CITY NATIONAL BANK
AN RBC COMPANY

PAYMENT SECURITY TOKENS

City National Business Suite® and Business Essentials User Guide

March 2021

CITY NATIONAL BANK
AN RBC COMPANY

Contents

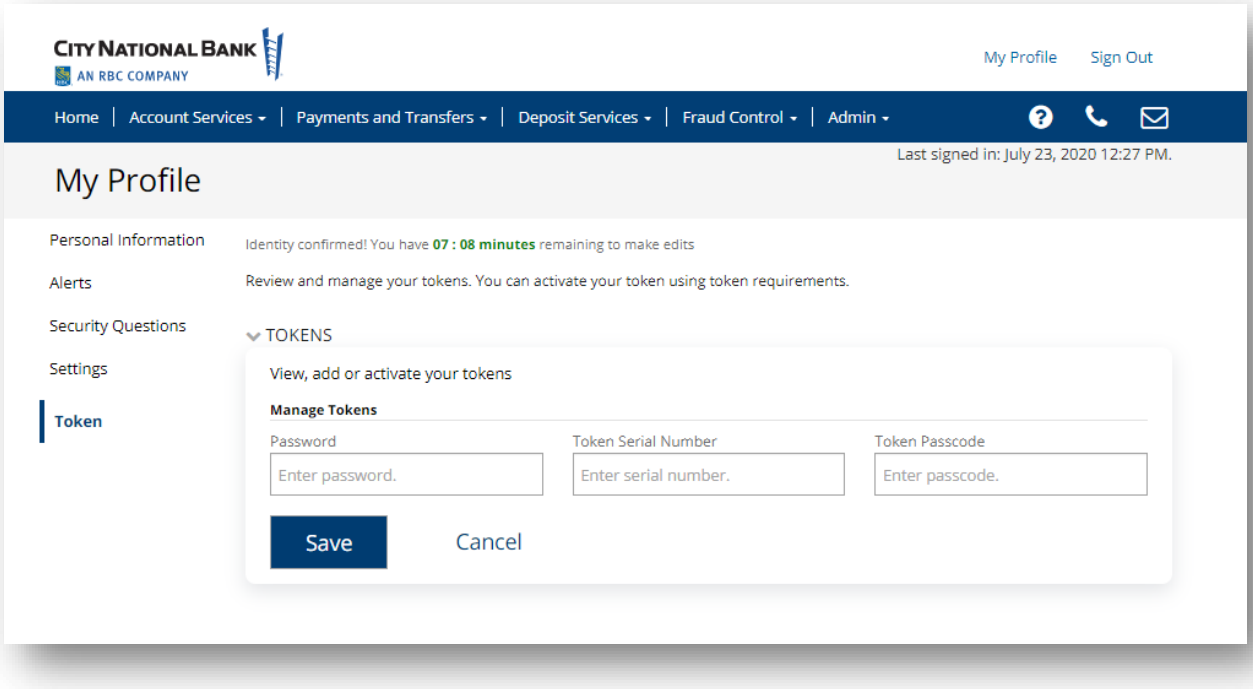
Introduction

To ensure the security of wire and ACH payment transactions, all City National Business Suite[SM] users responsible for approving such payment transactions must have a security token device in order to generate and then enter a security passcode before the transaction can be sent. These passcodes are one-time-use.

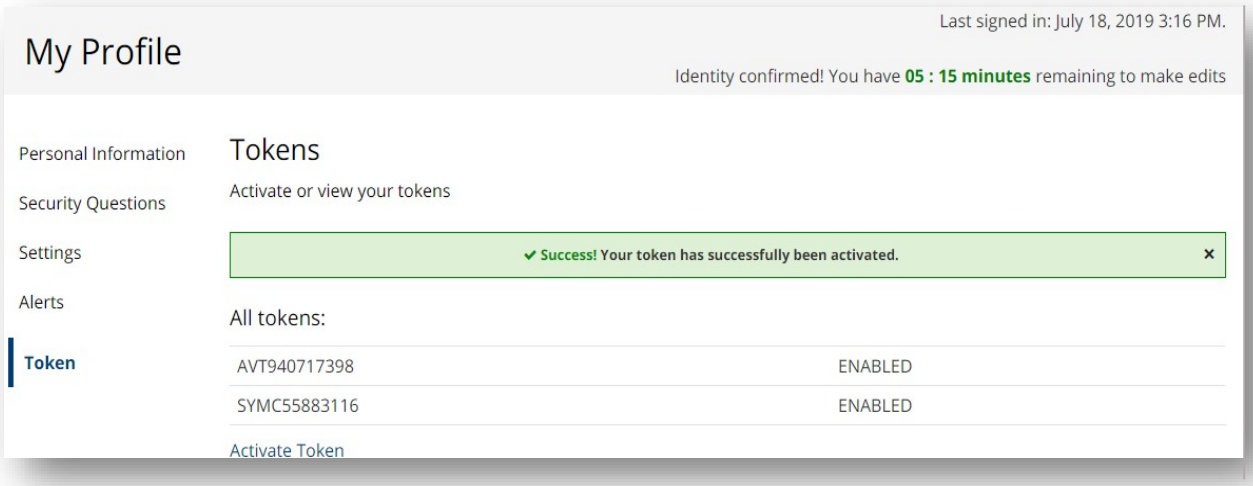
City National will provide security tokens to your Client Administrator who will then be responsible to distribute them to each user with the payment approval responsibility. This guide covers how to activate and use your security token as well as best practices for safeguarding it.

How to activate your security token

1. Select My Profile from the upper right header.
2. Complete the My Profile verification process. This if for your security since sensitive information can be updated from within My Profile.
3. Select Token from the left navigation of My Profile.
4. Enter your Business Suite password, your Token device Serial Number and the Token Passcode on the device. The Token Passcode is a code that changes every 30 seconds.



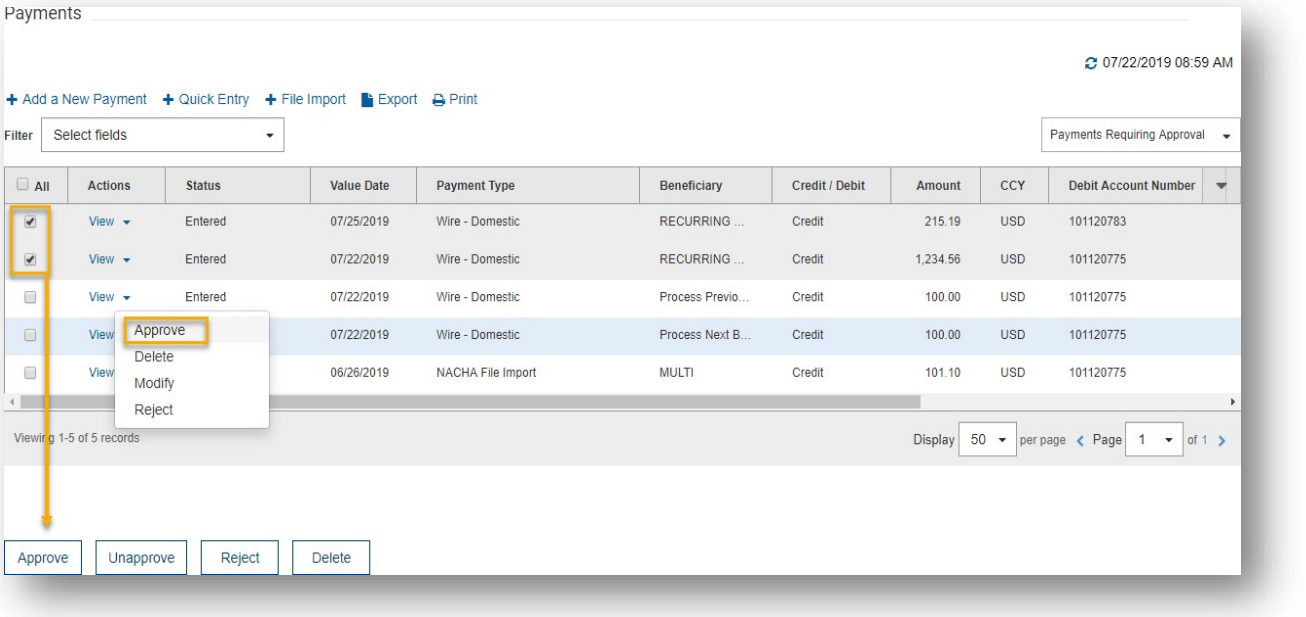
Upon successful activation, you will receive a Confirmation message that your token is activated.



How to use your security token

All Wire and ACH payments must be validated during the approval process with a one-time-use security token passcode. The following instructions explain how to use your security token passcode to approve a payment.

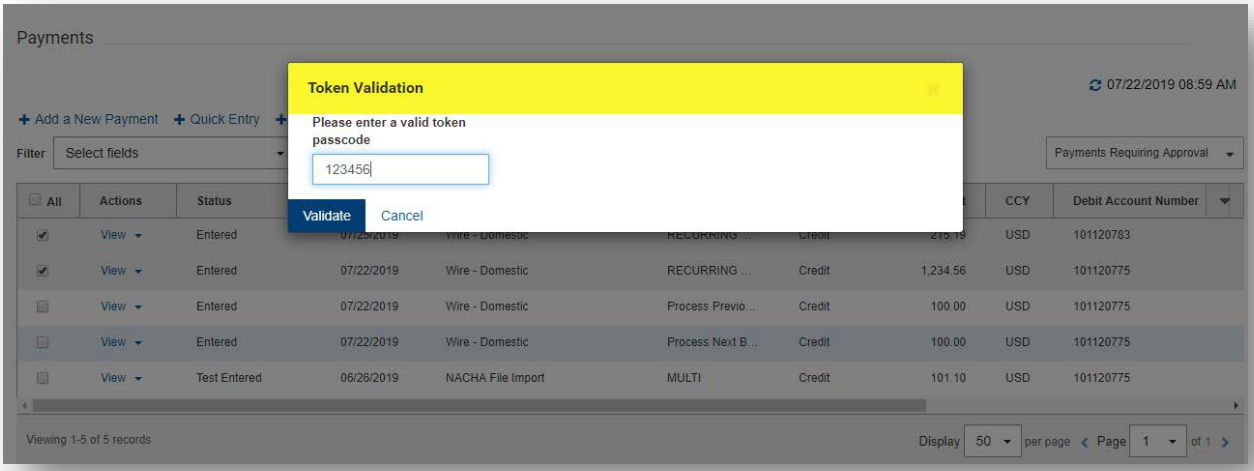
1. In the Payments List, once a payment is in Entered status, it must then be approved. To approve a payment, select Approve from an individual transaction's dropdown. Or, select multiple payments in Entered status and then select the Approve button at the bottom of the list.



Note: in some cases, if your company does not require Dual Approval (i.e., you can approve your own payments), then you will be prompted during the initial payment submission to enter your token passcode.

2. Upon selecting **Approve**, you will receive a prompt for a token passcode. Enter the 6-digit security passcode from your security device. Then click **OK**.

Note: the security passcode changes every 30 seconds.



3. If the Passcode validation and approval completes successfully, you will receive a green confirmation message listing the payments approved successfully. If it does not complete successfully, you will receive a red error message. Review the error message, if it reads “Token challenge did not complete successfully”, you may have entered the token passcode incorrectly and you may need to try again.

How to safeguard your security token and passcodes

As a user responsible for approving payment transactions via City National Business Suite, it is important to understand how to safeguard your security token and its passcodes. Please review the following guidelines.

1. **Use the security token passcode only for its appropriate function.**

   Once your security token is successfully activated, its passcode should only be used for the approve step and on the screen above designed for entering passcodes during the payment transaction workflow.

   Note: Certain malware enables fraudsters to place a security token passcode entry field on the login screen, thus you should **NEVER ENTER A PASSCODE AT LOGIN**. It would mean that you have malware on your computer. And fraudsters could then retrieve your passcode, take over your

user session, and use it to submit a fraudulent transaction.

2. **Carefully secure your security token and all of your computer and mobile devices.**

   To safeguard your security token and all devices used for banking activities, follow these recommended rules:
   - Keep your security token locked or hidden.
   - Password-protect your computer and mobile devices.

3. **Report lost or stolen security tokens immediately.**

   If you lose your security token or suspect it has been stolen, notify your Client Administrator immediately. Your Client Administrator will then be able to notify City National, who can delete the security token from your Business Suite user profile, so that it can no longer be used for payment transaction approval.

4. **Return your security token if no longer in use.**

   If your job function changes or you leave your company, be sure to return your security token to your Client Administrator who can work with City National to delete the security token from your Business Suite user profile.

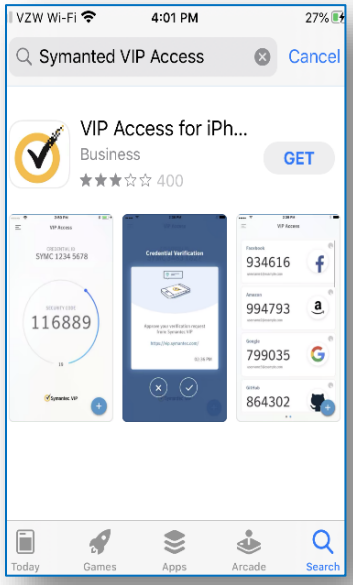
Alternative Symantec VIP Access App, aka a Mobile Soft Token

Hard tokens are City National's standard token device. However, you may opt to use the Symantec Mobile App available in the iPhone and Android App Stores.

Instruct users to download the free Symantec VIP Access Mobile App.

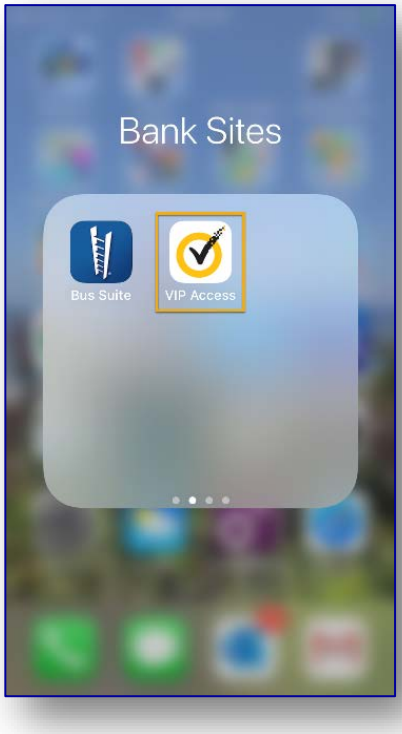
Within the App Store, search for Symantec VIP Access and select **Get** Button.

Note: Instruct your users to password-protect or otherwise secure their mobile phones when using the mobile security token.



Access the VIP Access App from the mobile phone

For instructions on how to activate and safely manage their mobile security token, refer your users to the instructions above.



Token Administration (Service Administrators)

As your company's Business Suite Service Administrator, you play a critical role in the proper implementation and maintenance of security tokens used for the approval of Wire and ACH payment transactions.

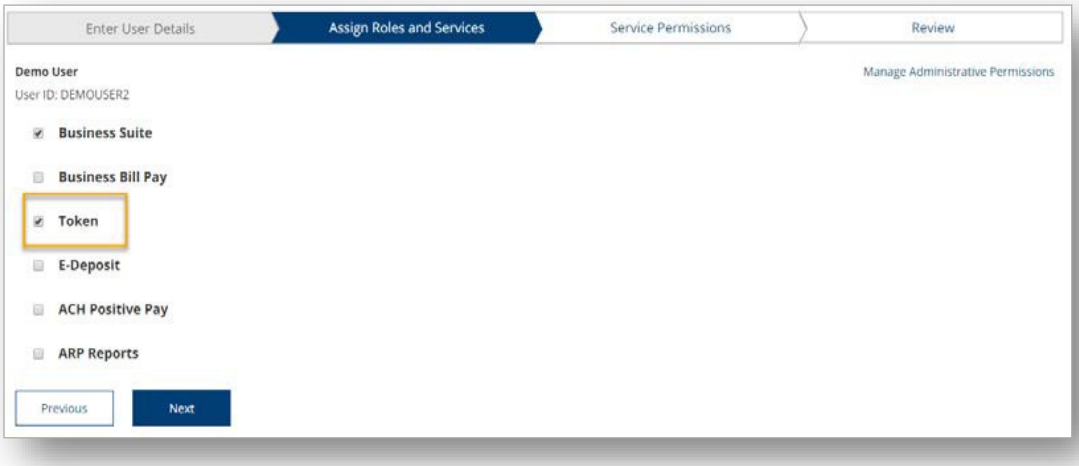
Set up Security Tokens for Payment Approver Users

When creating a new user with the function to approve Wire and ACH payments, the user must also be entitled for tokens.

1. **Request security tokens**

   We will FedEx you the number of security tokens you request as a part of the enrollment process. To request additional security tokens, please contact Treasury Management Client Services at (800) 599-0020 between 5:30 a.m. and 7:00 p.m. Pacific Time Monday through Friday.

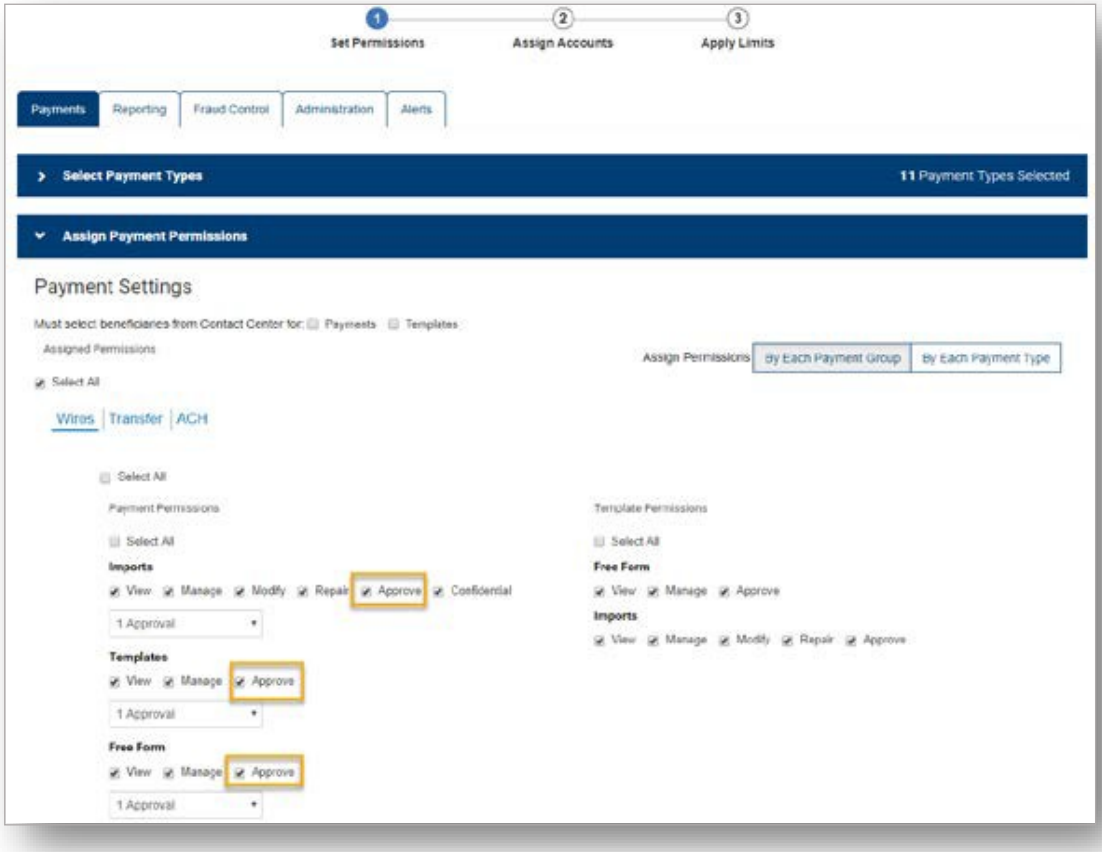
2. **Entitle all Wire and ACH approvers with Tokens.**



Users are entitled for tokens during the Assign Roles and Services step.

Assign Token to users with approve permissions for Wires and/or ACH.

Ensure users that should approve payments have the “Approve” entitlement.



3. **Provide the user with the token device**

   For instructions on how to activate and safely manage their security tokens, refer your users to the instruction above.

4. **Five active tokens, per user, is the limit.**

   Active tokens can be a combination of hard and soft tokens. If five active tokens are listed under the user's profile, the page will not display "activate token" link until they disable an active token.

Disconnecting Security Tokens from your Users

If a user no longer requires a security token, the security token may be disconnected from the user. Disconnected security tokens may be reassigned to new users.

1. **Deactivate or remove Wire and/or ACH payment approve permissions**

   Deactivate the user or remove their payment permissions as appropriate.

2. **Request that the security token(s) be deleted from the user**

   Contact Treasury Management Client Services to request that all security tokens be deleted from the user. Client services will delete tokens from the user's profile.

3. **Re-activate the security token for a new or different user** - If you still have the token, you can provide the security token to a new user by following set up procedures above.

Important note:
To safeguard the security tokens and all devices used for banking activities, instruct your users to keep their security token locked or hidden, and to password-protect their computers and mobile phones.

Frequently Asked Questions

What is a security token?

A security token is a device or application that provides a one-time passcode for use with online transactions. Because a passcode cannot be re-used, it is more secure than using just a user ID and password at login that could be obtained by fraudsters in a variety of ways and then re-used to access your service. Physical or hard tokens are City National's standard token device.

May I opt out of using a security token?

No, a security token must always be used by Business Suite users who are responsible for approving wire and ACH payments.

Is there a soft token mobile app option?

Hard tokens are City National's standard token device. However, users may opt to also use the Symantec VIP Access Mobile App available in the iPhone and Android App Stores.

Do I need to securely store my security token?

Yes, you should safeguard your security token and all devices used for banking by locking or hiding your security token and by password/PIN-protecting your computer and mobile devices.

Can security tokens be shared?

No, you should not share your security token. Each user who requires a security token for payment approval should be provided his or her own individual security token. Please note there is no charge for additional security tokens.

Is there a limit for how many tokens I can have?

Yes, there is a limit of 5 active tokens, per user, that can be a combination of hard and soft tokens.

When do I use the security token?

Every time you approve a wire or ACH payment transaction, the Business Suite service will prompt you for a "PASSCODE." Enter the six-digit one-time Passcode from the security token. For further assistance, refer to the procedures above.

Will my pop-up blocker affect my ability to use the security token?

Yes, the "Enter your PASSCODE" window is a pop-up, so if you normally block these, you will need to add Business Suite as a "trusted site" for the browser(s) you use.

What do I do with my physical or hard security token if I leave my job?

Return the security token to your Client Administrator.

What do I do if I my security token is lost, stolen or damaged?

If you believe that your security token is lost, has been stolen or is damaged or your mobile device with the Symantec VIP Access app has been lost or stolen, inform your Client Administrator immediately. Your Client Administrator can then contact City National Client Services to disconnect the security token from your user profile and provide you with a new security token.

When do I use the security token?

Every time you approve a wire or ACH payment transaction, the Business Suite service will prompt you for a "PASSCODE." Enter the six-digit one-time Passcode from the security token. For further assistance, refer to the procedures above.

Will my pop-up blocker affect my ability to use the security token?

Yes, the "Enter your PASSCODE" window is a pop-up, so if you normally block these, you will need to add Business Suite as a "trusted site" for the browser(s) you use.

What do I do with my physical or hard security token if I leave my job?

Return the security token to your Client Administrator.

What do I do if I my security token is lost, stolen or damaged?

If you believe that your security token is lost, has been stolen or is damaged or your mobile device with the Symantec VIP Access app has been lost or stolen, inform your Client Administrator immediately. Your Client Administrator can then contact City National Client Services to disconnect the security token from your user profile and provide you with a new security token.