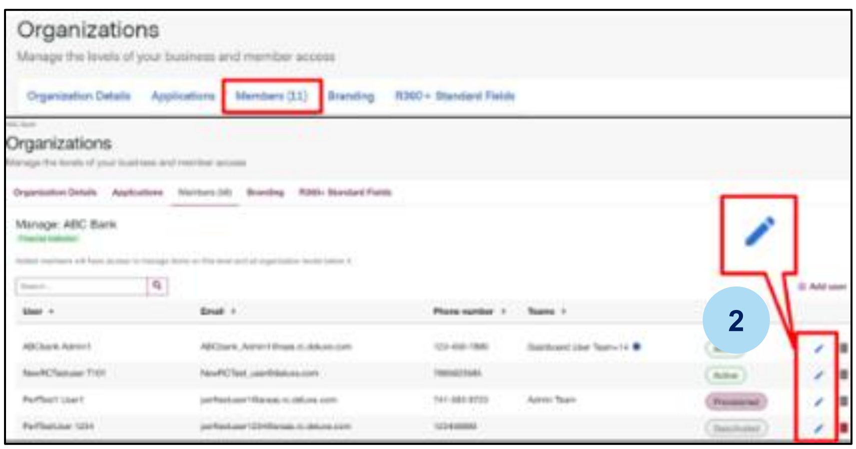
4. Click the magnifying glass or press **Enter** to search.



Edit a Member

An existing user can be updated to change the access level or identifying information. Email addresses cannot be updated.

1. Under **Admin** select the **Members** tab.
2. Click the **pencil** to the right of the user row to edit the user.



All users are listed for this organization.

In the **Status** column:

- **ACTIVE** specifies the user has completed the enrollment process in Okta. An active member can be suspended, deactivated, or can be sent a password reset email.
- **DEACTIVATED** specifies the user has been deactivated and will be removed as a member as part of an automatic regular cleanup process. A deactivated member can be activated.
- **LOCKED OUT** specifies a user has locked themselves out. This usually occurs when they have tried to log in with the wrong password 5 times. The user will be automatically unlocked in 15 minutes.

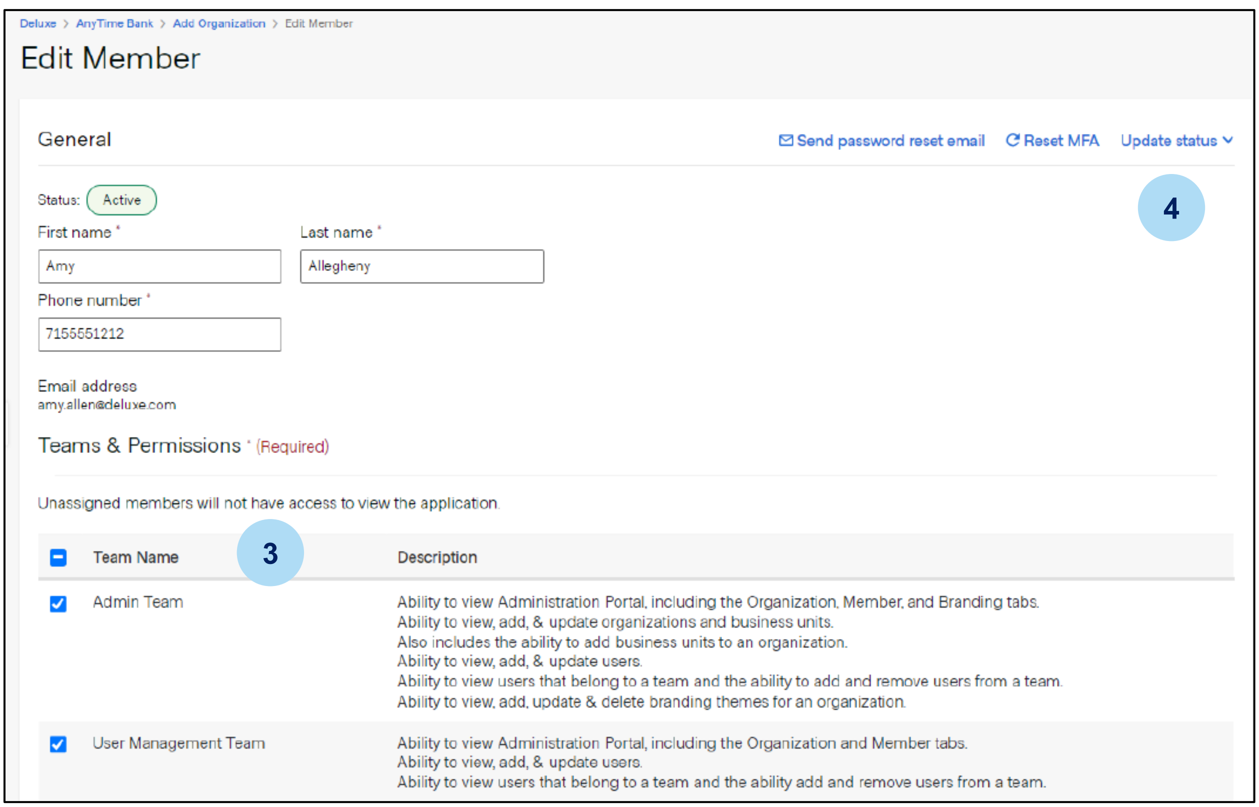
- **PASSWORD EXPIRED** means the user's password has expired and they must be sent the password reset email.
- **PROVISIONED** means the user didn't complete the activation process and their user account cannot be used. This user can be deactivated or resent the activation email.
- **RECOVERY** specifies that the user has been sent a password recovery email and they have not yet completed the password reset process. The password recovery email can be resent, or the user can be deactivated.
- **SUSPENDED** specifies that the user account has been suspended by another user. A user would have to Unsuspend the account to make the user active again.

The **Edit Member** screen displays.

The First Name, Last Name and Phone Number fields can be edited, but the email address cannot. The Phone Number is required for multi-factor authentication (MFA).

3. Change the user's identifying information or change the **Team** access at the bottom of the screen.
4. Click **Update Member**.

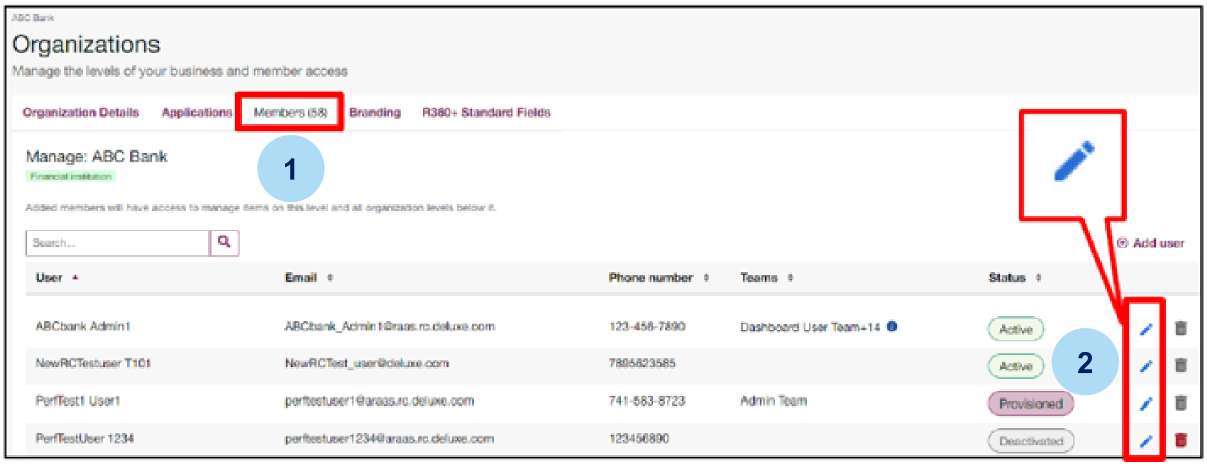
NOTE: Update Member is not an available option until a change has been made.



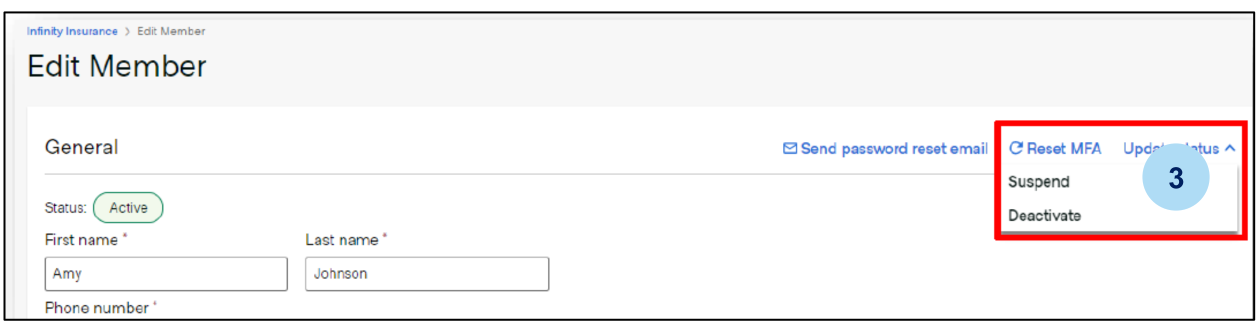
Suspend, Deactivate, or Delete a Member Account

A user account can be suspended, deactivated or deleted. A suspended account will lock a user account so that the user cannot log in. An account should be deactivated if the user is out for an extended time or likely will not access this system again. Once a user is deactivated, it can be deleted completely from the system if the user will never log in again, i.e., a user that is no longer working for the company.

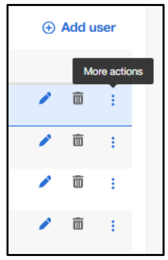
1. Under **Admin** select the **Members** tab.
2. Click the **pencil** to the right of the user row to edit the user.



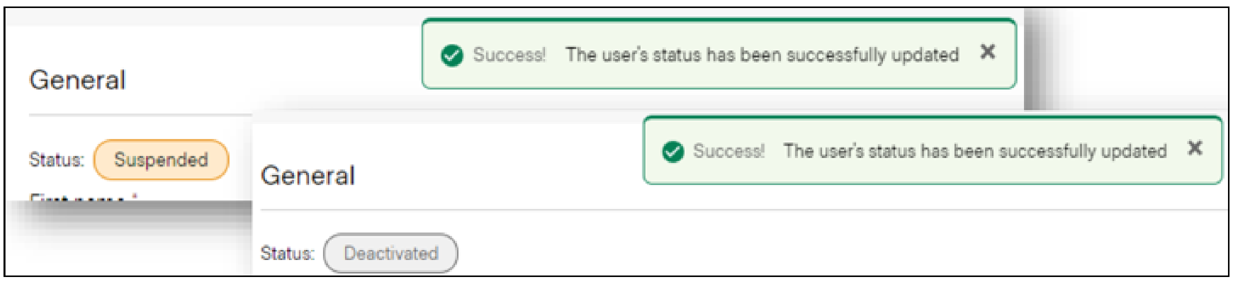
3. In the **Edit Member** screen, click **Update Status | Suspend** to temporarily disable a user account; the user will not be able to log in. If the account should instead be deactivated because the user will never log in again, select **Update Status | Deactivate**.



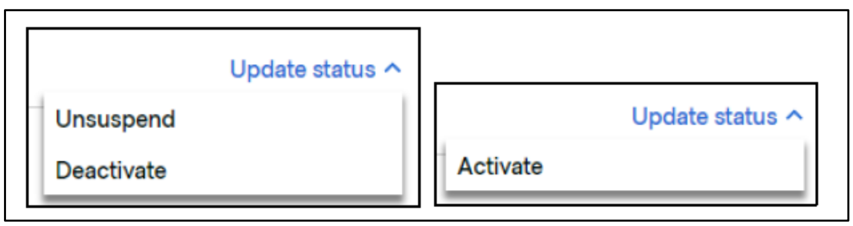
NOTE: In some cases, clicking on the 3-vertical dots on a user record will provide other menu options.



The following message will display for the **Suspended** or **Deactivated** account. Note the updated status of the user.



A suspended user can be unsuspended by clicking **Update Status | Unsuspend**. If the user account was deactivated, it can be reactivated by clicking **Update Status | Activate**.

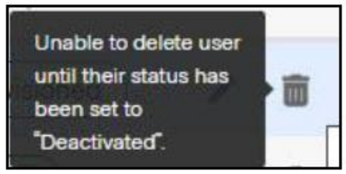


Delete a Member

Once the member is deactivated, it can be permanently deleted.

1. Click the **trash** icon next to the member.

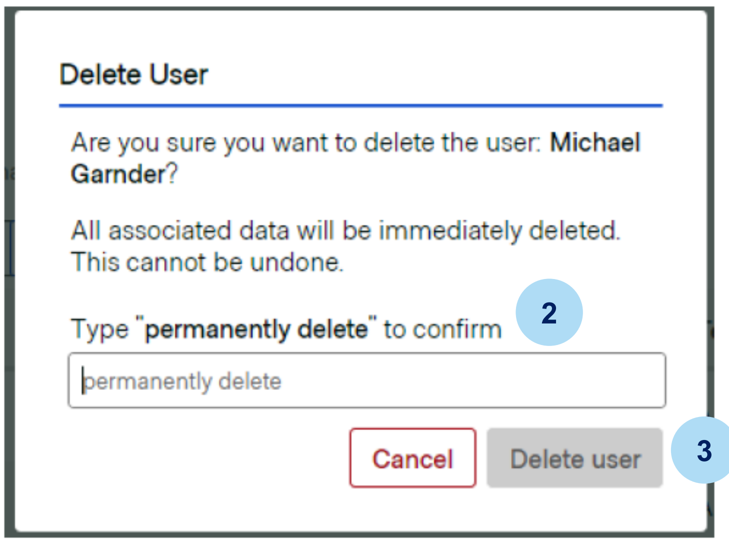
NOTE: If the member has not been deactivated, deletion will not be allowed, and the following message will display.



2. Type "**permanently delete**" in the text field to delete the user.

3. Click **Delete User**.

The user is removed from the system. The page may need to be refreshed to see the user removed.



Reset a Member Password

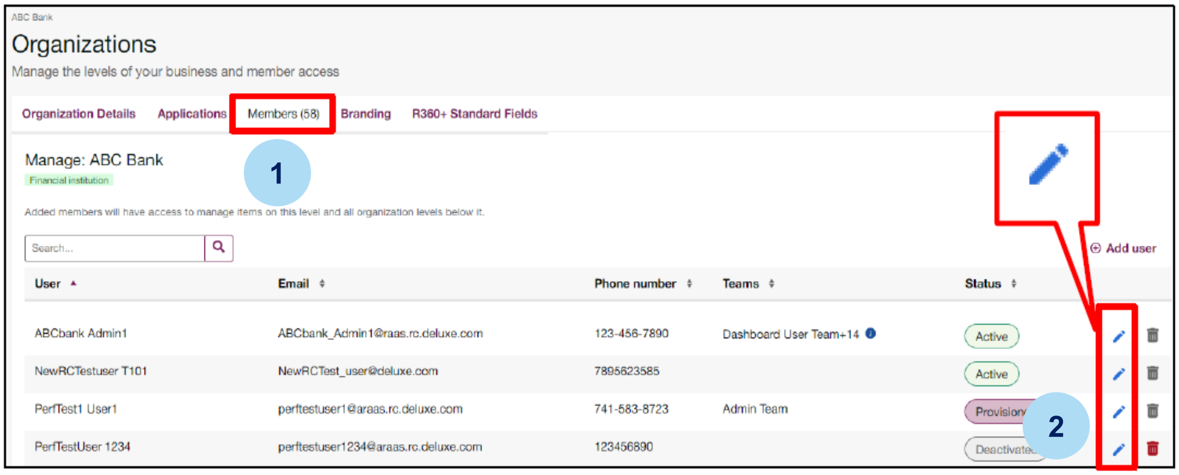
A user can reset their password by going to the login page and selecting **Forgot Password**. The user will be walked through the steps to reset the password. Otherwise, a user administrator can send an email directly to the user which can be used to reset their password.

NOTE: If the user has entered the wrong password 5 times, the account will be locked for 15 minutes. After 15 minutes, the user may attempt to log in again.

1. Under **Admin** select the **Members** tab.

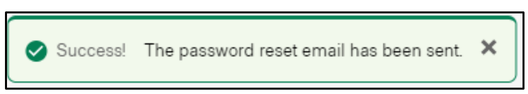
2. Click the pencil to the right of the user row to edit the user.

The **Members** screen displays.



3. On the **Edit Member** page, select **Send password reset email**.

The following message will display.

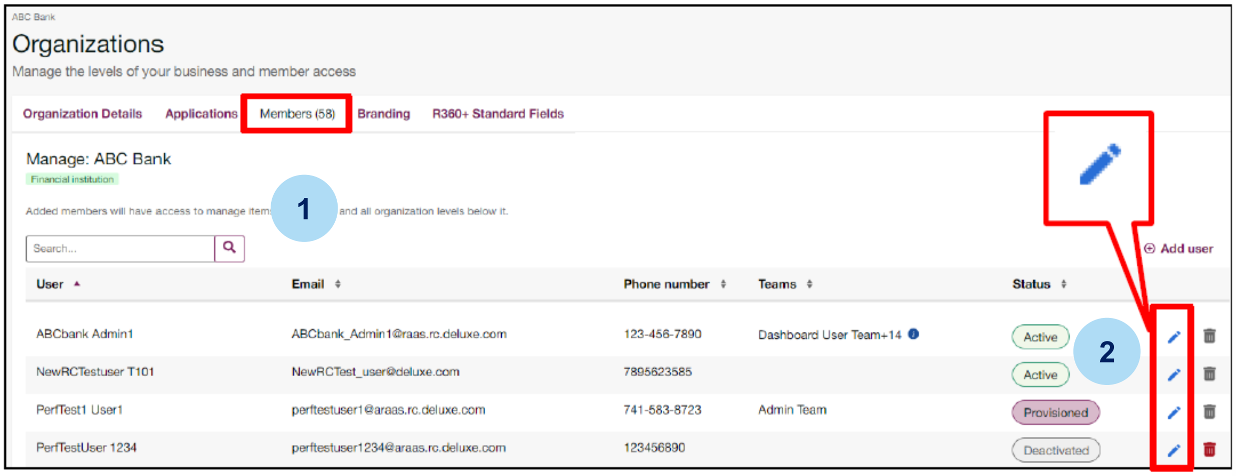


The user will be placed in **Recovery status** until the password reset process is completed.

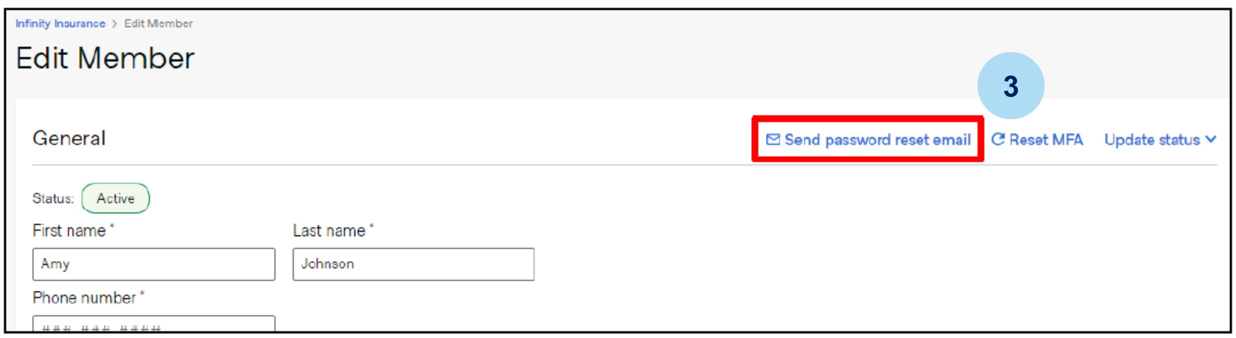
Reset Multi-Factor Authentication

In some cases, a member may set up values incorrectly during the MFA setup process, or possibly they no longer have access to that MFA option or device. The MFA setup can be reset, allowing the user to set up MFA again.

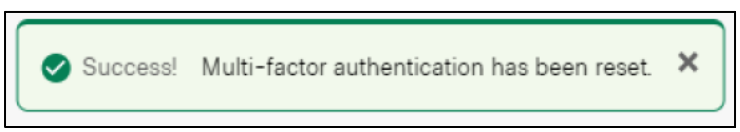
1. Under **Admin** select the **Members** tab.
2. Click the **pencil** to the right of the user row to edit the user.



3. Select **Send password reset email** on the **Edit Member** screen.



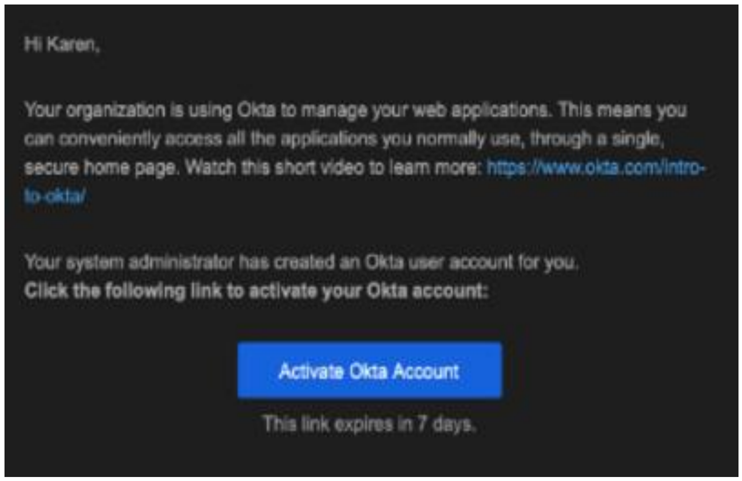
The following message will display.



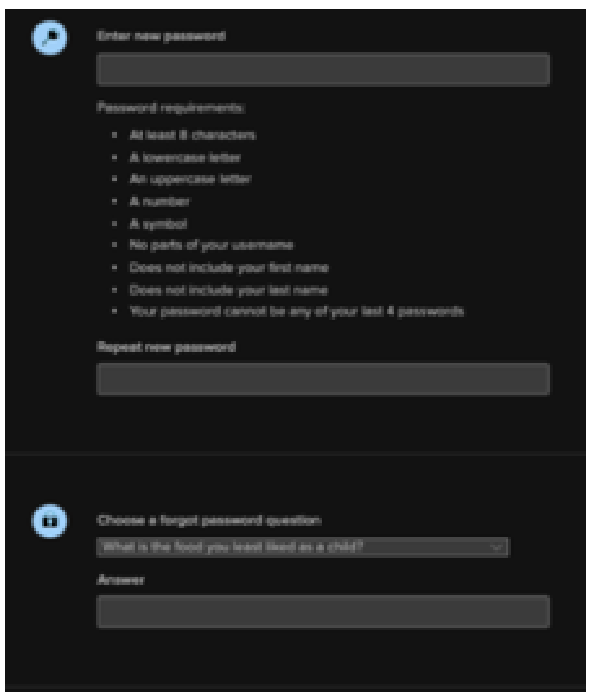
Appendix

Okta Activation Process Overview

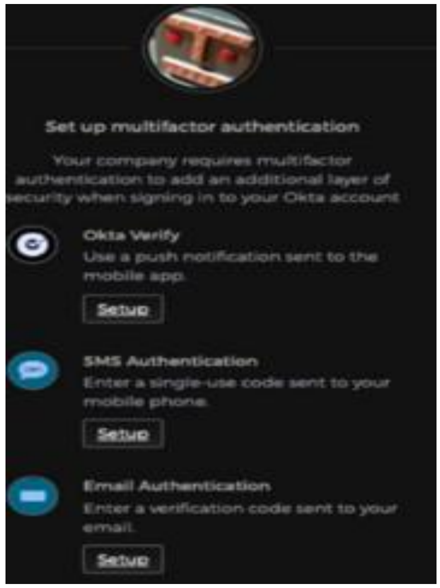
When **Add Member** is selected to create a new user, the user will be sent an activation email to complete the setup of their **Okta account**. This email will expire in 7 days



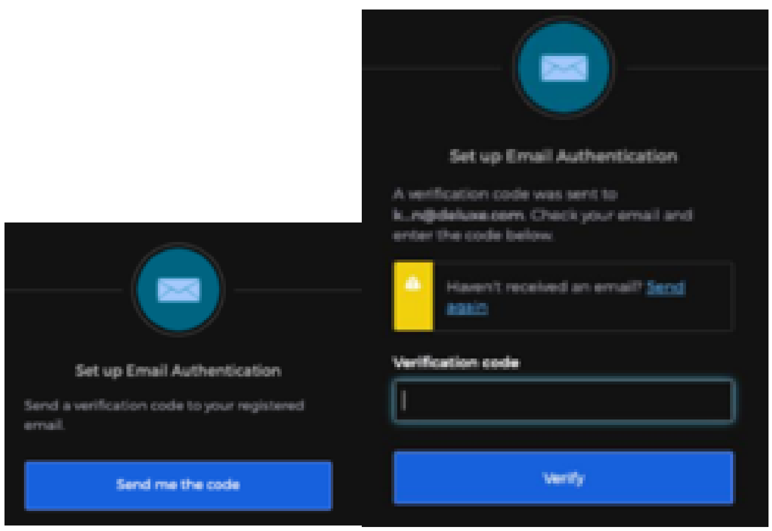
When the user selects to **Activate Okta Account** in the email, they will be required to set up a password that requires specific characters to meet the password rules.



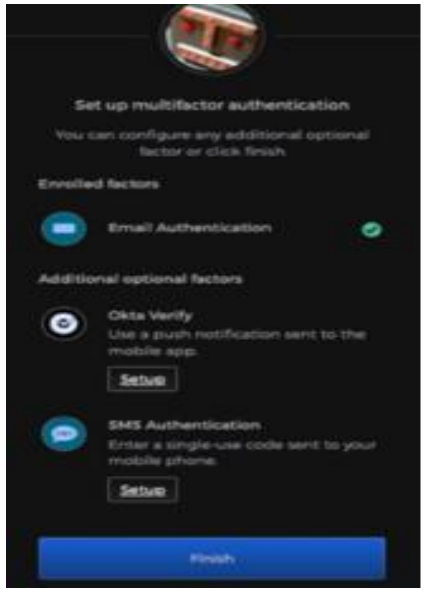
If the customer is configured to require **Multi Factor Authentication (MFA)**, the following screen will display to allow the user to select the delivery method for MFA. If MFA is not used, the MFA screens will not display, and the user can finish the account setup.



Any MFA delivery method will require the user to verify the delivery method with a verification code.



After the code is verified, the user may select another MFA option to use as an additional verification option.



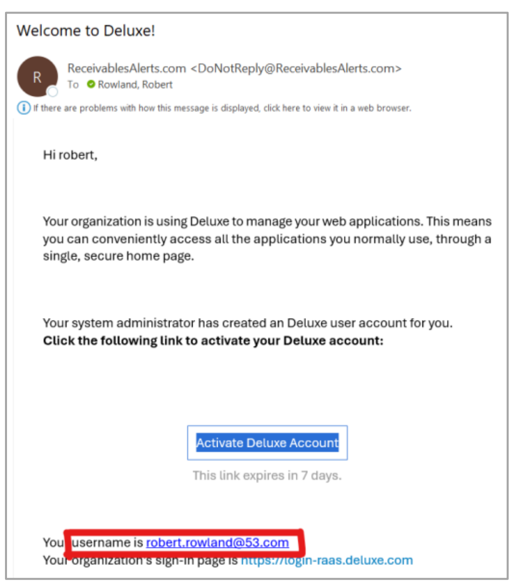
After the verification options are configured, select **Finish.**

Receivables 360+ Activation Notification

When the bank sets up the company admin or when the company admin sets up a new user, an email will be sent to that user notifying them to activate their account and complete their setup. The email is received from DoNotReply@ReceivablesAlerts.com. This email will provide a user name (i.e. email) and have a link for the user to complete their setup (i.e. multi-factor authentication and password).

Once the activation link is selected, follow the prompts to finish setting up the account.

NOTE: This email link will expire 7 days from its sent date.



Have a question? Contact your relationship team or call our Commercial Support Center at 866-475-0729, Monday through Friday, 7 a.m. to 10 p.m., ET.