

**Multi-Factor Authentication Overview**

Cardinal requires Multi-Factor Authentication (MFA) to access the **Cardinal Portal** from outside the Commonwealth of Virginia (COV) network. When users log into Cardinal from outside the COV network for the first time, they are prompted to configure MFA. If the user does not select the **do not challenge me on this device again** option, they will be prompted to enter the information based on the authentication option selected when they configured MFA. There are three options available in VITA (Okta) for enabling MFA:

- **SMS Authentication:** Requires you to have a mobile phone registered in the United States or Canada. This function generates a random authentication code and sends a text to your mobile phone (standard text messaging rates apply).
- **Voice Call Authentication:** Requires you to have access to a phone (mobile or land line) registered in the United States or Canada. This function generates a random authentication code and places a call to the phone number set up and the code is verbally stated for entry.
- **Google Authenticator** (not recommended by Cardinal): Requires you to download the **Google Authenticator** app to your mobile device (must be Apple, Android, or Blackberry) and standard data usage rates apply.

This Job Aid provides the steps to configure MFA for the options listed above.

We are recommending you utilize a current version of either the Chrome or Internet Explorer browser when accessing Cardinal. If issues are encountered with one of these browsers, try the other browser option. If you experience issues, please submit a Helpdesk ticket via email to [VCCC@vita.virginia.gov](mailto:VCCC@vita.virginia.gov) and include the word **Cardinal** in the subject line of the email.

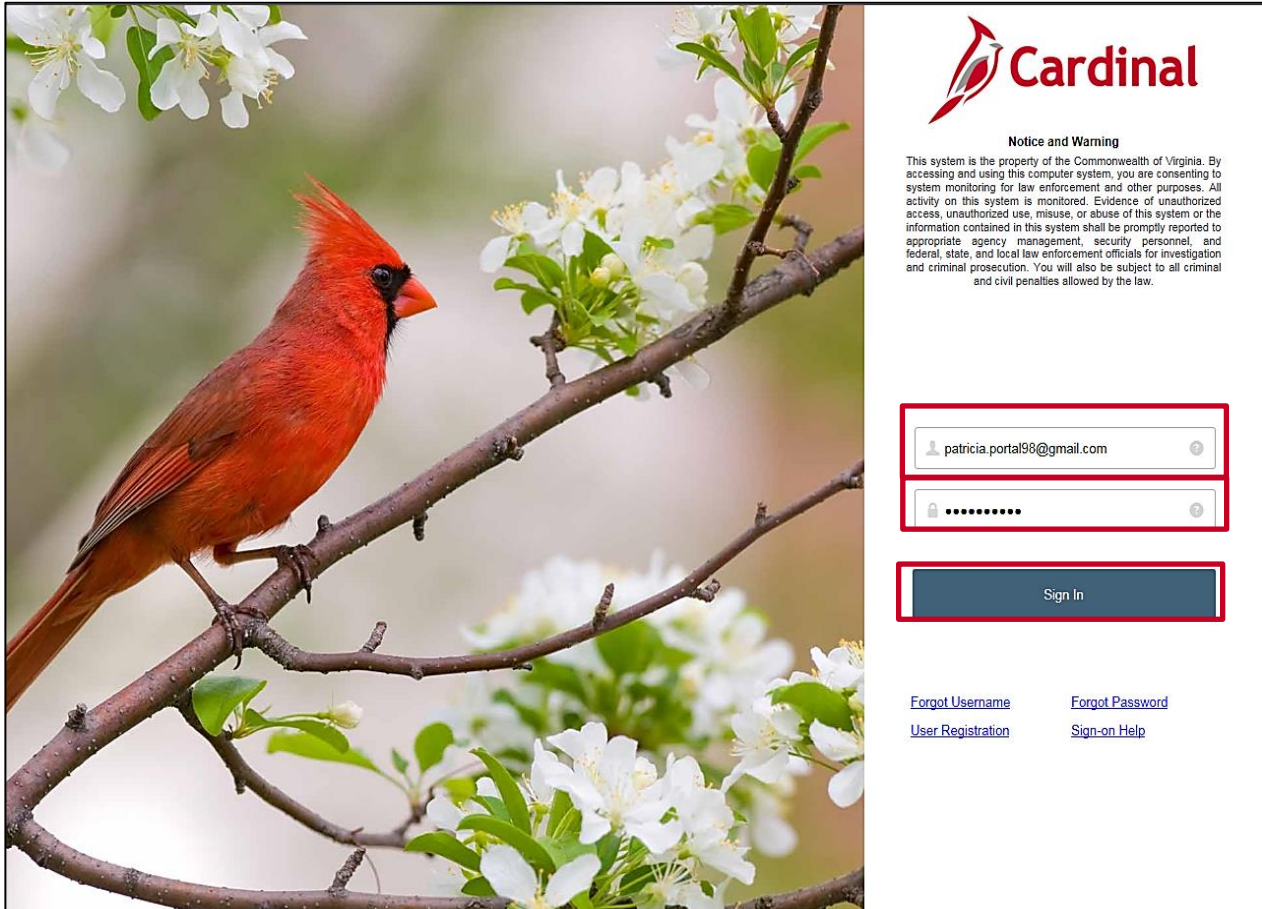
**Table of Contents**

Accessing Multi-Factor Authentication .....	3
Setting Up SMS Authentication .....	6
Logging in After Setting up SMS Authentication .....	11
Setting Up Voice Call Authentication.....	14
Logging in After Setting up Voice Call Authentication.....	20
Appendix.....	22
Setting Up Google Authenticator .....	22
Barcode – Can’t scan .....	29
Logging in After Setting up Google Authenticator .....	35

### Accessing Multi-Factor Authentication

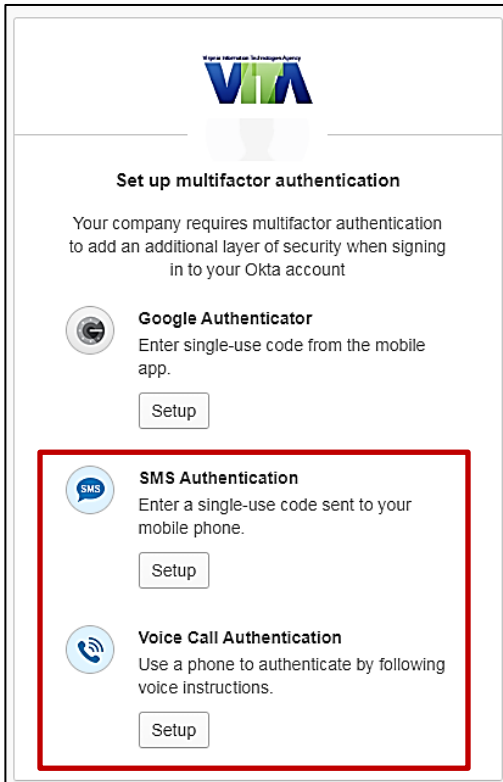
1. Start by entering the following URL in your computer browser: [my.cardinal.virginia.gov](https://my.cardinal.virginia.gov).

The **Cardinal Login** page displays.



2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
  - a. COV users: enter your network password.
  - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.

When you are outside the Commonwealth of Virginia (COV) network, the **VITA Set up multifactor authentication** page displays.



5. Go to the appropriate section in this Job Aid based on the authentication method you choose.

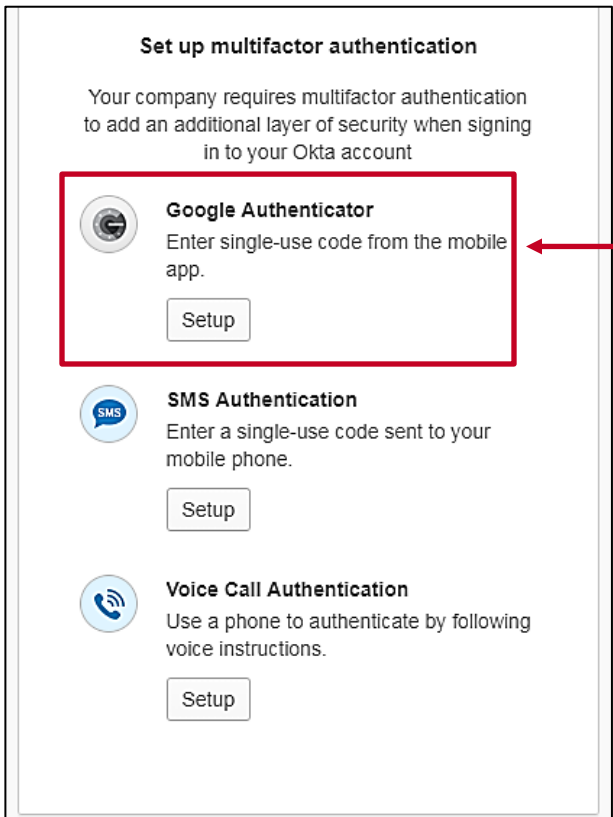
MFA options:

a. **SMS Authentication**

- Your mobile phone must be registered in the United States or Canada to select this option
- A text message is sent to your mobile phone with an authentication code you will need to enter on your computer/device
- Standard text messaging rates apply

b. **Voice Call Authentication**

- Your phone must be registered in the United States or Canada to select this option
- Once you enter your phone number (mobile or land line) in the system, a phone call is placed to the number. Once you answer the call, the code is verbally stated twice
- Enter the code into your computer/device



**Google Authenticator** is not recommended by Cardinal. See the Appendix section of this Job Aid for more information about this option.

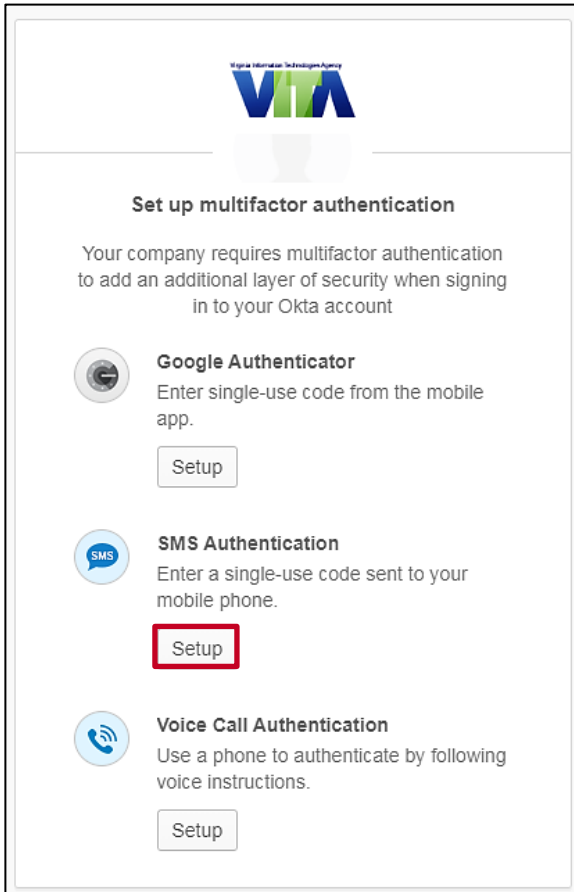


- c. **Google Authenticator** is not recommended by Cardinal – see the **Appendix** to use this option)
- You must have an Apple, Android, or Blackberry mobile device
  - You must download the Google Authenticator app to your mobile device
  - Standard data usage rates apply

**Note:** If you are using an online version of this Job Aid, click on one of the options above to access that portion of the Job Aid.

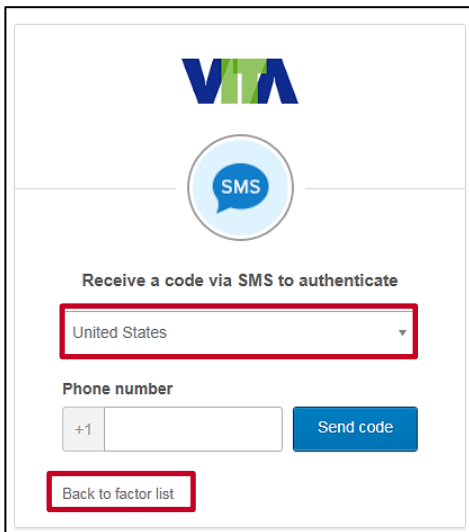
### Setting Up SMS Authentication

Receive a One-Time Passcode (OTP) via SMS. A random authentication code is generated on your mobile phone (standard text messaging rates apply). Your mobile phone must be registered in the United States or Canada to select this option.



1. Click the **Setup** button under the **SMS Authentication** section of the screen.

The **SMS** page displays.



VITA

SMS

Receive a code via SMS to authenticate

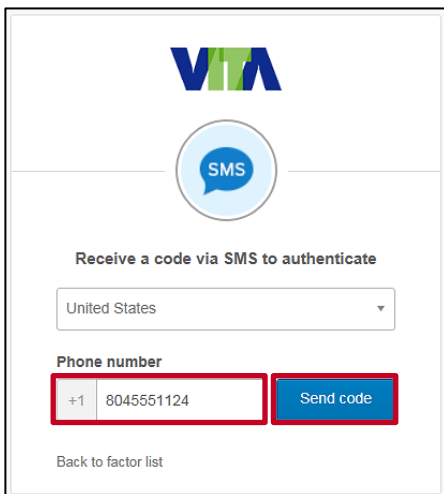
United States

Phone number

+1  Send code

Back to factor list

2. In order to use this option, you must have a mobile phone registered in the United States or Canada. **“United States”** defaults in the **Country** field.
  - a. If your phone is registered in the United States, go to the next step.
  - b. If your phone is registered in Canada, click the drop-down menu, select **Canada**, and then go to the next step.
  - c. If your phone is not registered in the United States or Canada, click the **Back to factor list** link to return and choose another method for authentication.



VITA

SMS

Receive a code via SMS to authenticate

United States

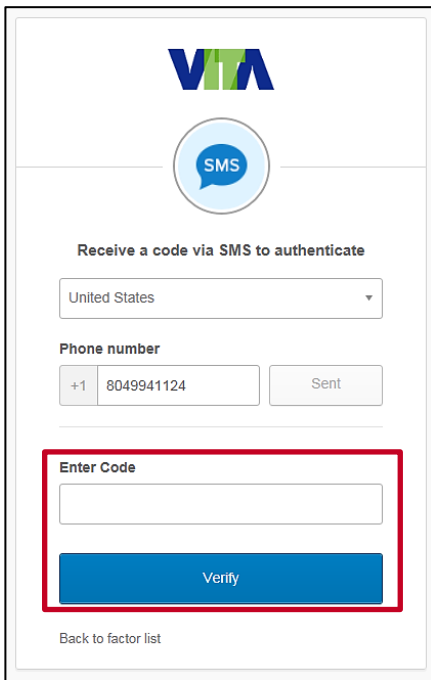
Phone number

+1 8045551124 Send code

Back to factor list

3. Enter your mobile phone number including area code with no dashes into the **Phone Number** field.
4. Click the **Send code** button.

The page refreshes and an **Enter Code** field and **Verify** button display.

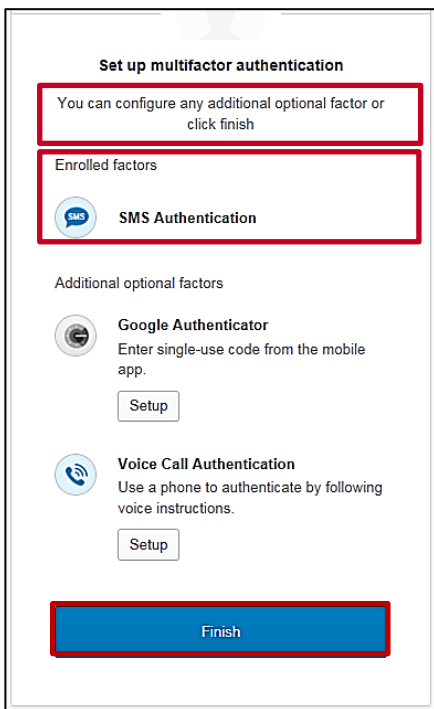


The screenshot shows the Cardinal Multi-Factor Authentication interface. At the top, there is the VITA logo and an SMS icon. Below this, the text "Receive a code via SMS to authenticate" is displayed. A dropdown menu shows "United States". Under "Phone number", there is a field with "+1 8049941124" and a "Sent" button. The "Enter Code" field and the "Verify" button are highlighted with a red box. At the bottom, there is a "Back to factor list" link.

5. A text message displays on your mobile phone with the authentication code. Enter the authentication code into the **Enter Code** field.
6. Click the **Verify** button.



The **Set up multifactor authentication** page displays.

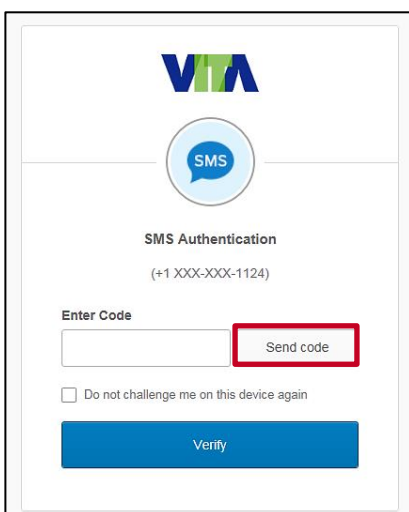


7. A message indicates that you can configure additional optional options or click finish. The authentication option you selected displays under the **Enrolled factors** section of the page.

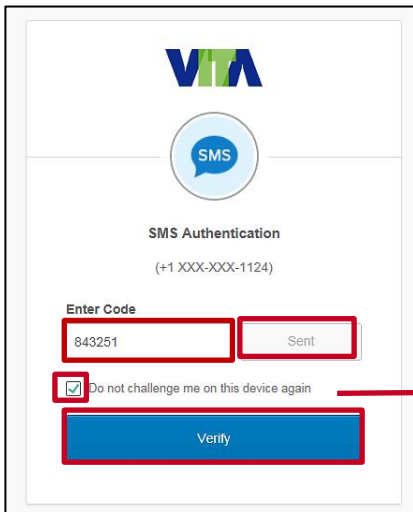
**Note:** If you are using Chrome, you will see a green checkmark next to your enrolled factor.

8. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the Cardinal Portal.

The **SMS Authentication** page redisplay.



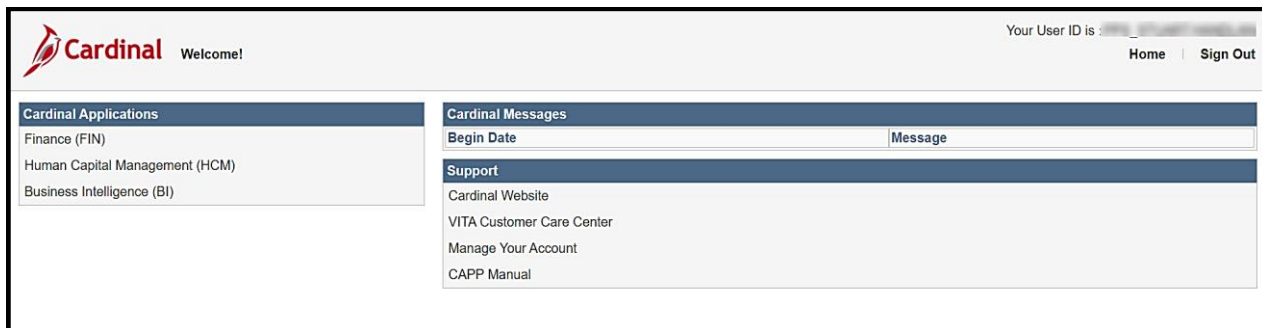
9. Click the **Send code** button to send a new authentication code.



Do not select this option if this is a shared computer/device.

10. An authentication code is sent to your mobile device. Enter the authentication code that displays on your mobile device in the **Enter Code** field on your computer/device.
11. To skip this step in the future, select the **Do not challenge me on this device again** check-box. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.
- Note:** If you clear the browser cache on your computer/device, you will need to enter the authentication code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the authentication code, to have settings added back to the computer/device.
12. Click the **Verify** button to access the **Cardinal Portal**.

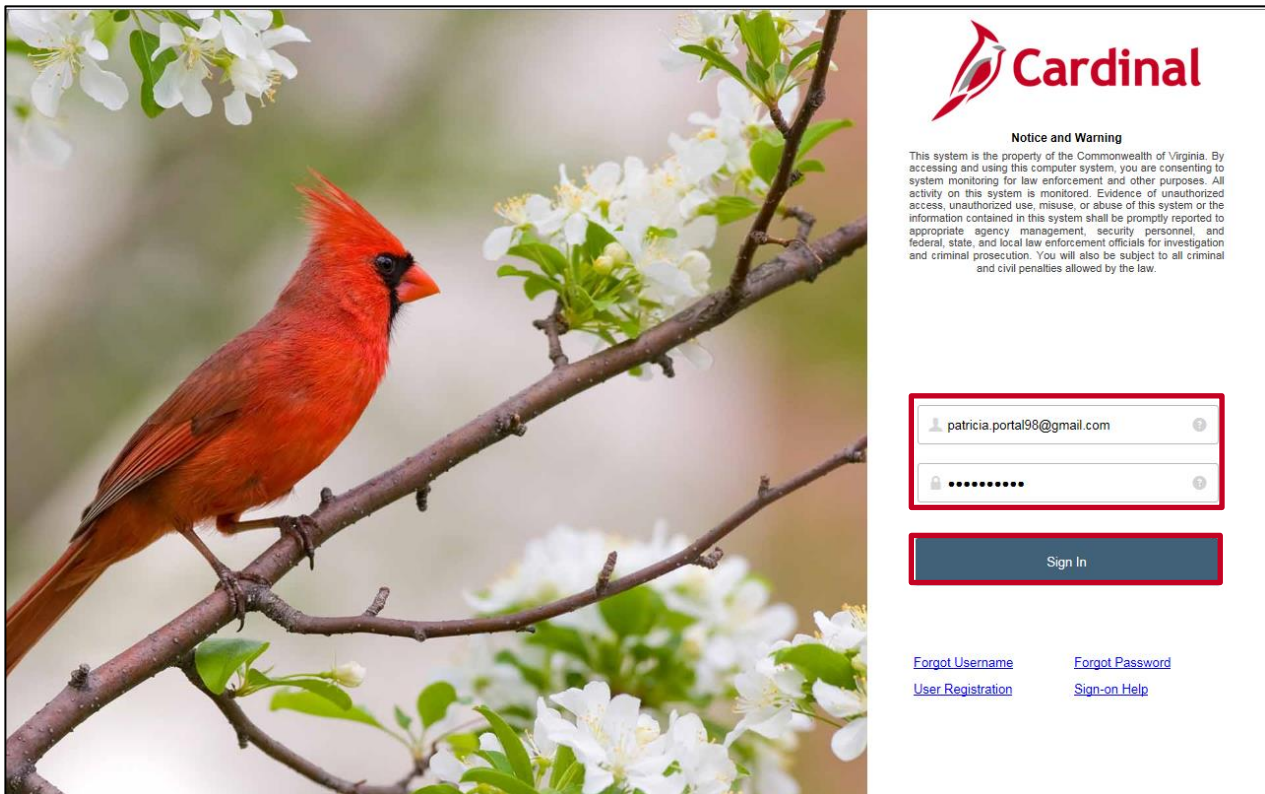
The **Cardinal Portal** displays.



### Logging in After Setting up SMS Authentication

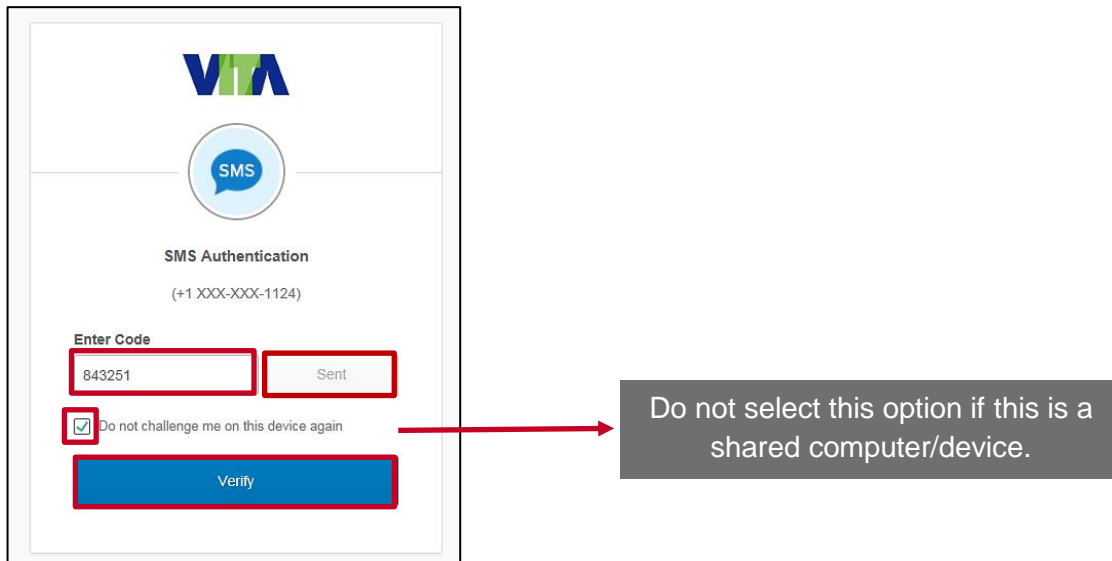
1. Start by entering the following URL in your computer browser: [my.cardinal.virginia.gov](https://my.cardinal.virginia.gov).

The **Cardinal Login** page displays.



2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
  - a. COV users: enter your network password.
  - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.

The **SMS Authentication** page displays.

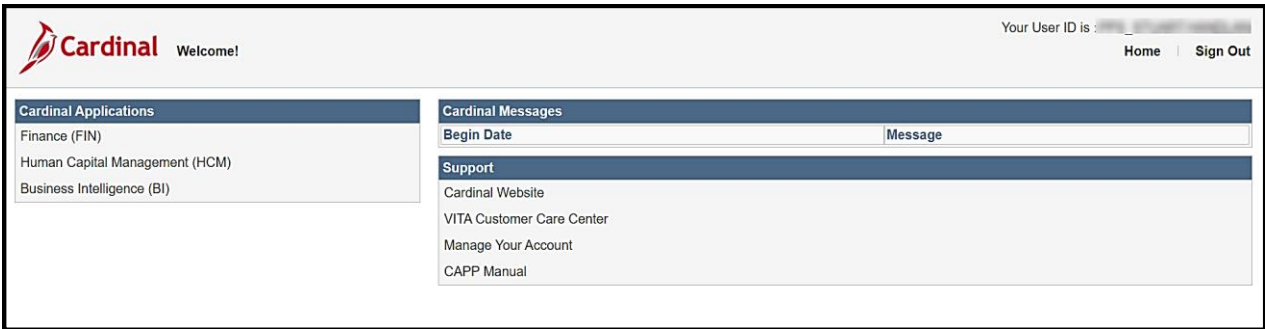


5. Click the **Send code** button.
6. Enter the authentication code received in the **Enter Code** field on your computer/device.
7. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

**Note:** If you clear the browser cache on your computer/device, you will need to enter the response again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the response, to have settings added back to the computer/device.

8. Click the **Verify** button.

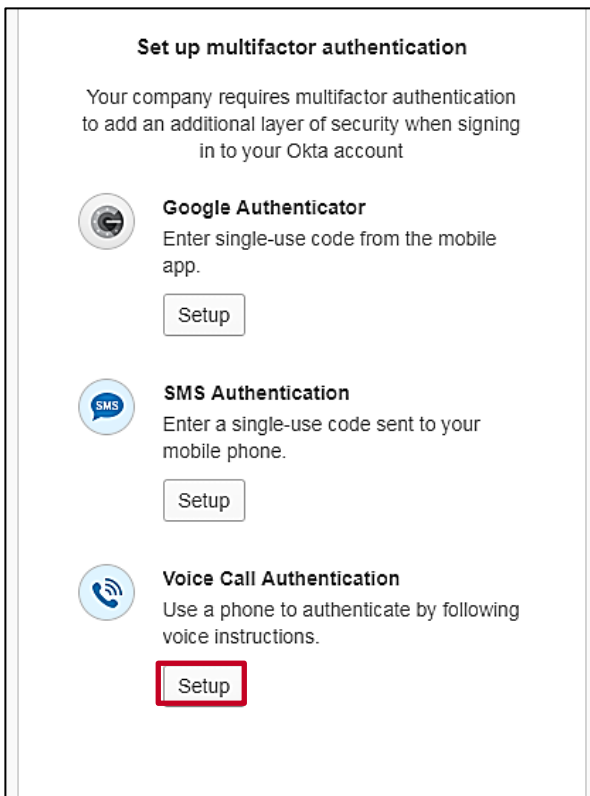
The **Cardinal Portal** displays.



The screenshot shows the Cardinal Portal interface. At the top left is the Cardinal logo and the text "Welcome!". At the top right, it says "Your User ID is:" followed by a blurred area, and links for "Home" and "Sign Out". The main content area is divided into two columns. The left column is titled "Cardinal Applications" and lists "Finance (FIN)", "Human Capital Management (HCM)", and "Business Intelligence (BI)". The right column is titled "Cardinal Messages" and contains a table with two columns: "Begin Date" and "Message". Below the messages section is a "Support" section with links for "Cardinal Website", "VITA Customer Care Center", "Manage Your Account", and "CAPP Manual".

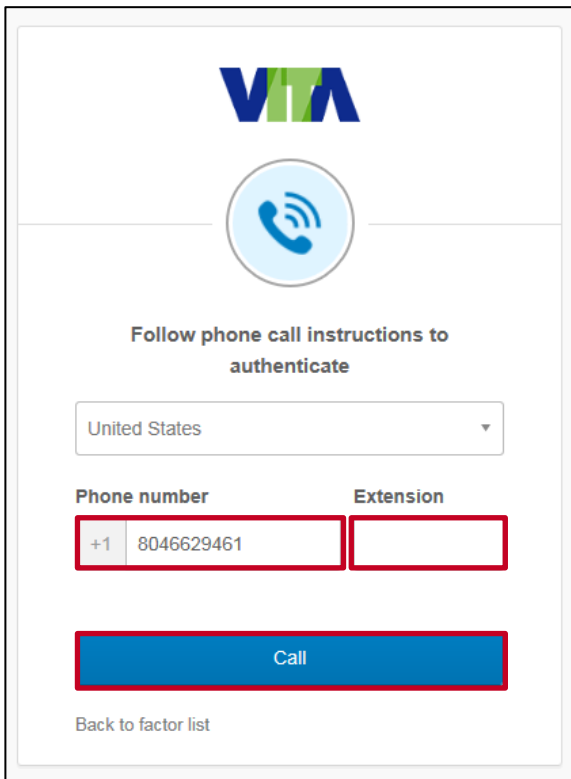
### Setting Up Voice Call Authentication

This additional authentication option allows you to use a mobile or land line to receive an authentication code. After entering your phone number and requesting the code, you will receive a call to the number you entered (land line or mobile). When you answer the call, a voice recording provides the authentication code you need to enter.



1. Under **Voice Call Authentication**, click the **Setup** button.

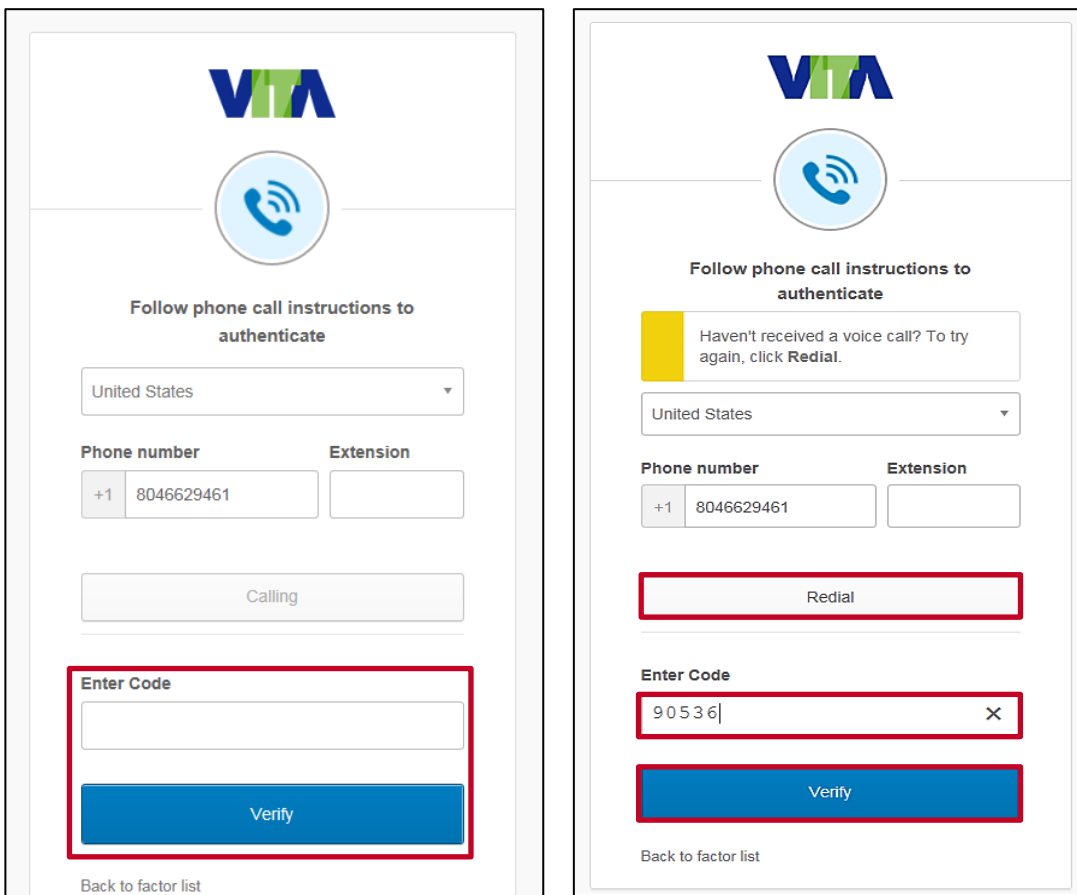
The **Follow phone call instructions to authenticate** page displays.



The screenshot shows a web interface for multi-factor authentication. At the top is the VITA logo. Below it is a circular icon of a telephone handset. The main heading is "Follow phone call instructions to authenticate". There is a dropdown menu for the country, currently set to "United States". Below that are two input fields: "Phone number" and "Extension". The "Phone number" field contains "+1 8046629461". The "Extension" field is empty. A blue button labeled "Call" is positioned below the input fields. At the bottom left, there is a link that says "Back to factor list".

2. Enter the phone number you want to receive the call in the **Phone Number** field with no dashes. The phone number can be either a mobile or land line phone, registered in the United States or Canada.  
If the phone requires an extension, enter it in the **Extension** field.
3. Click the **Call** button.

The page refreshes and an **Enter Code** field and **Verify** button display.



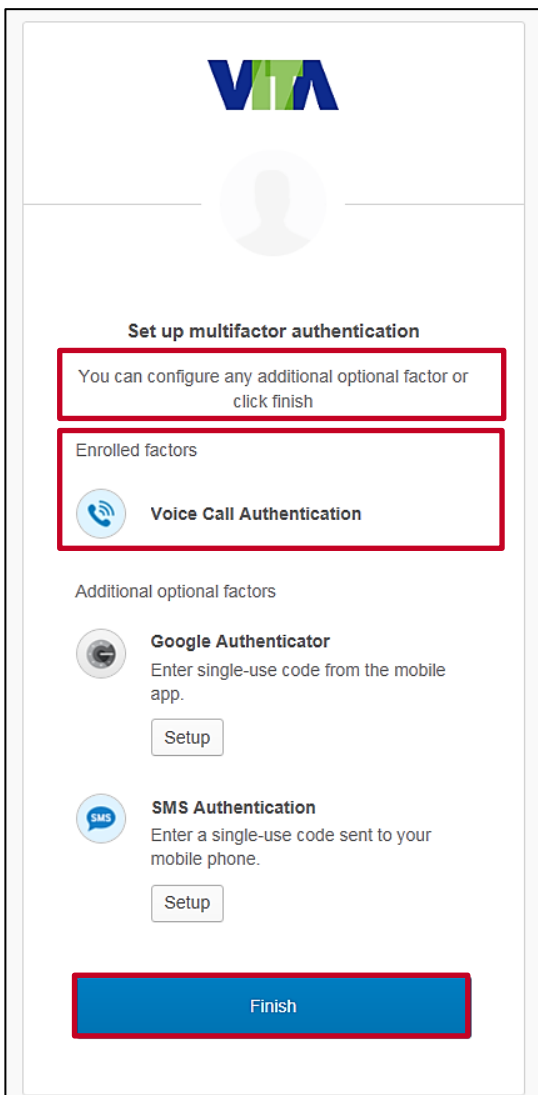
The image displays two screenshots of the VITA (Voice Interactive Transaction Authentication) interface. Both screenshots feature the VITA logo at the top and a phone icon. The left screenshot shows the 'Calling' state, with a 'Calling' button and an 'Enter Code' field and 'Verify' button highlighted in red. The right screenshot shows the 'Redial' state, with a 'Redial' button and an 'Enter Code' field containing '90536' and a 'Verify' button highlighted in red. A yellow message box in the right screenshot reads: 'Haven't received a voice call? To try again, click Redial.'

**Note:** The **Call** field changes to **Calling** when the call is in process and **Redial** after the call has disconnected. A message displays “**Haven’t received a voice call? To try again, click Redial.**”

4. A call is made to the number you entered. When you answer the call, a voice recording says: “**Hello. Thank you for using our phone verification system. Your code is XXXXX. Once again your code is XXXXX. Goodbye.**” The call then disconnects.
5. Enter the authentication code received in the **Enter Code** field on your computer/device.
6. Click the **Verify** button.

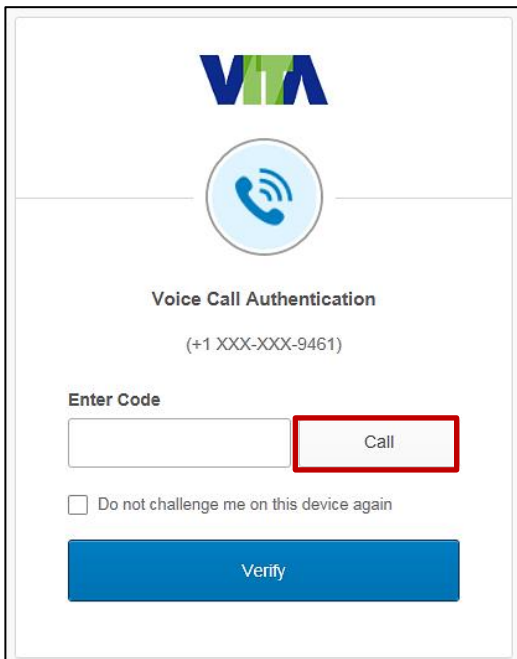


The **Set up multifactor authentication** page displays.



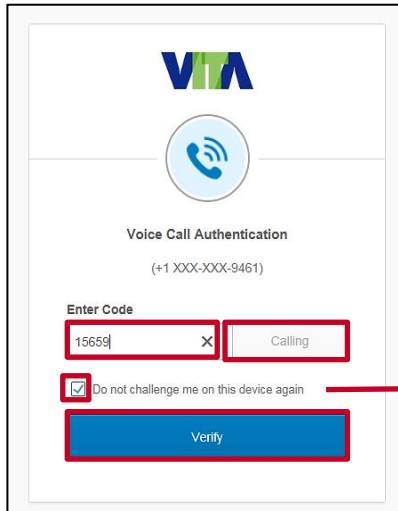
7. A message indicates that you can configure additional optional options or click finish. The authentication option you selected displays under the **Enrolled factors** section of the page.  
**Note:** If you are using Chrome, you will see a green checkmark next to your enrolled factor.
8. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the **Cardinal Portal**.

The **Voice Call Authentication** page displays.



The screenshot shows a web interface for Voice Call Authentication. At the top is the VITA logo. Below it is a circular icon with a blue telephone handset and signal waves. The text "Voice Call Authentication" is centered, followed by the phone number "(+1 XXX-XXX-9461)". There is a label "Enter Code" above a text input field. To the right of the input field is a "Call" button, which is highlighted with a red border. Below the input field is a checkbox labeled "Do not challenge me on this device again". At the bottom is a large blue "Verify" button.

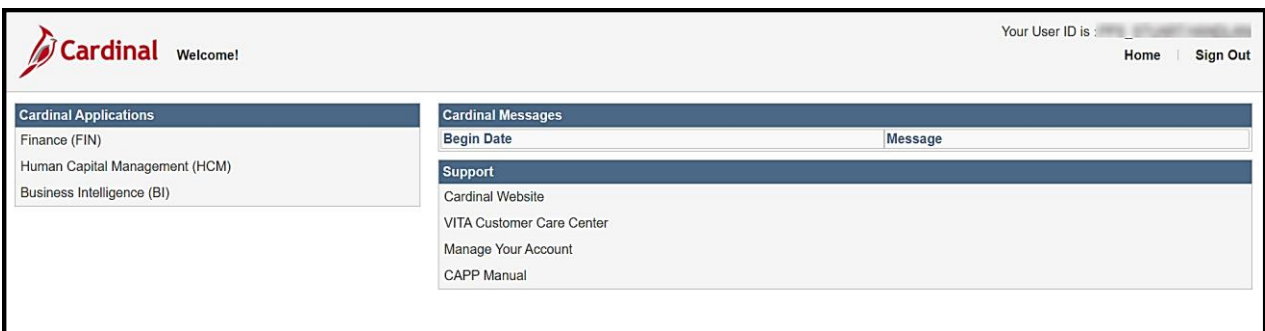
9. Click the **Call** button to receive a new authentication code.



Do not select this option if this is a shared computer/device.

10. Once you receive the call, enter the authentication code in the **Enter Code** field on your computer/device.  
**Note:** The **Call** field changes to **Calling** when the call is in process and **Redial** after the call has disconnected.
11. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.  
**Note:** If you clear the browser cache on your computer/device, you will need to enter the authentication code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the authentication code, to have settings added back to the computer/device.
12. Click the **Verify** button to access the **Cardinal Portal**.

The **Cardinal Portal** displays.

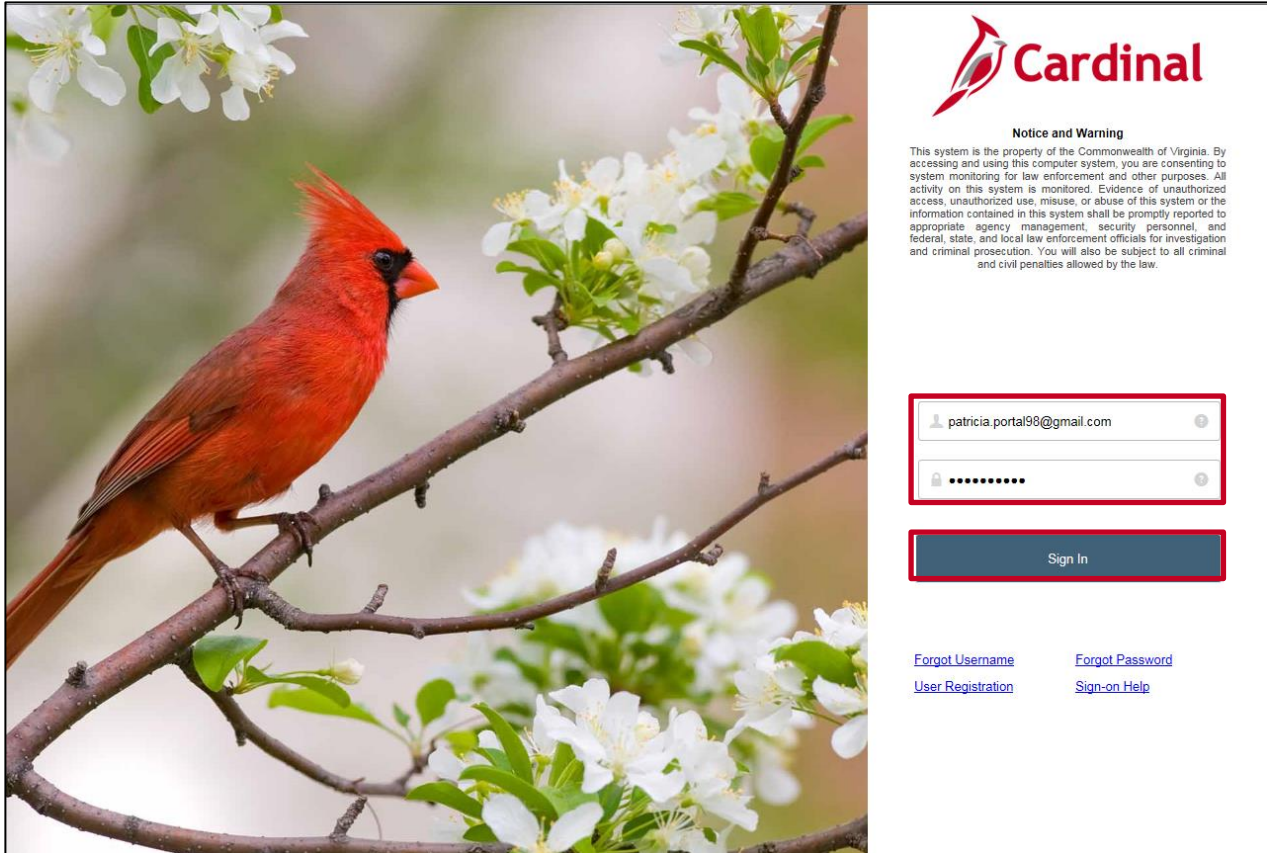


### Logging in After Setting up Voice Call Authentication

The next time you use the same computer/device to log in to the **Cardinal Portal**, the authentication option you selected is retained.

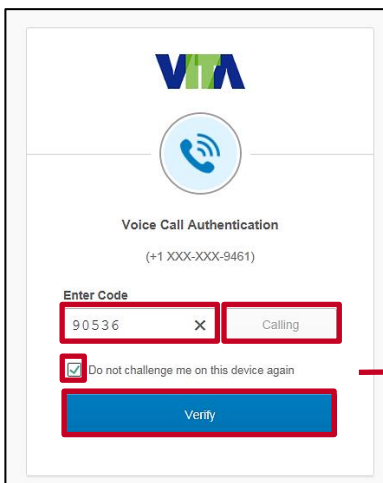
1. Start by entering the following URL in your computer browser: [my.cardinal.virginia.gov](https://my.cardinal.virginia.gov).

The **Cardinal Login** page displays.



2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
  - a. COV users: enter your network password.
  - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.

The **Voice Call Authentication** page displays.



Do not select this option if this is a shared computer/device.

5. Click the **Call** button.

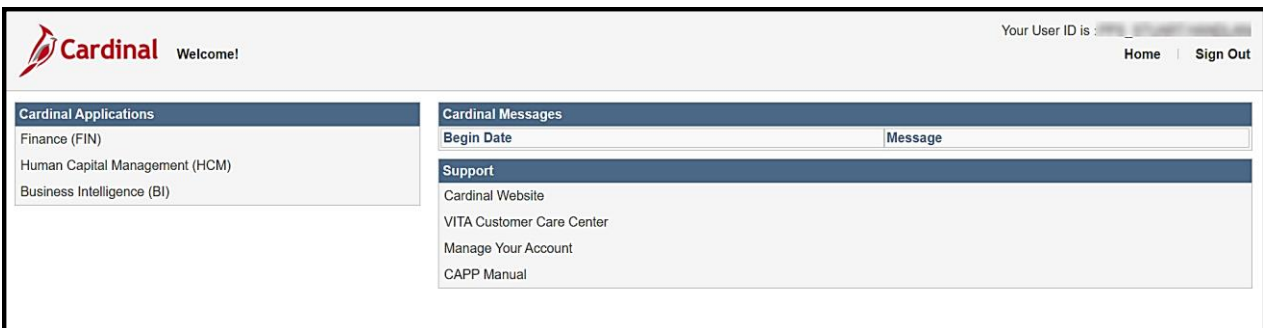
**Note:** The **Call** field changes to **Calling** when the call is in process and **Redial** after the call has disconnected.

6. Enter the authentication code received in the **Enter Code** field.
7. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

**Note:** If you clear the browser cache on your computer/device, you will need to enter the authentication code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the authentication code, to have settings added back to the computer/device.

8. Click the **Verify** button.

The **Cardinal Portal** displays.

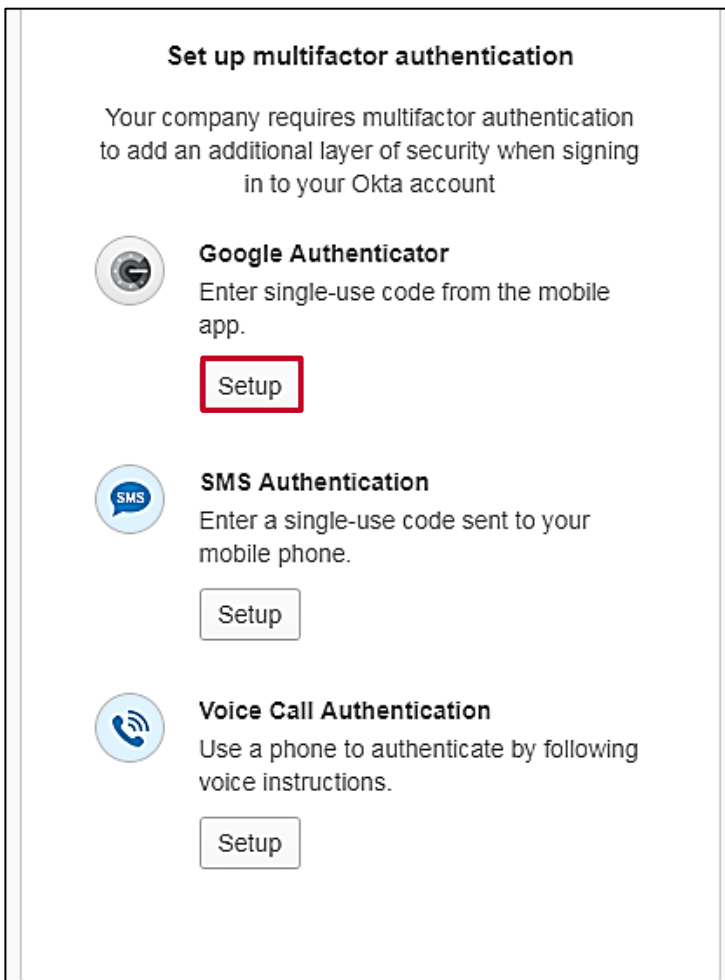


### Appendix

#### Setting Up Google Authenticator

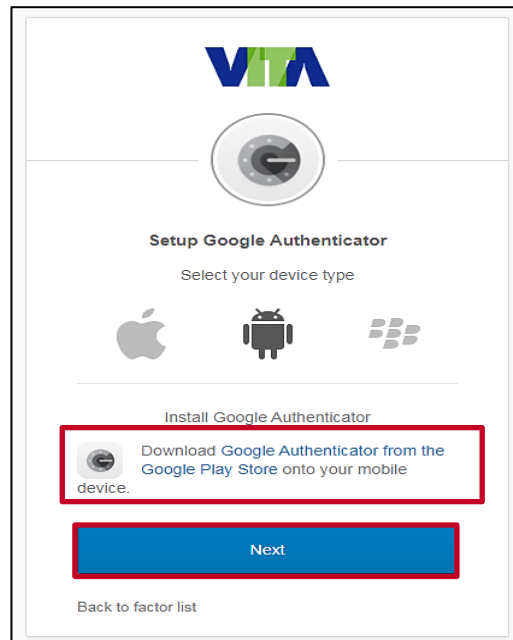
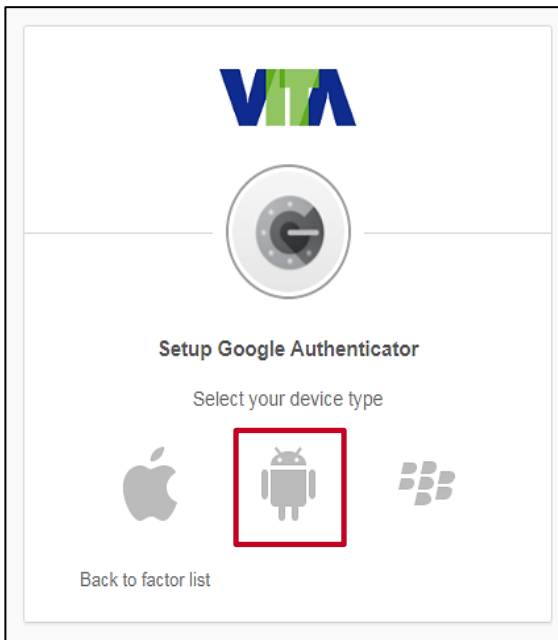
Since the Cardinal Team is not enabled to support the Google Authenticator app, we do not recommend this option.

Google Authenticator requires you to download the **Google Authenticator** app to your mobile device. The app generates a random token code which changes every 30 seconds. Standard data usage rates apply.





1. Click the Setup button within the **Google Authenticator** section.

The **Setup Google Authenticator** page displays.



2. Click the image for the type of mobile device you want to set up:

- a.  : Apple
- b.  : Android
- c.  : BlackBerry

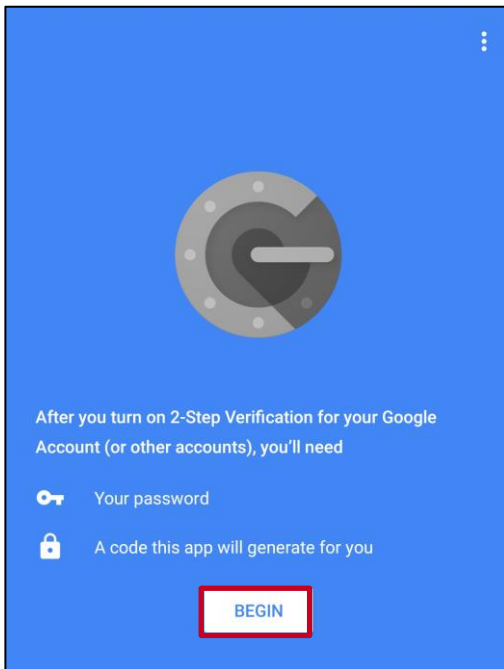
**Note:** If you do not have one of these mobile devices, click the **Back to factor list** link to return and choose another method for authentication.

3. After you select your device type, a Download message displays. Search for the **Google Authenticator** app (it is free) on your mobile device:

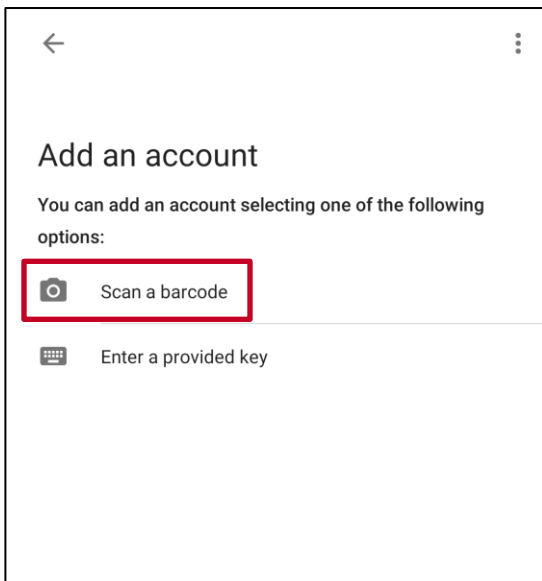
- a. Apple: go to the App Store
- b. Android: go to the Playstore
- c. BlackBerry: go to the World Store

4. Once you locate the app on your mobile device, install and open the app on your mobile device.

**Note:** Screens may vary based on mobile device type. These screenshots are based on Android.

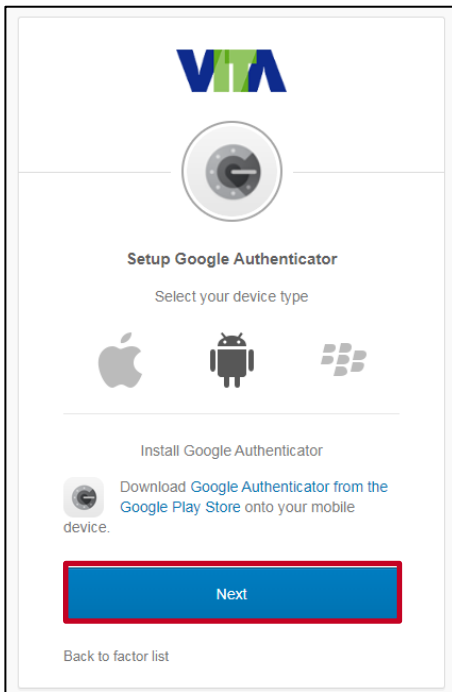


5. The **Google Authenticator** app displays on your mobile device. Click the **BEGIN** button. The **Add an account** page displays.



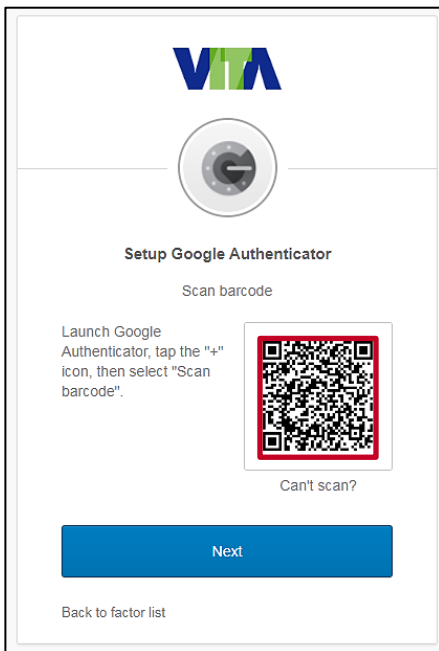
6. Select the **Scan barcode** option. This opens the camera on your mobile device.





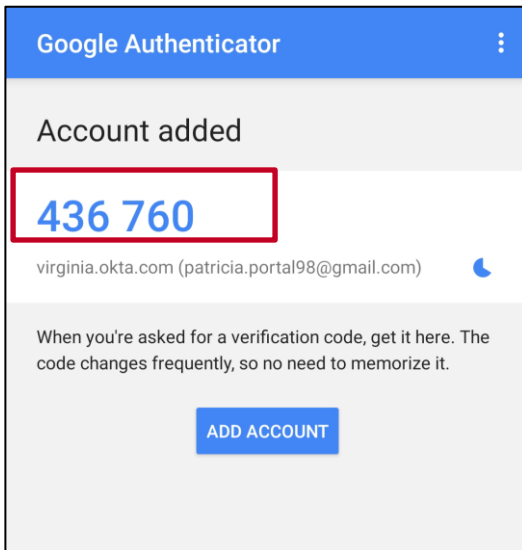
7. On your computer/device screen, click the **Next** button.

The **Setup Google Authenticator** page redisplay with a bar scan.



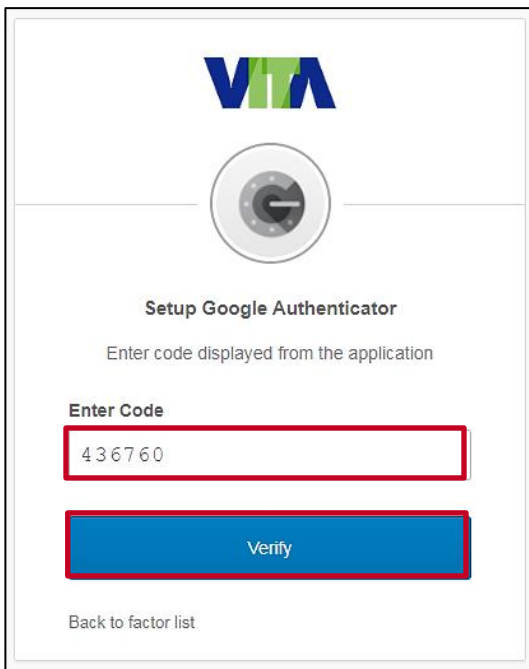
8. Point the camera of your mobile device at the barcode.

**Note:** If the barcode does not scan, follow the instructions in the **Bar Code – Can't Scan** section of this Job Aid.



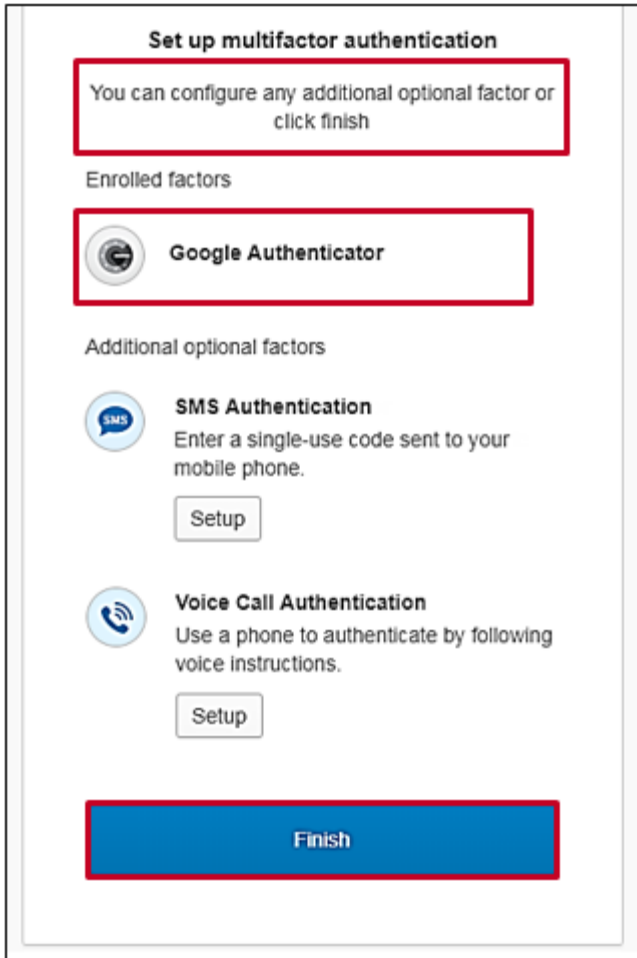
9. The **Google Authenticator** app on your mobile device recognizes the user account and displays a random token code.

**Note:** The token code will change every 30 seconds.



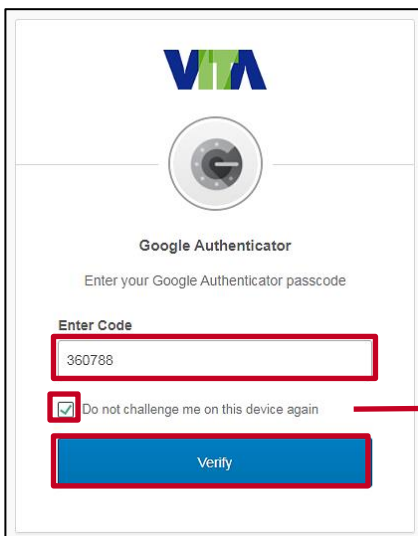
10. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
11. Click the **Verify** button.

The **Set up multifactor authentication** page displays.



12. A message indicates that you can configure any additional optional factor or click finish. The authentication option you selected displays under the **Enrolled factors** section of the page.  
**Note:** If you are using Chrome, you will see a green checkmark next to your enrolled factors.
13. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the **Cardinal Portal**.

The **Google Authenticator** page redisplay.



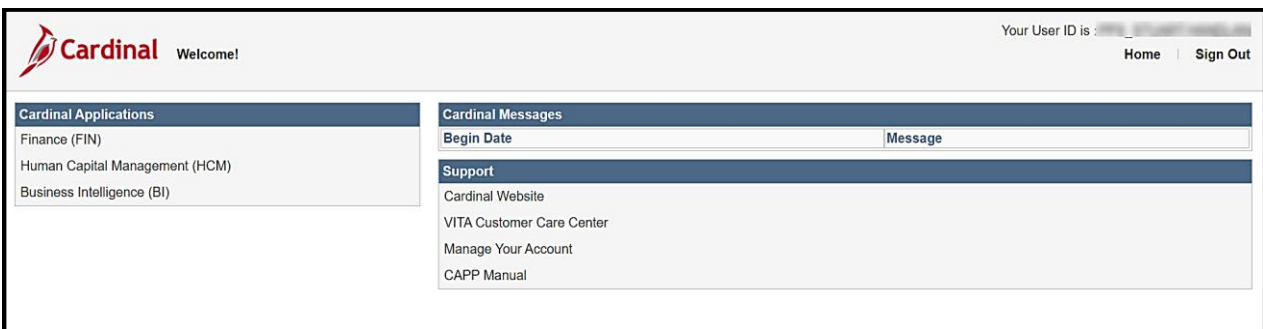
Do not select this option if this is a shared computer/device.

14. Open the **Google Authenticator** app on your mobile device.
15. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
16. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

**Note:** If you clear the browser cache on your computer/device, you will need to enter the token code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the token code, to have settings added back to the computer/device.

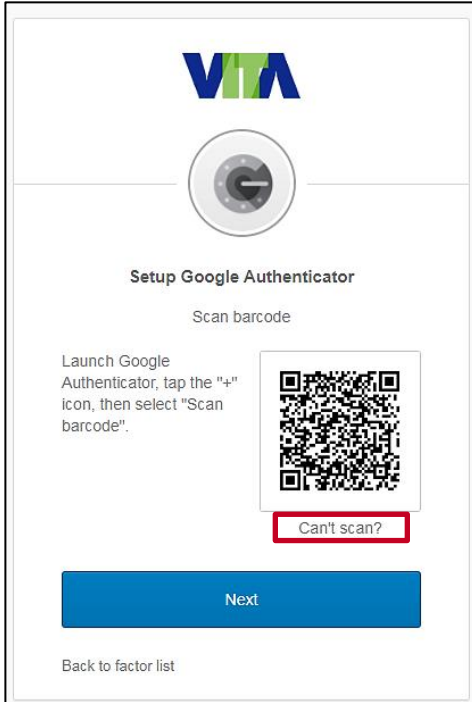
17. Click the **Verify** button.

The **Cardinal Portal** displays.



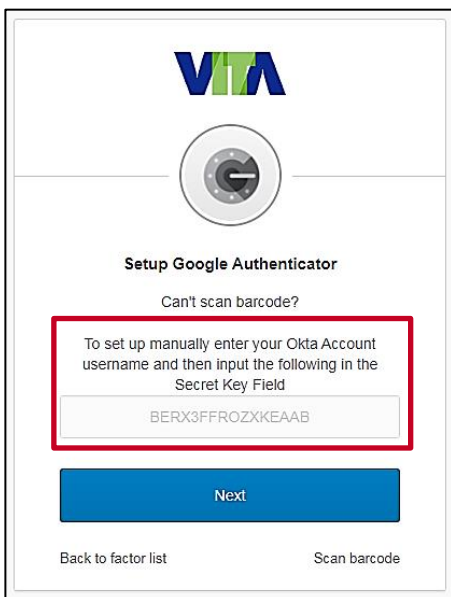
### Barcode – Can't scan

If your mobile device is unable to scan the barcode, follow the steps below:

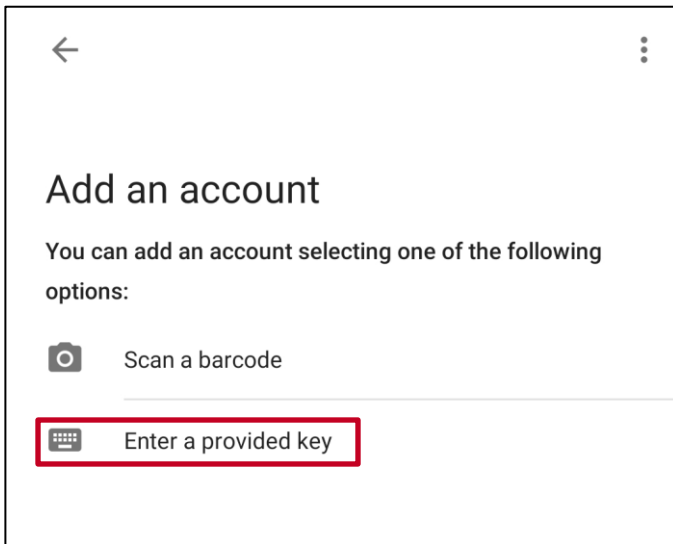


1. Click the **Can't scan?** link on your computer/device.

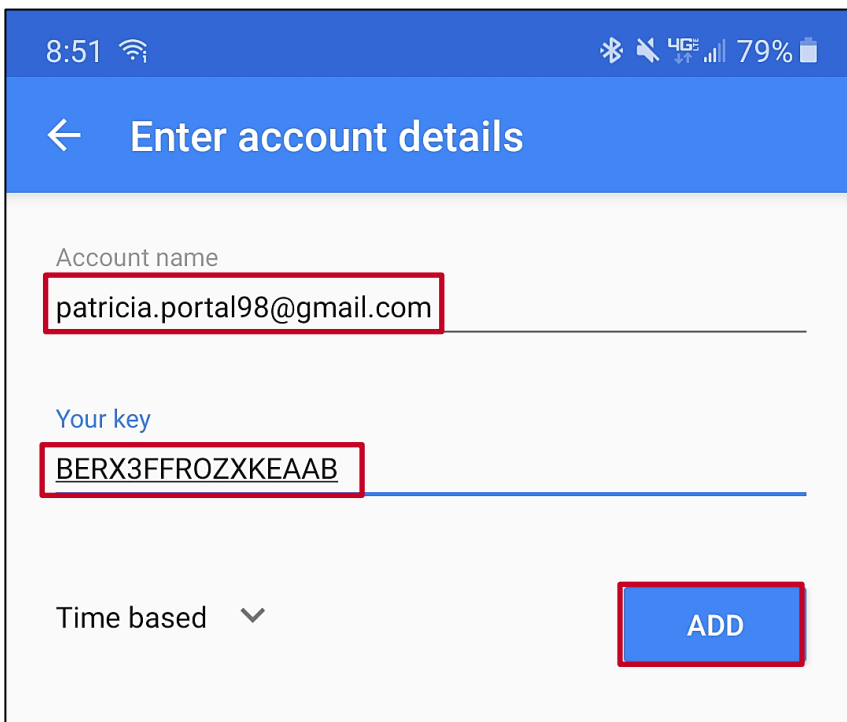
The **Setup Google Authenticator** page displays.



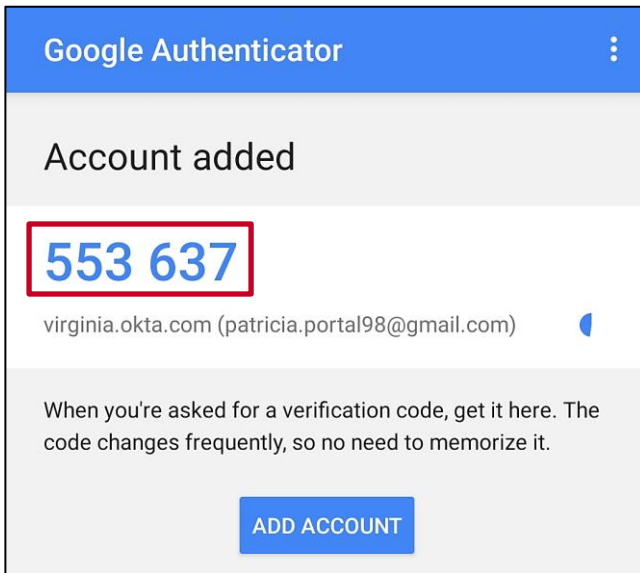
2. Follow the instructions on this page to enter the information on your mobile device.



3. On your mobile device, select the **Enter a provided key** option.

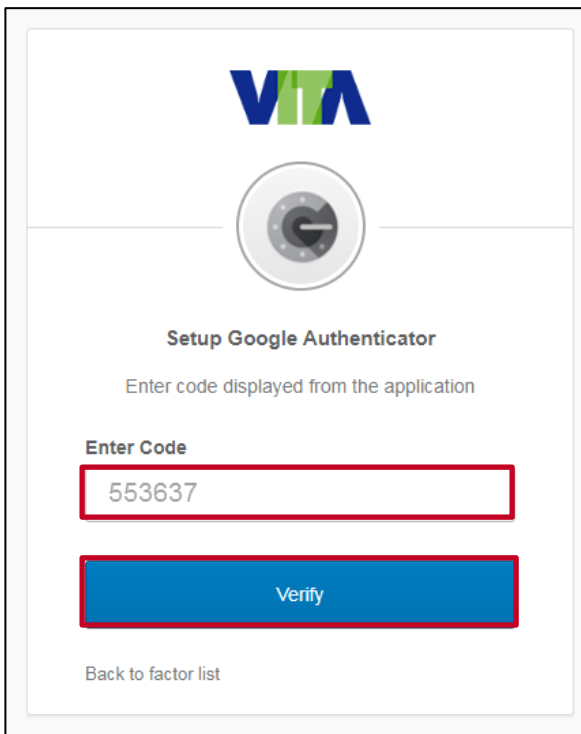


4. On your mobile device, the **Enter account details** page displays. Enter the following as noted below:
  - a. **Account name:** Enter your Cardinal Username
  - b. **Your key:** Enter the code that was provided on your **Google Authenticator** page on the computer/device.
5. Click the **ADD** button.



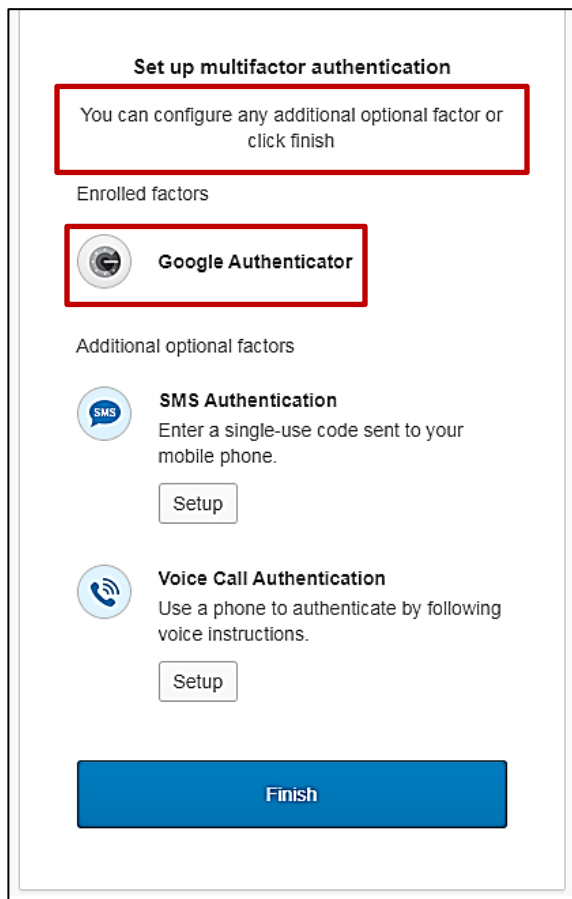
6. The **Google Authenticator** app on your mobile device opens the **Account added** page.
7. The token code displays.

**Note:** This code changes every 30 seconds.



8. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
9. Click the **Verify** button.

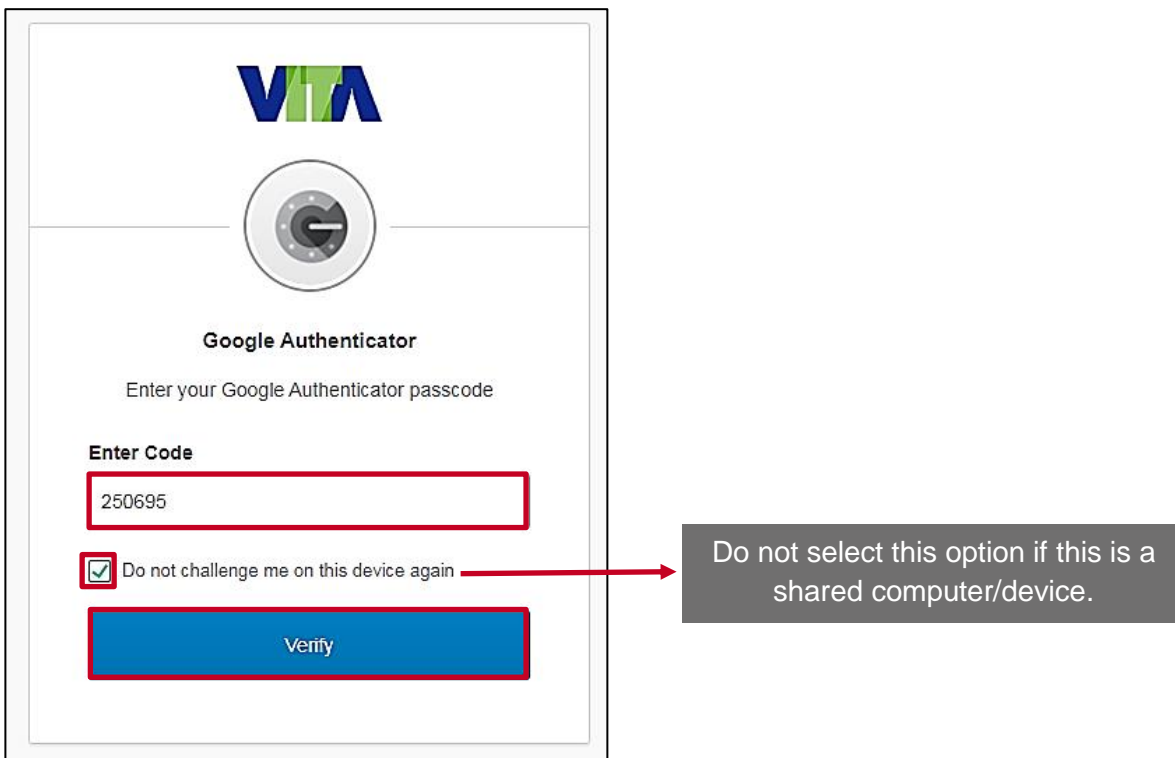
The **Set up multifactor authentication** page displays.



10. A message indicates that you can configure any additional optional factor or click finish. The authentication method you selected displays under the **Enrolled factors** section of the page.  
**Note:** If you are using Chrome, you will see a green checkmark next to your enrolled factors.
11. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the **Cardinal Portal**.



The **Google Authenticator** page redisplay.



VITA

Google Authenticator

Enter your Google Authenticator passcode

Enter Code

250695

Do not challenge me on this device again

Verify

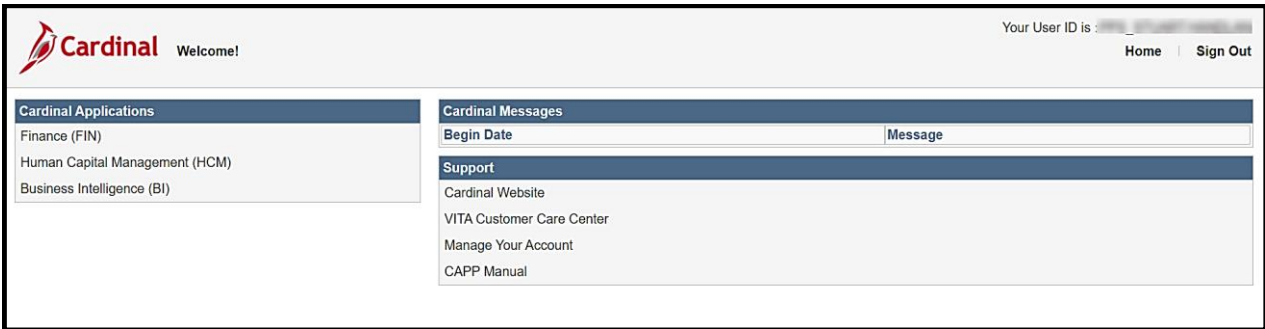
Do not select this option if this is a shared computer/device.

12. Open the **Google Authenticator** app on your mobile device.
13. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
14. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

**Note:** If you clear the browser cache on your computer/device, you will need to enter the token code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the token code, to have settings added back to the computer/device.

15. Click the **Verify** button.

The **Cardinal Portal** displays.



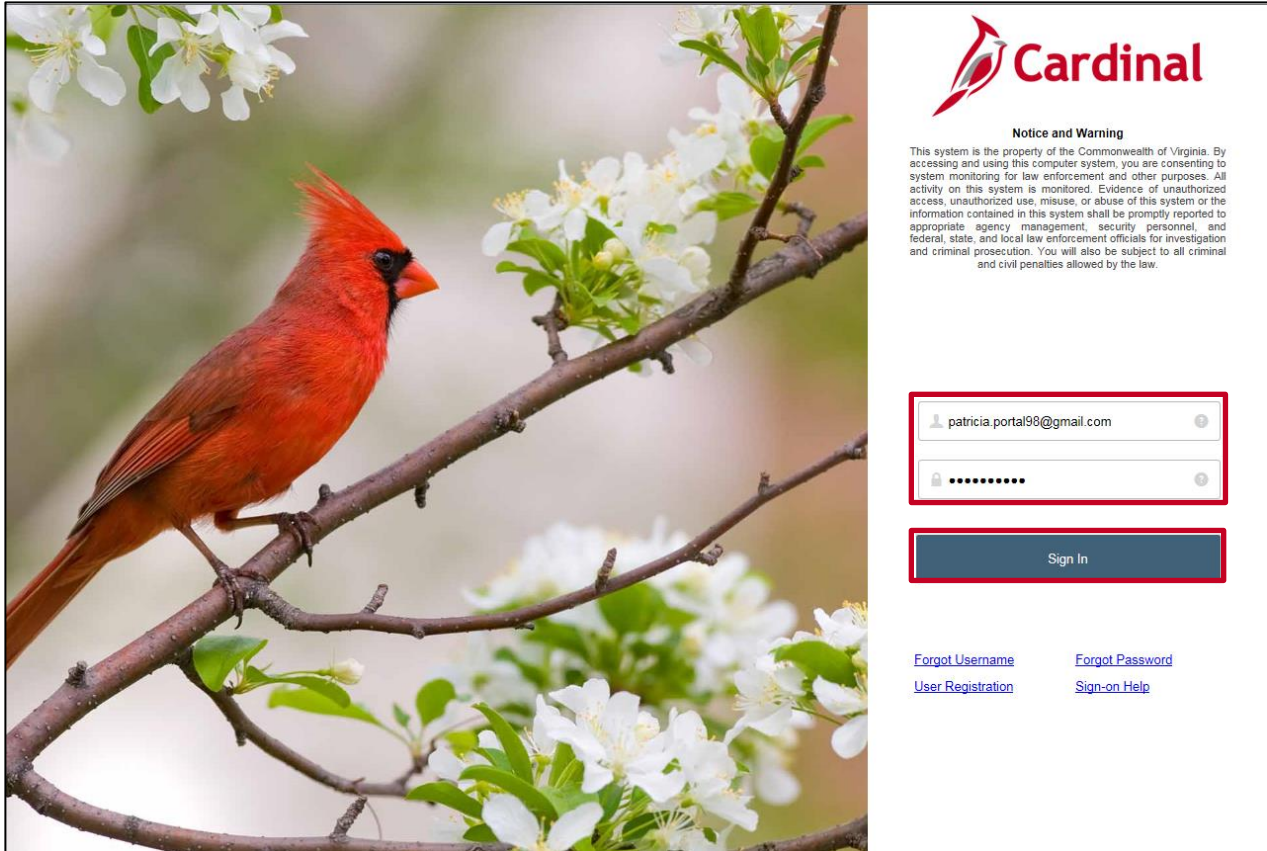
The screenshot shows the Cardinal Portal dashboard. At the top left is the Cardinal logo and the text "Welcome!". At the top right, it says "Your User ID is:" followed by a blurred user ID, and links for "Home" and "Sign Out". The dashboard is divided into two main columns. The left column is titled "Cardinal Applications" and lists "Finance (FIN)", "Human Capital Management (HCM)", and "Business Intelligence (BI)". The right column is titled "Cardinal Messages" and contains a table with two columns: "Begin Date" and "Message". Below the messages section is a "Support" section with links for "Cardinal Website", "VITA Customer Care Center", "Manage Your Account", and "CAPP Manual".

### Logging in After Setting up Google Authenticator

The next time you use the same computer/device to log in to the **Cardinal Portal**, the authentication option you selected is retained.

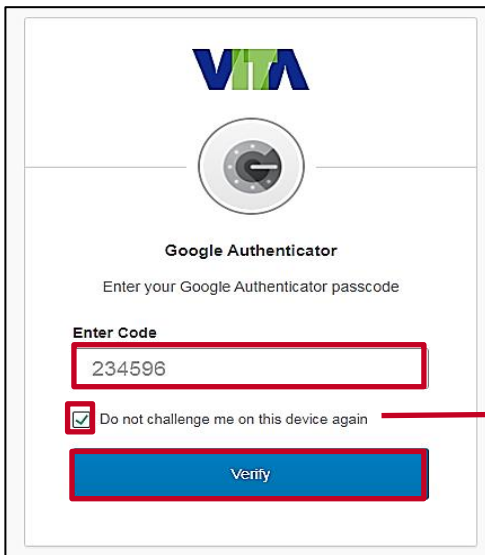
1. Start by entering the following URL in your computer browser: [my.cardinal.virginia.gov](https://my.cardinal.virginia.gov).

The **Cardinal Login** page displays.



2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
  - a. COV users: enter your network password.
  - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.

The **Google Authenticator** page displays.



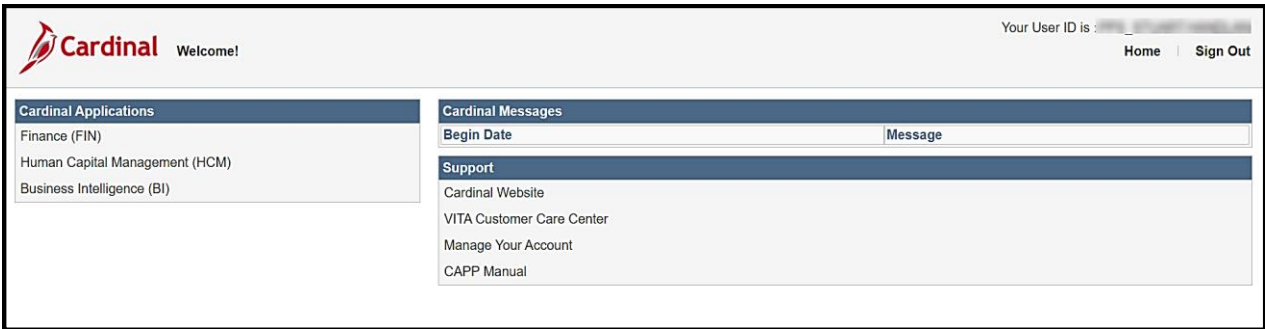
Do not select this option if this is a shared computer/device.

5. Open the **Google Authenticator** app on your mobile device.
6. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
7. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

**Note:** If you clear the browser cache on your computer/device, you will need to enter the token code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the token code, to have settings added back to the computer/device.

8. Click the **Verify** button.

The **Cardinal Portal** displays.



The screenshot shows the Cardinal Portal interface. At the top left is the Cardinal logo and the text "Welcome!". At the top right, it says "Your User ID is:" followed by a blurred area, and "Home | Sign Out" links. The main content area is divided into two columns. The left column is titled "Cardinal Applications" and lists "Finance (FIN)", "Human Capital Management (HCM)", and "Business Intelligence (BI)". The right column is titled "Cardinal Messages" and contains a table with two columns: "Begin Date" and "Message". Below the messages section is a "Support" section with links for "Cardinal Website", "VITA Customer Care Center", "Manage Your Account", and "CAPP Manual".