Regions OnePass℠ USER GUIDE
# Regions OnePass User Guide

## Table of Contents

### Section I. OnePass Basics
- What Is OnePass?  
- Minimum Browser Requirements  
- Logging In – For Existing Users  
- Logging In – For First Time Users  
- The OnePass Landing Page

### Section II. OnePass Administration
- Viewing the Company Profile  
- Editing the Company Profile  
- Applications in the Company Profile  
- Viewing the User Profile  
- Adding a User  
- Editing the User Profile  
- Resetting a User Password  
- Unlocking a User Profile  
- Resetting a User Security Code (ROOBA)  
- Binding an Application Account to a OnePass Profile  
- Deactivating a User Profile  
- Reactivating a User Profile  
- Removing an Application from a User  
- Deactivating User Access to a Company’s Application(s)  
- Reactivating User Access to a Company’s Application(s)

### Section III. My User Profile – Self Service Profile Maintenance
- User Initiated Phone Number Changes  
- User Initiated Security Code Changes  
- User Initiated Password Reset

### Section IV. Regions Out-of-Band Authentication (ROOBA)
- ROOBA Scenario: A OnePass Administrator Accesses the Admin Console  
- ROOBA Scenario: A OnePass User Attempts to Access an Application as an Administrator  
- ROOBA Scenario: An Entitled User Attempts to Release a Wire/ACH transaction in iTreasury  
- ROOBA Scenario: A Regions Client Services Associate Initiates Manual Authentication

### Section V. Multi-Factor Authentication

### Section VI. What Happens When an Application is Added to OnePass
- Pre-Registration
- Self-Registration
- Closed Registration

### Additional Assistance

---

**Tip:** Click on a desired section to navigate to the page you wish to view.
Section I. OnePass Basics

What is OnePass?

OnePass is a single sign-on portal that allows clients to access multiple online products and services using a single set of login credentials.

Minimum Browser Requirements

Regions OnePass supports Internet Explorer® 8 and 9, Firefox® 10 and 11, Chrome® 19 and Safari® for Mac 5.1.

Logging in to OnePass – Existing User

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

1. Locate the two emails from donotreply@regions.com. One is an email containing a link and a validation code. The other email contains your temporary password.

2. Click the link in the email containing the validation code. When prompted, enter the validation code from the email in the box provided. Click Confirm.

3. You will then be routed to the login page. Here, type in your Login ID. This is the email address where you received the two emails above.

4. Click Next.

5. Enter the temporary password emailed to you by Regions.

6. Click Login.

7. 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).

8. 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 two alphabetic character(s).
   d. Password must be at least six character(s) long.
   e. Password must contain at least one lowercase letter(s).
   f. Password must contain at least one numeric character(s).
   g. Password must contain at least one uppercase letter(s).
   h. Password must start with an alphabetic character.
   i. Password must not match or contain the user ID.

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

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

12. Enter a response to each question in the corresponding Answer fields.

13. Click Submit.

**Answer Requirements**
- Maximum answer length is 50 characters
- Answers must be at least 3 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.

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

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

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 OnePass Profile, users will be taken to the main landing page. Click Create.
The OnePass Landing Page

The Landing Page is the home page of the 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.

Home - This option will take you back to the landing page wherever you are in OnePass.

Admin Console - This option will take you to the Admin Console. Here, you can reset users and maintain permissions. Only available to Admins.

My Profile - This option will allow you to view and make changes to their profile.

Logout - This option will log you out of OnePass.

Messaging - Banner messaging sections

Services you have registered with OnePass - Clicking these links will take you into the applications.

Other Regions Services - A list of links to other Regions online applications not yet integrated with OnePass.

Note: The options available in the Link Bar at the top will vary depending on the user’s level of access; for example, designated company administrators only will have access to the Admin Console.
Section II. OnePass Administration

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

Viewing the Company Profile

1. Click the Admin Console link at the top of the landing page.

2. The Administrator Console will open in a new page.

3. Click the Companies tab on the console header. A list of company profiles will be displayed.

4. To locate a specific company, scroll through the list or utilize the search function by clicking the Search icon. The Companies list can be sorted by any of the list values by clicking the column label at the top of the list. Only the companies a user has access to will be displayed.

5. Clicking the Search icon reveals an additional set of fields that allow the user to enter specific search criteria. Users can utilize one or multiple fields to narrow the results. Again a user will only be able to search companies they have access to. Search options include:
   a. Name
   b. Tax ID
   c. Address
   d. City
   e. State

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

8. The company profile will be displayed.

![Company Profile](image)

**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.

3. Click the **Users** tab on the console header. To view all users associated with your company, use the Company drop down list. The list will only contain companies to which each user has access.

4. This drop down list contains a search function that will allow you to narrow the choices. Simply begin typing your company name in the search box to narrow the list if you have multiple companies.

5. You can locate a specific user by using the search option. After selecting the appropriate company, click the **Search** icon in the upper right corner.

6. Clicking the Search icon reveals an additional set of fields that can be used to narrow the search results. Search options include:
   a. Name
   b. Email/User ID
   c. Status
      - Active
      - Inactive
      - Deactivated
      - Reactivated
      - Deleted
7. After entering appropriate values, click **Search**.

8. Search results will appear beneath the list header.

9. Click the name of the user you wish to view.

10. 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 OnePass Users page after selecting the company from the list.

2. Enter the user’s email.

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

4. Select **Save**.

5. The user will then receive the emails containing their validation code and their temporary passcode.

6. Next, you will need to create the new user’s entitlements for the application. See the “Binding an Application Account to a OnePass Profile” below.
Editing the User Profile

1. To edit the user profile, click the **Edit User** link in the upper right corner. The form will go into edit mode.

2. Make any necessary changes to the information presented.

3. Click **Save** to save changes.

4. Click **Cancel** to exist edit mode without saving changes.

**Note:** Phone numbers and Contact Preferences in this profile are tied directly to Out of Band Authentication. Users will not be able to modify the actual Primary or Secondary Phone numbers. The primary / secondary designation can be modified as well as the Contact Preference, however all phone number changes must be made by the Customer Admin or requested by calling Regions Client Services at 1-800-787-3905.

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

7. The user will log in to OnePass using their User ID and the temporary password provided.

8. The user will then be prompted to reset their password.

9. All users have a self-service option for password resets. 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 one of their security questions. 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 click **Save**.
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 login attempt the user will be prompted to select a new security code.
After establishing access to the OnePass application, the user’s OnePass profile must be connected to any application account the user may have. For instance, if the user has access to iTreasury and Quick Deposit, her accounts in each of these applications need to be tied to her OnePass profile. This is what allows the user to access her TM accounts directly from the OnePass landing page. This function is primarily handled by the designated company administrator, but for troubleshooting purposes, it may occasionally be necessary for perform this function on the admin’s behalf.

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. Under the App Name column, select the application the user needs to access through OnePass.

6. Enter a description of the account. (i.e., “Lockbox Admin,” “Recon Profile”). This description is presented to users when accessing an application under a company for which they have multiple application profiles.

7. 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 the user’s iTreasury account, for example, to their OnePass account.
8. Click the **Save** icon.

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

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

![Application Profiles](image)

This is shown in the Admin column as either ‘true’ or ‘false’. If the user is designated as an administrator in the TM application, he or she also becomes a designated administrator in the OnePass application 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 here. 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 follow the steps below.

1. Navigate to the User’s profile.

2. Click the **Deactivate** link in the upper right corner.

3. A user who has been deactivated will not be able to log in to OnePass until their profile has been reactivated.

4. Navigate to the user’s profile.

5. Click the **Deactivate** link in the upper right corner.

6. 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 into 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 follow the steps below.

1. Navigate to the user’s profile.
2. Click the Reactivate link in the upper right corner.

Removing an Application 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.

1. Navigate to the User’s profile.
2. Under the Application Profiles section, locate the Company associated with the application.
3. Under the Company group, locate the application to be removed.
4. Click the Delete User icon in the actions column.
5. 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.
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 this Company are now inactive.

Reactivating User Access to a Company’s Applications

To return 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.
Section III. My User Profile
Self Service Profile Maintenance

Users have the ability to update certain pieces of information in their user profile, while others pieces can only be modified by Regions Client Services. To access the user profile maintenance options, start from the 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 maintained 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.

User Initiated Phone Number Changes

1. Note that while the Phone Number section can be edited, the only options available to the user are:
   a. Change the calling order of 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 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 Reset

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.
Section IV. Regions Out-of-Band Authentication (ROOBA)

Regions is implementing a new method for step-up authentication which replaces the RSA SecurID Token. This method is called Regions Out-of-Band Authentication or ROOBA.

Instead of using a token serial number to complete certain login functions or to release ACH and Wire transactions, users will now establish a Security Code in the OnePass system for that purpose.

In cases where additional authentication is required ROOBA will provide that additional layer of authentication. The system works by initiating a call to the phone number listed in the user’s OnePass profile. The user will either be contacted via Voice or Text (SMS) based on their selected preference. 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 provided matches the code in their OnePass profile, the system will proceed with the login or with the release of the transaction.

There will be multiple scenarios where ROOBA will be used for security purposes. Those scenarios are as follows:

ROOBA Scenario: A OnePass Administrator Accesses the OnePass Admin Console

- When the 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 OnePass Customer Attempts to Access an Application as an Administrator

- When a user selects an application link in 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 iTreasury for Acme Inc., when Jim accesses iTreasury from his OnePass Landing Page, he will receive a ROOBA request before being allowed to enter iTreasury.
- Again, a user should only be ROOBA authenticated once during a valid OnePass session.

ROOBA Scenario: An Entitled User Attempts to Release a Wire or ACH in iTreasury

- Currently, to release a Wire or ACH batch in iTreasury requires the user to enter their RSA token PIN and Passcode. In cases of Wire transfer, the user must also enter their Wire PIN in addition to the RSA information.
- Going forward, 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 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 Service associate will receive a validation message and will continue assisting the user.
Section V. 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 Questions.

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.

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. The user will select one of the five options and then provide an answer to that 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 3 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.
- Inappropriate (obscene) language is not permitted
Section VI. What Happens When an Application is Added to OnePass

While the first two releases of OnePass include Image Lockbox and iTreasury, Regions is planning on integrating all commercial online applications under OnePass in Phases. As with Image Lockbox and iTreasury, when integrating into OnePass, an application (and its users) will go through three phases of integration: Pre-Registration, Self-Registration and Closed Registration. It is important to Note that only users existing in the respective application goes under OnePass will be subject to these phases. Once an application is under OnePass, any new users will not go through these phases.

Pre-Registration

Pre-Registration represents a short period of time (between 1 and 3 weeks depending on the application) prior to an application being integrated into OnePass, where the users are given the opportunity to create their OnePass Profiles (if they do not already have one) and bind or activate their OnePass profile to their Application Profile. It is important to Note that during this period, the application isn’t integrated with OnePass, so the user will still have to enter their normal application credentials to access the application, just as they normally would. There are two ways a user can experience Pre-Registration of an application.

Pre-Register an Application from the Native Application URL Link

1. User accesses their native application URL and is redirected to the Pre-Registration screen for the given application.

2. a. If the user selects Continue to ‘Application’, they will be directed to the native application log in page as they would normally.

   b. If the user elects to create their OnePass profile by clicking Register ‘Application Name,’ they are redirected to the application verification screen.

3. User enters their application credentials and clicks Verify.

   Note: The credentials presented for verification will vary depending on the application being registered.
4. From this point, the user will enter the profile creation process referenced earlier in this user guide.

5. Once completed, the user will be directed to their Landing Page and can select their respective application under the **Services Registered** section. The user will be prompted to enter their application credentials until Pre-Registration is over.

6. The user should bookmark OnePass and begin using it to access all of their Regions applications.

---

**Pre-Register an Application from the Landing Page**

Users already utilizing OnePass to access their applications may never experience the URL redirection shown above since all of their activity originates from the OnePass Landing Page. In those instances, the user will see an application in Pre-Registration appear under the **Services available for Registration** section. By clicking the link there, the user will be taken through the verification step above, but will not be required to create a profile (since they already have one).

---

**Self-Registration**

Self-Registration represents a short period of time (between 3 and 5 weeks depending on the application) after an application has been integrated into OnePass, where the users are required to create their OnePass Profiles (if they do not already have one) and bind or activate their OnePass profile to their Application Profile.

This time period represents the last opportunity a user has to join their OnePass and application credentials. Once this period ends, the user will need to contact their System Administrators to have their OnePass profiles created.

There are two ways a user can experience Self-Registration of an Application.
Self-Register an Application from the Native Application Link

1. User accesses their native application URL and is redirected to the Self-Registration screen for the given application.

2. a. If the user selects I have a Regions OnePass Profile, they will be directed to the OnePass login page and can register their application through the Landing Page (described below).

   b. If user elects to create their OnePass profile by clicking Register for Regions OnePass, they are redirected to the application verification screen.

3. User enters their application credentials and clicks Verify.

   Note: The credentials presented for verification will vary depending on the application being registered.

4. From this point, the user will enter the profile creation process referenced earlier in this user guide.

5. Once completed, the user will be directed to their Landing Page and can select their respective application under the Services Registered section to access their application.

6. If the user has other profiles for that application to register, they simply select the link again under Services available for registration and complete the verification process.

7. The user should bookmark OnePass and begin using it to access all of their Commercial Applications.
Self-Register an Application from the Landing Page

Users already utilizing OnePass to access their applications may never experience the URL redirection, since all of their activity originates from the OnePass Landing Page. In those instances, the user will see an application in Self-Registration appear under the **Services available for Registration** section. By clicking the link there, the user will be taken through the verification step above, but will not be required to create a profile (since they already have one).

Closed Registration – Administrator Action Required

Closed Registration represents the period of time after an application completes the Self-Registration period and is considered the final state of the application under OnePass. Once an application is in Closed Registration status, the users can no longer bind or activate their OnePass profiles with their applications profiles, or initiate the OnePass profile creation process without the assistance of their System Administrator. Users’ access the native application URL addresses will be routed to the OnePass Login Page, and the application name will no longer appear under the **Services available for registration** section. At this point, the System Administrator will have to create the user in OnePass and create the entitlement / activate the users OnePass profile with the application profile.

Additional Assistance

If you have questions after reading this guide, please contact Client Services at 1-800-787-3905 from 7 a.m. to 6 p.m. Central Standard Time.
This guide is for general informational and reference purposes only and is entirely subject and subordinate to
the terms of the respective written agreements for the products and services described above. This guide does
not constitute a contract or representation or warranty of any kind, express or implied, nor does it in any way
supplement, replace, modify, or amend the terms and provisions of the written agreements that govern the
products and services. You should review actual product and service agreements carefully to understand the
terms that govern the products and services and the rights, responsibilities, and liabilities of parties thereunder.