Regions OnePass

User Guide
# CONTENTS

## Regions OnePass Basics
- What is Regions OnePass? .......................................................... 4
- Minimum Browser Requirements .................................................. 4
- Logging in to OnePass – Existing User ........................................ 4
- The Regions OnePass Landing Page ............................................ 8

## Regions OnePass Administration
- Viewing the Company Profile .................................................... 9
- Editing the Company Profile ......................................................... 11
- Applications in the Company Profile ........................................... 11
- Viewing the User Profile ............................................................. 11
- Adding a User ............................................................................. 13
- Editing the User Profile .............................................................. 14
- Resetting a User Password ......................................................... 15
- Unlocking a User Profile ............................................................ 16
- Resetting a User Security Code (ROOBA) ................................. 17
- Linking an Application Account to a Regions OnePass Profile ...... 18
- Deactivating a User Profile .......................................................... 20
- Reactivating a User Profile ......................................................... 20
- Removing Application Access from a User ................................. 21
- Deleting a user profile ............................................................... 21
- Deactivating User Access to a Company’s Applications ............... 22
- Reactivating User Access to a Company’s Applications ............... 22

## My Profile ................................................................. 23

## User Self Service Profile Maintenance ........................................ 23
- User Initiated Phone Number Changes ....................................... 23
- User Initiated Security Code Changes ........................................ 24
- User Initiated Password Change ................................................ 24

## Regions Out-of-Band Authentication (ROOBA)................................ 25
- ROOBA Scenario: A Regions OnePass Administrator Accesses the OnePass Admin Console ......................... 26
- ROOBA Scenario: A Regions OnePass Customer Attempts to Access Certain Applications as an Application Administrator ............................................................................. 26
- ROOBA Scenario: An Entitled User Attempts to Release a Wire or ACH in iTreasury ........................................... 26
- ROOBA Scenario: A Regions Client Services Associate Initiates Manual Authentication ............................................ 26
- ROOBA Scenario: A Regions OnePass Administrator creates a new user ....................................................... 27
REGIONS ONEPASS BASICS

WHAT IS REGIONS ONEPASS?

Regions OnePass is a single sign-on portal that enables access to multiple Regions commercial banking online products and services using a single set of login credentials.

MINIMUM BROWSER REQUIREMENTS

Regions OnePass supports Internet Explorer® 11 and Edge, Firefox® 45 or later, Chrome® 57 or later, and Safari® for Mac 10.1 or later.

LOGGING IN TO ONEPASS – EXISTING USER

2. Enter your Login ID. This is your email address.
3. Enter your password.
4. Click Login.
5. You have successfully logged in to Regions OnePass. You will see the OnePass Landing page as displayed below.
Logging in to Regions OnePass – First Time

1. Locate the two emails from onepass@regions.com. One is an email containing a Validation Code, while the other email contains your Temporary Password.

2. Go to the Regions OnePass login page (https://onepass.regions.com/onepass) and enter your user ID. Your user ID will be the email address at which you received the two emails (Validation Code and Temporary Password).

3. Enter the Temporary Password emailed to you by Regions.

4. Click Login.

5. Your Temporary Password must now be changed. Enter your old password (which would be the Temporary Password from the Regions email for a first-time user).

6. Enter your new password. The new password must meet all the following criteria:
   a. Password must not match or contain first name.
   b. Password must not match or contain last name.
   c. Password must contain at least 2 alphabetic characters.
   d. Password must be at least 6 characters long.
   e. Password must contain at least 1 lowercase letter(s).
   f. Password must contain at least 1 numeric character(s).
   g. Password must contain at least 1 uppercase letter(s).
   h. Password must not be one of the 6 previous passwords.
   i. Password must start with an alphabetic character.
   j. Password must not match or contain the user ID.

7. Confirm your new password by entering it a second time.

8. Click Submit.
9. After setting your new password you will be prompted to establish your security questions. Select three security questions.

10. Enter a response to each question in the corresponding answer fields.

11. Click Submit.

**Answer Requirements**
- Maximum answer length is 50 characters.
- Answers must be at least 5 characters.
- Answers cannot be repeated. Each must be unique.
- Answers cannot have more than 2 repeating characters.
- The following special characters are allowed: ! @ # $ % ^ & * ( ) - _ ~ `{ } | ; ' " , . / < > ?
- Answers are not case sensitive.

12. When prompted for a Validation Code, in the box provided enter the Validation Code from the other email you received.

13. Click Confirm.
14. You will now need to complete your Regions OnePass Profile. Fields marked with a red asterisk are required.

Enter your name and address in this section.

Occasionally users will be contacted via phone as an additional means to verify identity. This is referred to as ROOBA (Regions Out-of-Band Authentication). Users must enter two phone numbers and select the appropriate country code from the drop-down menus. Next, the user will select a messaging (contact) preference for each phone number. This determines whether validation attempts will be initiated via voice (telephone) call or text message. Users have their choice of numbers to use for each validation.

Create a Security Code that will be used to respond to verification requests in the future. The security code must be at least four characters, cannot be sequential or the same number repeated four times.

15. After successfully completing the Regions OnePass Profile, users will be returned to the main Regions OnePass landing page. Click Create.
THE REGIONS ONEPASS LANDING PAGE

The Landing Page is the home page of the Regions OnePass system. It will be the first page encountered after logging in. Functionality and potential links are added or removed based on user role and application access. Essentially, each user will only see what is applicable to them on this page. All functions identified on the landing page will be explained in detail later in this guide.

Note: The options available in the Link Bar located at the top of the screen will vary depending on each user’s level of access; for example, designated company administrators only will have access to the Admin Console.
REGIONS ONEPASS ADMINISTRATION

Administrative access for client users is determined by their status in one of the connected (linked) applications. If a user is flagged as an administrator in one of the applications or has access to administrative functions in an application (Regions iTreasury or Image Lockbox, for example), they will be an administrator in Regions OnePass. Be aware that if a user’s status is changed (from entitled user to administrator or vice versa) in the respective application, their OnePass status will not change immediately. There is an intraday update process that must take place for the Regions OnePass user status to change. For immediate change, the System Admin can remove and re-add the entitlement in the Regions OnePass Admin Console.

VIEWING THE COMPANY PROFILE

1. Click the Admin Console link at the top of the landing page. A ROOBA challenge will be triggered. See page 25 for additional information.

2. If ROOBA is successful, the Administrator Console will open in a new page.

3. Click the Companies tab on the console header.

4. To locate a specific company, enter information into the Company Name or Tax ID field and select Search.
5. The Companies that fit your search criteria will be listed and can be sorted by any of the list values by clicking the column label at the top of the list. You will only see companies in the search results to which you have access.

6. Search results will appear beneath the list header. In the list view, click the name of the company you wish to view.

7. The company profile will be displayed.
EDITING THE COMPANY PROFILE

1. In the upper section, you will see the company’s details. To edit this information, click the **Edit Company** link in the upper right corner of the page.

2. After completing the changes, click **Save**. Click **Cancel** to leave the page without saving your changes.

APPLICATIONS IN THE COMPANY PROFILE

In the lower section is the Application Profiles list. This contains a list of all Treasury Management applications to which your company subscribes. Only Regions administrators can add or remove applications in a company’s list.

VIEWING THE USER PROFILE

1. Click the **Admin Console** link at the top of the landing page.
2. The Administrator Console will open in a new page / tab. Click the Users tab on the console header.

To view all users associated with a given company, select the company from the drop-down list and select Search. You can also search for a specific user in a company by entering values in the Name or Email / User ID field, selecting your company from the drop down and selecting Search.

3. Search results will appear beneath the list header.

4. Click on the name of the user you wish to view.

5. The User Profile will be displayed.
ADDING A USER

1. To add a user, click the plus sign in the right-hand corner of the Regions OnePass Users tab.

2. In the drop down, select the company to which you want the user to be added. You will only see companies you have access to in the drop-down list.

3. Enter the user’s email.

4. Enter the user’s first and last name.

5. Select Save.

6. A ROOBA challenge will be triggered. See page 25 for additional information. If successful, the user will be created.

7. The new user will then receive the two emails containing their Validation Code and their temporary passcode.

8. All Admin users in the company will receive an email confirming the new user creation.

9. Next, you will need to create the new user’s entitlements for the application. See the “Linking an Application Account to a Regions OnePass Profile” below.
EDITING THE USER PROFILE

1. To edit the user profile go to the User Profile by first selecting a user from your search results on the User tab.

2. Once the User Profile is presented, click the **Edit User** link in the upper right corner. The form will go into edit mode.

3. Make any necessary changes to the information presented.

4. Click **Save** to save your changes.

5. Click **Cancel** to exit edit mode without saving changes.
RESETTING A USER PASSWORD

1. To reset a user’s password, navigate to the Admin Console.

2. Navigate to the user’s profile.

3. Click Edit User on the top right corner, followed by the Reset Password link in the lower left corner of the profile page.

4. A dialogue will appear asking for confirmation to reset the user’s password.

5. To continue with the password reset, click Yes. To exit without resetting the password click No.

6. You will then see the following confirmation. Select the X to close the confirmation.

7. An email similar to the one displayed to the right, will be sent to the user’s email address on file.

8. The user will log in to Regions OnePass using their User ID and the Temporary Password provided.
9. The user will then be prompted to reset their password.

10. All users have a self-service option for password resets or account locks. After entering the User ID in OnePass, users will be presented with the Password screen. In the lower left corner of the password dialogue is a *Forgot your password?* link. Clicking that link prompts the user to answer a security question or ROOBA challenge. If answered correctly, the system will generate a new Temporary Password. That Temporary Password will then be emailed to the user at the address on file.

### Unlocking a User Profile

1. After three invalid login attempts, the user will see the following message:

   ![User account is disabled. Please contact Regions Client Services at 1-800-787-3905.]

   This message indicates that the user’s profile has been locked.

2. To unlock a user’s account, navigate to the Admin Console.

3. Navigate to the user’s profile. If the profile is locked, the Locked field in the lower left corner will display confirmation with a “Yes.”

4. Click the **Edit User** link in the upper right corner.
5. Remove the checkmark from the Locked field and select **Save**.

**Note: Users can self-service locked accounts by selecting the “Forgot Password” link on the password entry page**

**RESETTING A USER SECURITY CODE (ROOBA)**

If a user cannot remember the Security Code they selected during initial setup, they will not be able to correctly respond to Regions Out-of-Band verification requests. As a result, it may be necessary to reset the Security Code allowing the user to select a new one.

1. To reset a user’s Security Code, navigate to the user’s profile.

2. In the lower left corner click the **Reset Security Code** link.

3. A dialogue will appear asking for confirmation to reset the user’s Security Code.

4. To continue with the Security Code reset, click **Yes**. To exit without resetting click **No**.

5. A confirmation will be displayed.

6. Click the **X** in the upper right corner to close the dialogue.
7. At the next log in attempt the user will be prompted to select a new security code.

**LINKING AN APPLICATION ACCOUNT TO A REGIONS ONEPASS PROFILE**

After establishing access to the Regions OnePass application, the user’s OnePass profile must be linked to any application account the user may have. For instance, if the user has access to Regions iTreasury and Regions Quick Deposit, their accounts in each of these applications need to be linked to his/her Regions OnePass profile. This is what allows the user to access their Regions Treasury Management services and accounts directly from the Regions OnePass landing page. This function is primarily handled by the designated company administrator.

Follow the instructions below.

1. Navigate to the user’s OnePass Profile.

2. Click the **Add New Company** link to the right of the Application Profiles heading.

3. Select the Company whose application access you wish to grant the user. *(Note that with this functionality, a user can have access to the applications of multiple companies. This accommodates third party users such as accounting firms who need access to the information of multiple Regions’ clients. Additionally, the Administrator will only be able to view companies to which they have access.)*

4. Click **Add Company**.
5. Select the application which you are adding to the user profile.

6. Enter the User ID from the selected application that belongs to this user. For instance, if the application is iTreasury, the user’s iTreasury User ID must be placed in this field. This is what binds or links the user’s iTreasury account, for example, to their OnePass account.

7. Enter a Profile Name for this entitlement of the account. (i.e., “QD Admin,” “Recon Profile”). This Profile Name may be referenced if a user is prompted to select from multiple profiles and may be displayed for reporting purposes.

8. Click the Save icon.

Note: If the user does not have an account in the selected application, you will be unable to bind or link an application account to the user’s Regions OnePass account. The user must be set up in both places. So, the first step for adding a new user to OnePass is adding that user to the underlying application (i.e., Regions iTreasury) first, just as the Administrator would have previously.

9. After the application is linked and the connection is made, OnePass can determine from the application side whether the user is an administrator in that application.

This information is shown in the Admin column as either ‘true’ or ‘false’. If the user is designated as an administrator in the respective application, he or she also becomes a designated administrator in Regions OnePass by default.

10. You can remove the connection by selecting the “X” under the “Actions” header.

Note: If an existing user’s status in an underlying application has been changed to “admin” status, there will be a delay in OnePass recognizing the status change. However, by removing the connection and then recreating it, the Admin flag will update in real time.
DEACTIVATING A USER PROFILE

A specific user can be locked in cases where a potential malware infection has occurred or the user needs to temporarily have their access suspended. To deactivate a user, navigate to the User’s Profile and follow the steps below.

1. Click the **Deactivate** link in the upper right corner.
2. Navigate to the user’s profile.
3. Click the **Deactivate** link in the upper right corner.
4. A user who has been deactivated will not be able to log in to OnePass until their profile has been reactivated.

REACTIVATING A USER PROFILE

A user whose profile has been deactivated will be unable to log in to Regions OnePass, and, by extension, will have no access to any of the services associated with their profile. If the reason for the deactivation no longer exists, the user must be reactivated before they will be able to regain access to the system. To reactivate a user’s access, follow the steps below.

1. Navigate to the user’s profile.
2. Click the **Reactivate** link in the upper right corner.
Removing Application Access from a User

Occasionally it may be necessary to remove a user’s access to an application. If a user changes positions within a company for instance and her responsibilities no longer justify continued access to iTreasury, her profile should be modified to remove this access. Follow the steps below to perform this function, removing application access from the user. Navigate to the user’s profile.

1. Under the Application Profiles section, locate the Company associated with the application.
2. Under the Company group, locate the application to be removed.
3. Click the Delete icon in the actions column.
4. The application will be removed from the list. If this was the only application under the selected company, the Company will be removed from the Application Profiles list.

Deleting a User Profile

If a user no longer needs access, they may be deleted after all their application access has been removed following the steps above.

1. Navigate to the user’s profile.
2. Follow the steps outlined in Remove Application Access from a User for ALL applications assigned to the user.
3. Click the Delete User link in the upper right corner.
DEACTIVATING USER ACCESS TO A COMPANY’S APPLICATIONS

In certain situations, it may be necessary to temporarily suspend a user’s application access. This can be completed by deactivating Company level access under the user profile. Follow the steps below to complete this function.

1. Navigate to the user’s profile.
2. Under Application Profiles, locate the company from which the user needs to be suspended.
3. Click the Deactivate link to the right of the company name.
4. The display will change to show applications under the company are now inactive.

REACTIVATING USER ACCESS TO A COMPANY’S APPLICATIONS

To restore a user’s access to applications that have been deactivated, follow the steps below.

1. Navigate to the user’s profile.
2. Under Application Profiles, locate the company to which the user needs access.
3. Click the Activate link to the right of the company name.
4. The display will change to show the Deactivate option. This indicates that application access has been restored.
MY PROFILE
USER SELF SERVICE PROFILE MAINTENANCE

Users have the ability to update certain pieces of information in their User Profile, while other pieces can only be modified by Regions Client Services. To access the User Profile maintenance options, start from the Regions OnePass landing page.

1. Click the **My Profile** link in the upper right corner. The OnePass User Profile will be displayed.

2. Any field marked with an Edit icon can be edited by the user. *(Note that the user’s OnePass password and Security Code can be changed from this page.)*

3. Clicking an **Edit** icon will reveal a set of fields that can be edited.

![My Regions OnePass Profile](image)

**USER INITIATED PHONE NUMBER CHANGES**

1. Note that while the Phone Number section can be edited by the profile owner (user), the only options available to the user are:
   a. Change the phone numbers between primary and secondary. Use the drop-down list to make the appropriate selection next to each phone number.
   b. Change the message preference between Voice and Text (SMS) by selecting the appropriate radio button below each phone number.

2. Edits to the phone numbers themselves can only be made by the System Administrator through the Admin Console, or by calling Client Services at 1-800-787-3905.
USER INITIATED SECURITY CODE CHANGES

1. To change the user’s ROOBA Security Code, click the Edit icon to enter edit mode. Enter the current security code and then the new security code.

2. When the changes are complete, click Save to retain the changes. Click Cancel to exit edit mode without saving the changes.

USER INITIATED PASSWORD CHANGE

1. To change the user password, click the Edit icon to enter edit mode. Enter the current password, new password and new password again to confirm.

2. When the changes are complete, click Save to retain the changes. Click Cancel to exit Edit mode without saving the changes.
REGIONS OUT-OF-BAND AUTHENTICATION (ROOBA)

Regions has implemented an additional step-up authentication method based on risk measured events initiated in Regions OnePass and the integrated applications. This method is called Regions Out-of-Band Authentication or ROOBA.

To complete certain login functions or to release ACH and Wire transactions, users will use their Security Code established in their OnePass Profile to validate those events.

In cases where additional authentication is required ROOBA will provide an additional layer of authentication. The system works by initiating a call or text to the phone number listed in the user’s OnePass Profile. When the user receives that call or text, they will see the following screen appear and will be prompted to respond to the message using their Security Code. If the code the user enters matches the Security Code in their OnePass Profile, the system will proceed with the event which triggered the ROOBA prompt.
There will be multiple scenarios where ROOBA will be used for security purposes. Those scenarios are as follows:

**ROOBA Scenario: A Regions OnePass Administrator Accesses the OnePass Admin Console**

- When the Regions OnePass administrator attempts to access the OnePass Admin Console, they will receive an out of band authentication request.
- A successful authentication will allow access. An unsuccessful authentication will prevent access.
- An administrator will only be prompted for the additional access once per session. For instance, if the user logs in to OnePass and clicks the Admin Console link, the user will receive a ROOBA request. If the authentication is successful, the user will be able to access the console. Once finished, the user can log out of the console. As long as the user remains logged in to OnePass, they will be able to access the Admin Console again without an additional ROOBA challenge. This is called a “session authentication.”

**ROOBA Scenario: A Regions OnePass Customer Attempts to Access Certain Applications as an Application Administrator**

- When a user selects certain application links in Regions OnePass and is directed from OnePass to that application, and if the user is flagged as an administrator in that application, the user will receive a ROOBA request.
- A successful authentication will allow access. An unsuccessful authentication will prevent access.
- For example, if Jim is an administrator in FX Online for Acme Inc., when Jim accesses FX Online from his OnePass Landing Page, he will receive a ROOBA request before being allowed to enter FX Online.
- Again, a user should only be ROOBA authenticated once during a valid OnePass session.

**ROOBA Scenario: An Entitled UserAttempts to Release a Wire or ACH in iTreasury**

- With Regions OnePass, users attempting to release either an ACH batch or a Wire transfer will receive a ROOBA request. If the user authenticates by providing the correct Security Code, the transaction will be released.
- If there is an error in the authentication, the transaction will return to its previous “Entered” status and will wait for the next authentication attempt.
- If a client is using dual control, each person required to release a transaction will receive a ROOBA challenge in order to complete the transaction.

**ROOBA Scenario: A Regions Client Services Associate Initiates Manual Authentication**

- As part of the Regions OnePass platform, Regions Client Services associates have the ability to trigger a manual ROOBA challenge.
- This tool will be used if an associate needs additional forms of identification in order to validate a user who has contacted Client Services.
- Once the user authenticates via their preferred method, the Client Services associate will receive a validation message and will continue assisting the user.
ROOBA SCENARIO: A REGIONS ONEPASS ADMINISTRATOR CREATES A NEW USER

- As an added security measure, new user creation results in a ROOBA challenge to the admin user creating the user.
- If the authentication is successful, the new user is created. If there is an error the new user will not be created until a successful ROOBA is performed.
- This authentication is in addition to the ROOBA that must be authenticated before entering the Admin Console.

MULTI-FACTOR AUTHENTICATION (MFA)

MFA provides real-time analysis and risk-based authentication at login to identify potential fraudulent activity. The system is designed to learn a user’s “typical” use patterns. That includes things such as:

- What IP address does the user log in from most often?
- What type of device/operating system does the user use most often?
- What day of the week or time of day does the user most frequently log in?

Based on information gathered by the MFA platform, a pattern of the user’s “typical” behavior can be established. Each login attempt is then compared to the user’s established pattern. If a login attempt deviates from that pattern, an additional level of authentication is initiated in the form of Challenge Choice (Question Challenge or ROOBA can be selected by the user).

Each of the scores is then evaluated to produce a total risk assessment. As the score goes up, the level of confidence in the validity of the user goes down, and when a score reaches the specified level, a challenge is presented to the user in addition to the standard credentials. In this case, the user is asked to provide the answer to one of the challenge questions they previously selected or respond to a ROOBA challenge.

While challenge questions and the user’s answers to each are stored as part of the user’s Profile, the MFA application manages that content as well as pattern monitoring and challenge initiation. In cases where a user needs to have their challenge questions or answers reset, this must be performed through the MFA application.

The first time a user logs in to OnePass, they will be prompted to select their challenge questions and provide an appropriate response for each. Challenge questions are broken into three categories:

- Favorites – questions that ask about things you like or prefer
- Historical – questions that ask about historical events in your life
- Relatives – questions associated with your family members

There are multiple questions associated with each category, but MFA randomly selects from each and presents them to the user if Questions Challenge is selected as the Challenge Choice. The user will select one of the five options and then provide an answer to that question. Users may also choose to initiate a ROOBA challenge instead of answering a challenge question. For issues with challenge questions or if a user forgets their answers or needs to have their questions reset, they can do so by contacting Client Services at 1-800-787-3905. Client Services can also leverage the challenge questions and answers to further authenticate a caller.
CHALLENGE QUESTIONS

ANSWER REQUIREMENTS:

- Maximum answer length is 50 characters
- Answers must be at least 5 characters.
- Answers cannot be repeated. Each must be unique.
- Answers cannot have more than 2 repeating characters.
- The following special characters are allowed: ! @ # $ ^ % ( ) = _ + ` ~ [ ] { } | ; ' " , . / < > ?