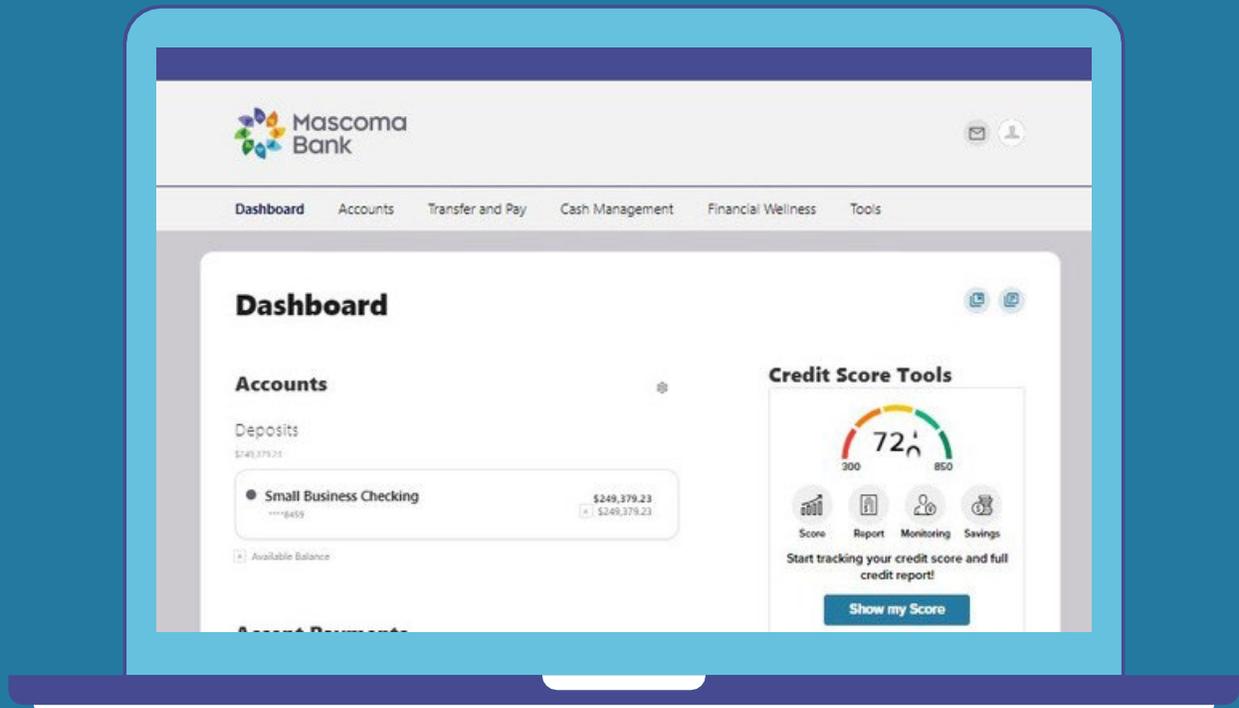


Digital Banking Security Token User Guide

Hard Tokens



Setting up Security Tokens

Physical/Hard Token

1. After logging in to the digital banking platform, go to the “Tools” widget then select “Settings” and navigate to the “Security” sub tab.

The screenshot displays the 'Settings' page in a digital banking application. The top navigation bar includes 'Dashboard', 'Accounts', 'Transfer & Pay', 'Cash Management', 'Card Management', 'Financial Wellness', and 'Tools'. The 'Tools' menu is open, showing 'Settings' (highlighted), 'Check Services', 'Alerts', 'Locations', and 'Message Center'. The 'Settings' page has sub-tabs for 'Profile', 'Security' (selected), 'Contact', 'Company Info', 'Accounts', and 'Applications'. The 'Security' section includes:

- Username and Password:** Username '2fatester' (with 'Edit' link) and Password '*****' (with 'Edit' link).
- Two-Factor Authentication:** 'Require at each login' is toggled on.
- SMS:** '0 Phone Numbers' (with 'View Details' link) and a toggle switch.
- Email:** '1 Email Addresses' (with 'View Details' link), 'PREFERRED METHOD' badge, and a toggle switch.
- Authentication App:** 'Authentication App Not Enrolled' (with 'View Details' link) and a toggle switch.
- Voice Call:** '0 Phone Numbers' (with 'View Details' link') and a toggle switch.
- Tokens:** '0 Tokens' (with 'View Details' link) and a toggle switch.

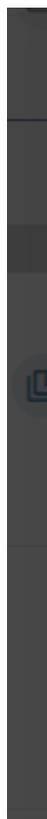
2. Under the “Two-Factor Authentication” section, locate the “Tokens” option and click “View Details”

Two-Factor Authentication

Require at each login

SMS 0 Phone Numbers View Details	<input type="checkbox"/>	Email 1 Email Addresses View Details	PREFERRED METHOD <input checked="" type="checkbox"/>
Authentication App Authentication App Not Enrolled View Details	<input type="checkbox"/>	Voice Call 0 Phone Numbers View Details	<input type="checkbox"/>
Tokens 0 Tokens View Details	<input type="checkbox"/>		

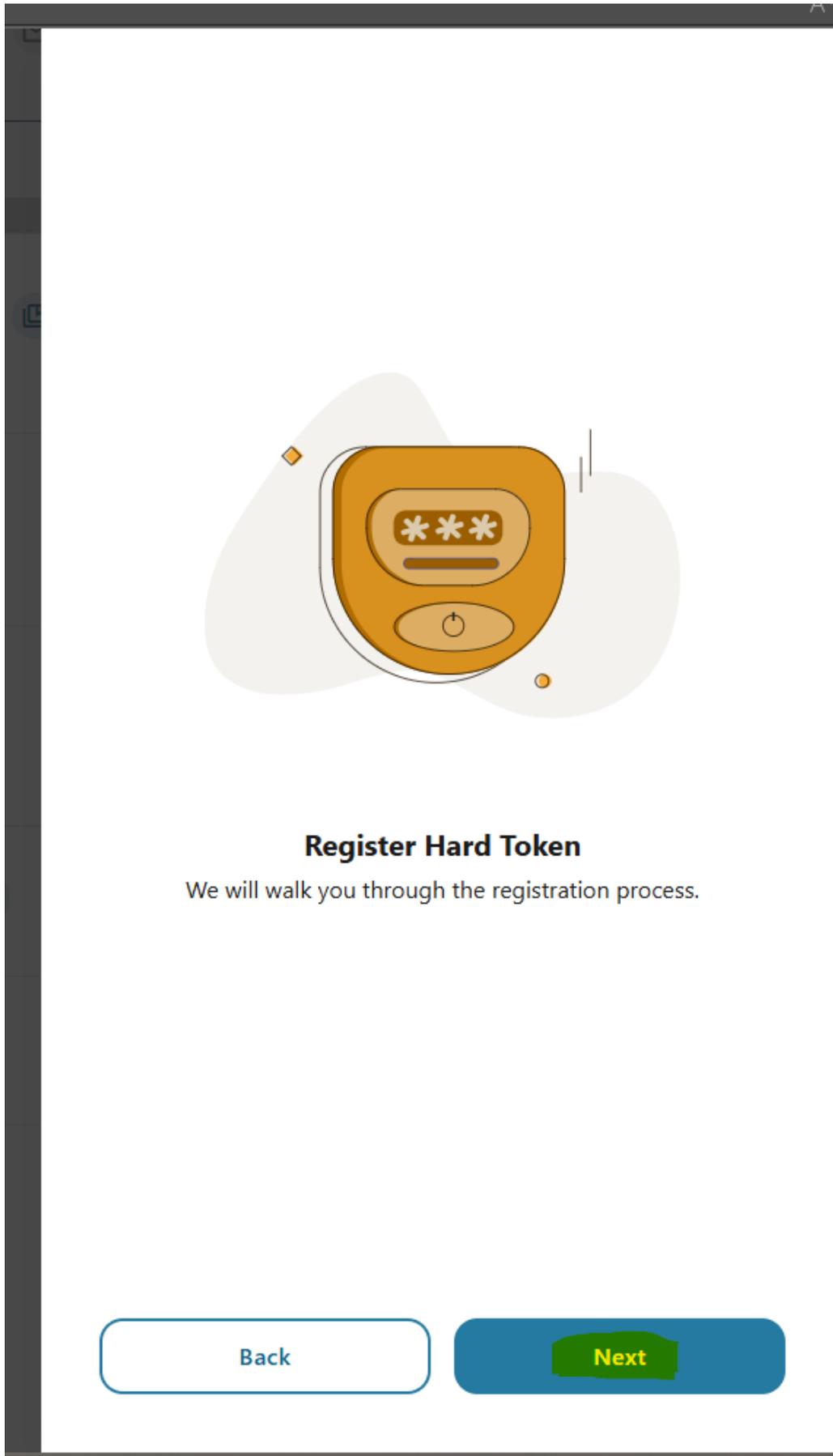
3. From the pop-out window choose “Register Hard Token”



Add New Token

- Soft Token** >
A software-based security token that generates a single-use login PIN.
- Register Hard Token** >
A hardware-based security token that generates a single-use login PIN.
- Request Hard Token** >
Send a request for a hardware-based security token to be provided to you.

4. Hit “Next”



Back

Next

5. Enter a nickname for your new token and the serial number as seen on the back of your hard token.

Register Hard Token

Enter a name for your token and the serial number from the back of the hard token.

Token Name

Kayla's Token

13 / 50

Token Serial Number

0200917386

6. Token serial number is located on the back of the token.



7. Click token button to receive first token code. Enter the code then hit “Submit”

Enter First Token Code

Press and hold the button on your token until the first code appears.

First Token Code

53195176

Back

Submit

8. Press and hold the token button until you receive a new code. Enter the second code then hit "Submit"

Enter Second Token Code

Press and hold the button again to receive the second code.

Second Token Code

09112738

Back

Submit

9. You will receive the following confirmation message. Hit “Done”



Hard Token Registered Successfully

Your new token has been added and may now be used for Two-factor Authentication.

Done

10. Set token as preferred authentication method.

Tokens

Tokens generate a code that can be used in place of a one-time password.

 **Kayla's Token** Delete
SN: 0200917324
Last Used: Never used

[+ Add New Token](#)

Set As Preferred Method

Tokens will appear as the first option when using Two-factor Authentication.

Cancel

Save