

CONTENTS

ENABLE SOFT TOKEN
FIRST-TIME SET UP
APPROVING
TRANSACTIONS WITH
SOFT TOKENS
TROUBLESHOOTING



BUSINESS ONLINE BANKING Soft Token User Guide

Questions? Please contact us at 800.350.3557, Option 2.



CONTENTS

ENABLE SOFT TOKEN

FIRST-TIME SET UP

APPROVING TRANSACTIONS WITH SOFT TOKENS

TROUBLESHOOTING

Soft tokens allow company users to use the **RSA SecurID Software Token app** on their mobile device to authenticate their identity at sign-in and/or transaction approval.

Transaction approval only applies to Wire and ACH Services.

Users can deploy multiple layers of security when logging in and approving wires and ACH by combining soft token with Out of Band Authentication (OOBA), also referred to as One Time Passcode, via SMS or telephone.

NOTE: Users cannot combine both soft token and hard token authentication.

MOBILE DEVICE REQUIREMENTS

The RSA SecurID Software Token App is supported on the following mobile platforms:

- Android OS Version 4.1 and newer
- iOS (Apple) version 8 and newer

NOTE: Blackberry OS and Windows Phone are not supported.

An internet connection is required to download the **RSA SecureID Software Token app**, and a camera is required for the activation process. Once downloaded, ensure that the app is enabled to access the camera under the Setting options for the device.

ENABLE SOFT TOKEN

A company administrator is responsible for adding Soft Token Services to users. Log in to Online Banking to activate soft tokens for each user. If you are not an administrator, you can skip to [step 6](#).

Best practice for first time Online Banking users: download the RSA SecurID Software token app from the Apple App Store or Google Play Store. The respective app displays are similar for each device type.

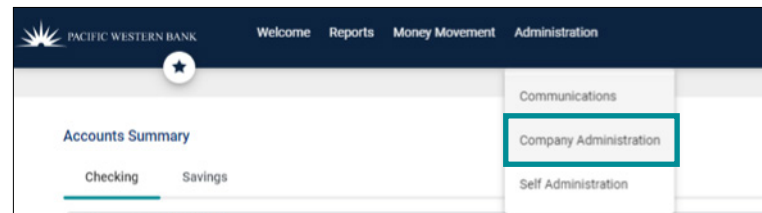
APPLE APP STORE



GOOGLE PLAY APP STORE



1. To gain access to soft tokens, you must first fill out the Online Banking Services Security Supplement. To obtain this form, please contact your relationship manager or dedicated customer service officer directly. If your company administrator has completed this form, please continue to the next step.
2. Hover over **Administration** and select **Company Administration**.



CONTENTS

ENABLE SOFT TOKEN

FIRST-TIME SET UP

APPROVING
TRANSACTIONS WITH
SOFT TOKENS

TROUBLESHOOTING

3. Click on the desired **User ID** under manage existing users.

Manage Existing Users

To manage a user's profile, roles, service & accounts, system access, or change limits, click on the appropriate user ID.

4. The user's profile will come up. Click on the edit icon next to Services & Accounts.

Services & Accounts



5. Scroll down to Soft Token Approval and click the plus (+) sign. Save at the bottom of the page.

Soft Token Approval



NOTE: Each company soft token user must complete [steps 6 - 16](#) to set up and deploy the soft token feature on their mobile device.

6. Depending on your mobile device type, download the RSA SecurID Token app in the Apple App Store or Google Play Store.

APPLE APP STORE

GOOGLE PLAY APP STORE



7. Log in to Online Banking for Business on a computer (if not already logged in).
8. You will be prompted to **set up the Software Token** when a token is required at sign-in. Click on the **Device OS** dropdown menu and select the applicable option.

Set Up Software Token Sign On

Device OS:

Continue Cancel

Device OS:

Android(OS 4.1 or higher)
Apple(iOS 8 or higher)



CONTENTS

ENABLE SOFT TOKEN

FIRST-TIME SET UP

APPROVING TRANSACTIONS WITH SOFT TOKENS

TROUBLESHOOTING

9. Click **Continue**.
10. Open the **RSA SecurID Software Token** app on your mobile device.
11. Scan the **QR code** with your device's camera.
12. Click **Continue**.



13. Once the QR code scan is successful, **create a unique eight-digit PIN** (exactly 8 digits) which can consist of numbers and letters – no special characters allowed.
14. Click **Continue**.

A screenshot of a mobile app screen titled "Set Up Software Token Sign On". Below the title is the instruction "Create your PIN.". There are two input fields: "PIN:" and "Confirm PIN:". The "PIN:" field has a red asterisk icon to its right. Below the "PIN:" field, it says "Your PIN: -> Must be 8-digits long.". The "Confirm PIN:" field also has a red asterisk icon to its right. At the bottom, there are two buttons: "Continue" and "Cancel".

15. Once you've been activated, you will be taken back to the Online Banking login screen
16. Input your current PIN and token code from the **RSA SecurID Software Token** app. You will now be logged in.

A screenshot of a mobile app screen titled "Sign in to Business eBanking". There are three input fields: "Company ID:", "User ID:", and "Passcode:". Below the "Passcode:" field, it says "Current PIN + token code:". At the bottom, there are two buttons: "Continue" and "Cancel".

CONTENTS

ENABLE SOFT TOKEN

FIRST-TIME SET UP

Login Authentication

ACH or Wire Transaction
Approvals

APPROVING TRANSACTIONS WITH SOFT TOKENS

TROUBLESHOOTING

FIRST-TIME SET UP

LOGIN AUTHENTICATION

When using a soft token for the first time, **download the RSA SecurID Software token app** from the Apple App Store or Google Play Store. The RSA SecurID Software token app logo is a cloud with a blue check mark. Once that is complete, enter your company ID and user ID. Once your company ID and User ID are validated, open the RSA SecurID Software token app, select your token, and then enter the PIN and token code.

APPLE APP STORE

A screenshot of the "Sign in to Business eBanking" form. It has two input fields: "Company ID:" with the value "111111" and "User ID:" with the value "admin". Below the fields is a blue "Continue" button. The "Company ID" and "User ID" labels are highlighted with red boxes.

GOOGLE PLAY APP STORE

A screenshot of the "Sign in to Business eBanking" form. It has two input fields: "Company ID:" with the value "2" and "User ID:" with the value "s". Below these is a "Passcode:" field with the placeholder text "Current PIN + token code.". There are blue "Continue" and "Cancel" buttons at the bottom. The "Passcode" field is highlighted with a red box.

NOTE: If you have both Soft Token Authentication and Soft Token Approval Services, you must complete the activation at sign-on; otherwise, you cannot access Online Banking. Once you complete the activation at sign-on, you are not required to complete activation again when approving an ACH or wire transaction.

ACH OR WIRE TRANSACTION APPROVALS

If you have the ability to approve transactions with a soft token, you will be required to register your token. You can delay setting up the soft token and continue to sign on, but you will not be able to approve ACH or wire transactions until you have activated your soft token at sign-on.

NOTE: PWB recommends that you complete the token approval setup when logging in. If this is delayed and not activated, you will not be able to activate it during the approval process. You will need to log out and complete activation at log on.

A screenshot of the "Set Up Software Token Sign On" form. It contains a message: "You can delay software token activation and continue signing on; however, you will be unable to approve transactions until activation is complete." Below the message is a "Device OS:" dropdown menu. At the bottom are blue "Continue" and "Cancel" buttons. The "continue signing on" text in the message is highlighted with a red box.

CONTENTS

ENABLE SOFT TOKEN

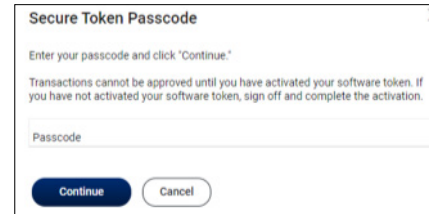
FIRST-TIME SET UP

APPROVING
TRANSACTIONS WITH
SOFT TOKENS

TROUBLESHOOTING

APPROVING TRANSACTIONS WITH SOFT TOKENS

When approving a wire or ACH transaction, you will be required to enter the secure token passcode after clicking on the transmit button. The secure token passcode includes the 8-digit PIN you created and the token code from the RSA SecurID Software Token app.



A screenshot of a web dialog box titled "Secure Token Passcode" with a close button (X) in the top right corner. The dialog contains the following text: "Enter your passcode and click 'Continue.'" followed by a smaller line of text: "Transactions cannot be approved until you have activated your software token. If you have not activated your software token, sign off and complete the activation." Below the text is a text input field labeled "Passcode". At the bottom of the dialog are two buttons: a dark blue "Continue" button and a light blue "Cancel" button.



CONTENTS

ENABLE SOFT TOKEN

FIRST-TIME SET UP

APPROVING
TRANSACTIONS WITH
SOFT TOKENS

TROUBLESHOOTING

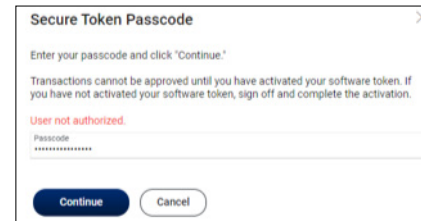
Locked User

Forgotten Password

TROUBLESHOOTING

LOCKED USER

You are allowed three unsuccessful entries before your token is locked. This will prevent you from logging in or approving transactions. You will see “user not authorized” when inputting incorrect information. You will need to contact your Online Banking company administrator to have the token reactivated.

A dialog box titled "Secure Token Passcode" with a close button (X) in the top right corner. The text inside says: "Enter your passcode and click 'Continue.'", "Transactions cannot be approved until you have activated your software token. If you have not activated your software token, sign off and complete the activation.", and "User not authorized." in red. Below the text is a passcode input field with a masked password "*****". At the bottom are two buttons: "Continue" and "Cancel".

Your company admin will need to go to your Online Banking user profile, click on System Access and deactivate the token. This will require you to reinstall the token on your mobile device.

A dialog box titled "Secure Software Token Settings". The text inside says: "Manage the software token settings for this user. Deactivate the user's software token in the case of a new, lost, or stolen mobile device. The user will be prompted to reactivate their mobile device on their next sign on.", "To enable a locked user, click reset token user.", "Software token serial number: 000415506017", and "Software token activation status: Activated". There is a button labeled "Deactivate software token" and a "Save Changes" button at the bottom.

To reinstall the token, you must return to the **ENABLE SOFT TOKEN** section above, beginning at [step 10](#).

FORGOTTEN PASSWORD

If you have forgotten your password, an admin user will need to deactivate the soft token on your Online Banking user profile. This will require you to reinstall the token on your mobile device.

A dialog box titled "Secure Software Token Settings". The text inside says: "Manage the software token settings for this user. Deactivate the user's software token in the case of a new, lost, or stolen mobile device. The user will be prompted to reactivate their mobile device on their next sign on.", "To enable a locked user, click reset token user.", "Software token serial number: 000415506017", and "Software token activation status: Activated". There is a button labeled "Deactivate software token" and a "Save Changes" button at the bottom.