



Registering Your Account – All Other Users

- Users using a personal email address (COV or Non-COV)
- Users using an agency provided email address (Non-COV)
- Users from a locality using locality provided or personal email. Use the Active state employee option demonstrated below.
- Terminated or retired employees

Note: The **Active state employee** and **Terminated/Retired state employee** options work exactly the same. The Active state employee option is demonstrated below.



 **Cardinal**

User Registration



What type of Cardinal application user are you?

☒ Active state employee
☐ Contractor working for a state agency
☐ Terminated/Retired state employee

[Back](#) [Next](#)

[Return to Login](#) [Sign-On Help](#)



1. The **Active state employee** option is selected. Click the **Next** button.




- The **Cardinal User Registration** page displays with validation criteria. Enter your Cardinal Employee ID including the leading zeros in the ***Enter 11 digit Employee ID** field.


Note: Your **Cardinal Employee ID** is made up of your 7-digit **BES**/9-digit **PMIS ID**. Both state and locality employees/retirees/terminated employees should use their Cardinal Employee ID (e.g., 00 prefix + 7-digit BES ID number + 00 suffix **OR** 9-digit PMIS ID + 00 suffix).

Note: If you do not know your Cardinal Employee ID, please work with your HR or Benefits staff to assist.

- Enter the last 4 digits of your social security number in the ***Enter last 4 digits of your SSN** field.
- Complete the **Cardinal re-captcha** field. Enter the code exactly as it appears. This field is case sensitive.
 - Refresh**  : click the refresh icon to have a new Cardinal re-captcha code display.
 - Speaker**  : click the speaker icon to receive an audible Cardinal re-captcha code.

- Click the **Next** button.



 **Cardinal**
User Registration
Please confirm the agency for which you are trying to register in Cardinal. If you do not find the agency listed below, notify Cardinal Security Team by sending an email to vccc@vita.virginia.gov
☒ LDUTY - Line of Duty Act Participants


[Return to Login](#) [Forgot Username](#)


6. The **Cardinal User Registration** page displays the agency/locality for which you are eligible to register an account. Confirm the information displayed is correct by selecting the radio button. The **Next** button becomes enabled.

Note: If the correct information does not display, **do not proceed**. Submit a Helpdesk ticket via email to VCCC@vita.virginia.gov and include “**Cardinal**” in the subject line of the email.

You will receive an email from the IT Service Desk <vccc@vita.virginia.gov> with an Incident number and a link to VITA's ticket system. Unfortunately, you will **not** be able to access the ticket system to track your issue. However, to assist with tracking, you will receive an update via every time a comment is added to your inquiry. The Cardinal Team also will contact you directly, using the contact information you provided, so that you can correspond about your incident. A new ticket is required for any new issues. Due to high ticket counts, response time may vary.

7. Click the **Next** button.



 **Cardinal**
User Registration

To Register, verify user details and confirm email address. If any user information is inaccurate, contact your agency HR.

First Name	<input type="text"/>
Last Name	<input type="text"/>
Agency	LDUTY - Line of Duty Act Participants
Email Address	<input type="text" value="3@hotmail.com"/>


* Confirm email address


[Back](#) [Register](#)

[Return to Login](#) [Forgot Username](#)

8. The **Cardinal User Registration** page displays. Verify the information displayed is correct and enter your email address in the ***Confirm email address** field.

Note: If any of the information displayed is not correct, do not proceed and contact your Human Resources Administrator.



 **Cardinal**

User Registration

To Register, verify user details and confirm email address. If any user information is inaccurate, contact your agency HR.

First Name

Last Name

Agency

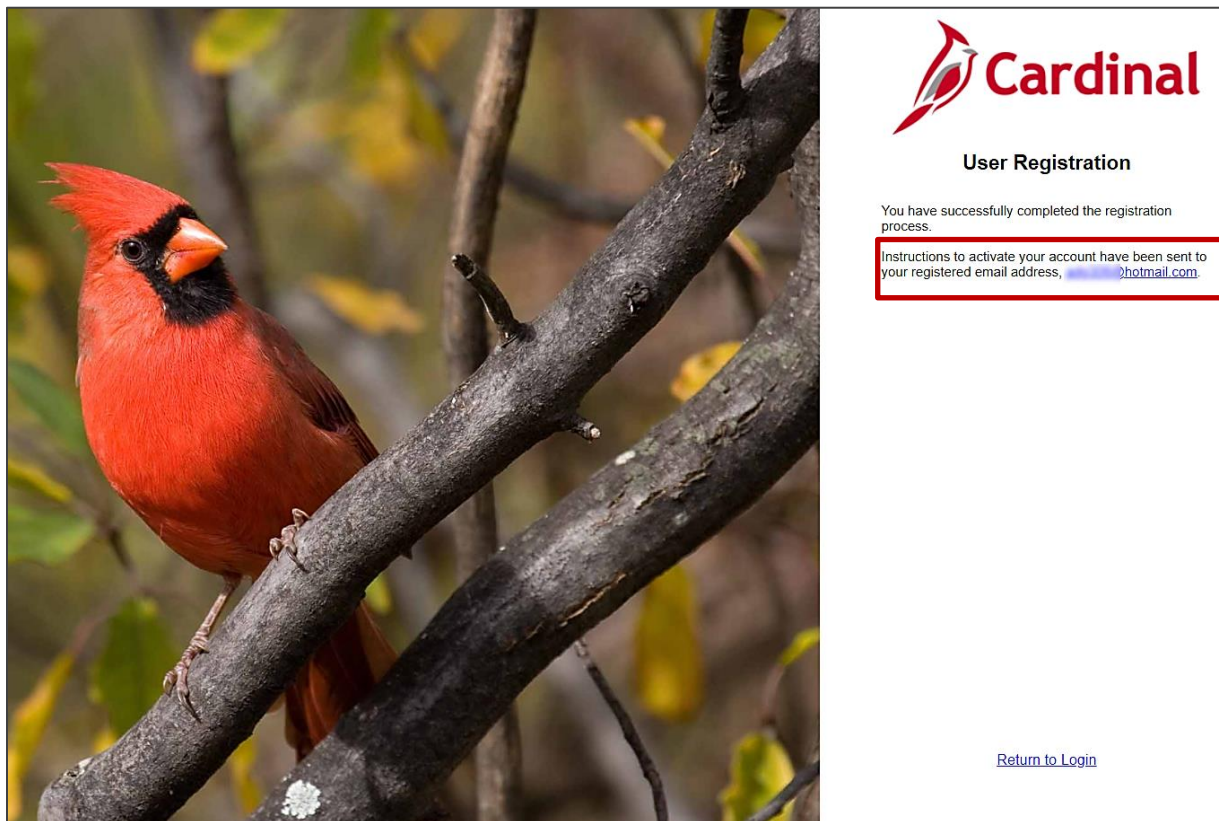
Email Address

* Confirm email address

[Back](#) [Register](#)

[Return to Login](#) [Forgot Username](#)

9. Click the **Register** button.



10. The **Cardinal User Registration** page displays a message stating you have successfully completed the registration process. Instructions to activate the account are sent to your registered email address which is displayed on the page.

11. Open your email account.



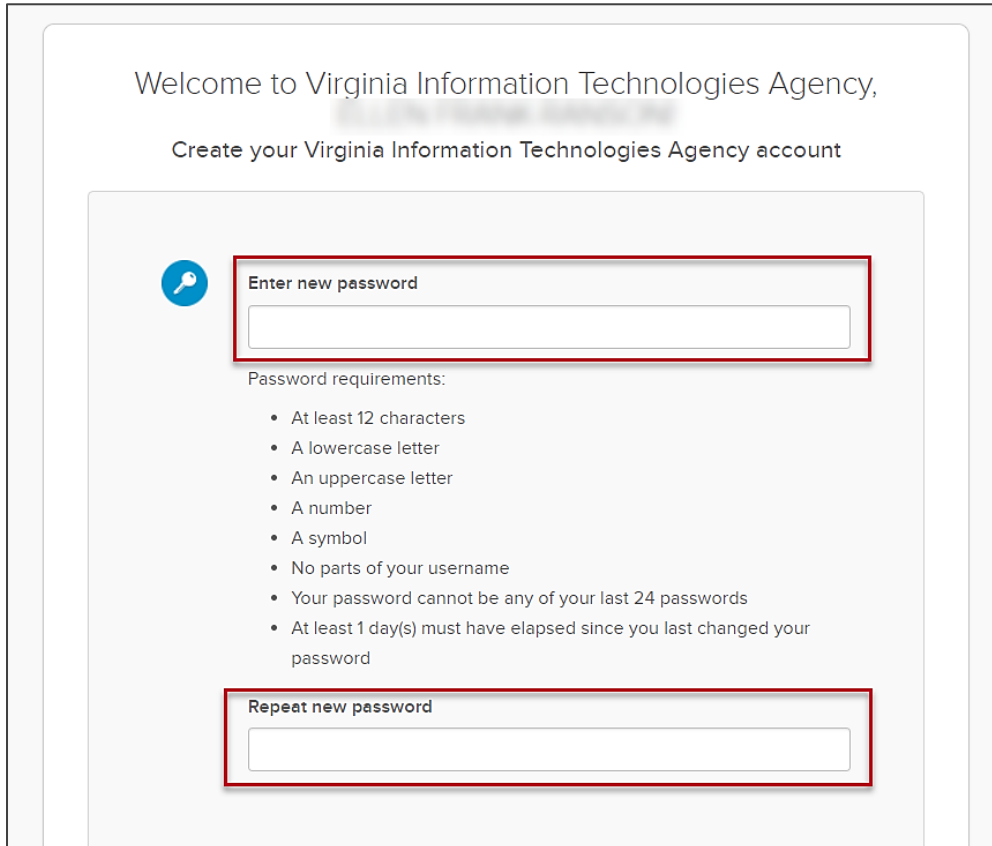
12. Check your email for a message from noreply.cardinal@doa.virginia.gov with the subject **"Welcome to Cardinal!"**. Open the email, then:

- Make note of your Cardinal Username, as this will be used each time you log into Cardinal.
- Click the link in your email message to activate your account.

Note: If you do not use the link to activate your account within seven (7) days, you will need to submit a help desk ticket to vccc@vita.virginia.gov and include **"Cardinal"** in the subject line. Indicate the activation link timeframe expired and you need to activate your account. If you do not receive an email, please check your Spam folder.


Activating Your Account

Activating your account is a one-time only process. During this process, you will set up your password, select a forgot password question, and choose a security image.



Welcome to Virginia Information Technologies Agency,

Create your Virginia Information Technologies Agency account

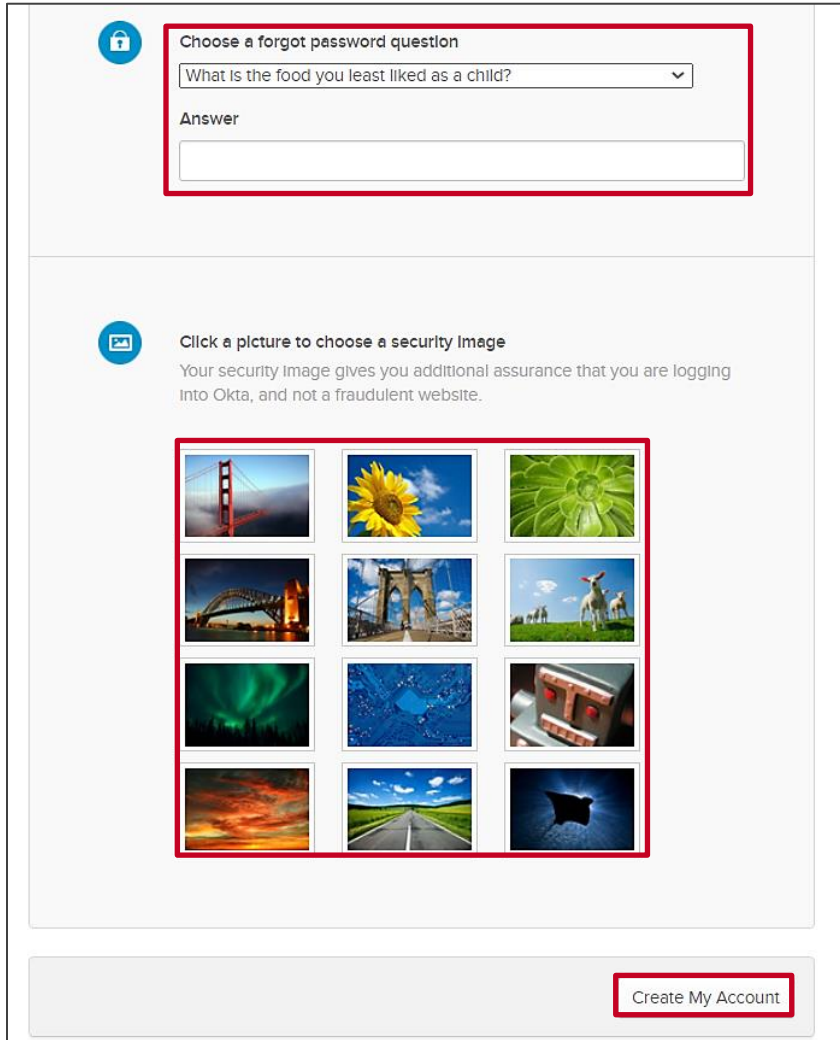
 Enter new password

Password requirements:

- At least 12 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Your password cannot be any of your last 24 passwords
- At least 1 day(s) must have elapsed since you last changed your password

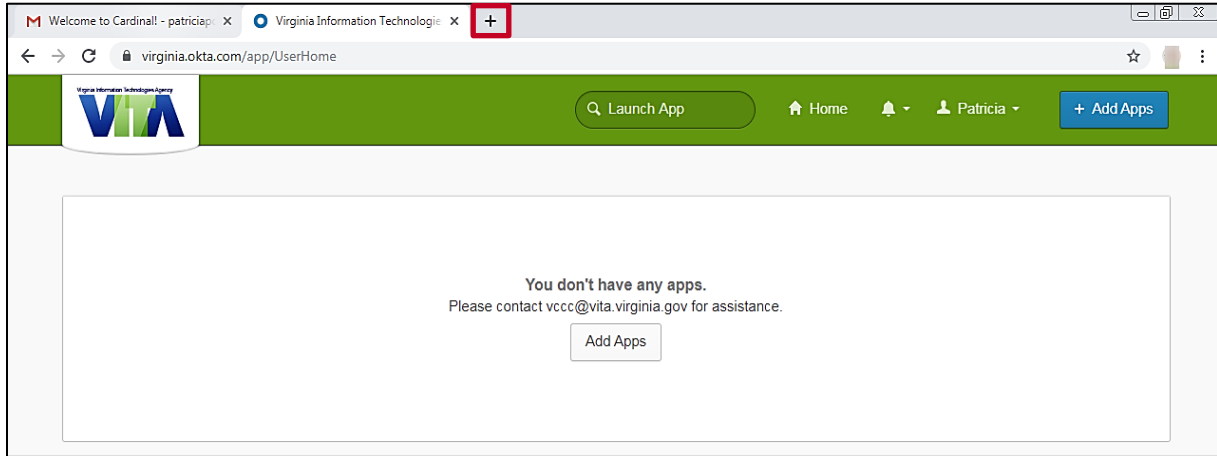
Repeat new password

1. The **VITA Create your Virginia Information Technologies Agency account** page displays. There are two (2) sections that need to be completed. They are:
 - a. **Enter new password**
 - b. **Choose a forgot password question**
2. Enter a password for your account in the **Enter new password** field. Follow the password requirements as listed on the page.
3. Enter the password again in the **Repeat new password** field.

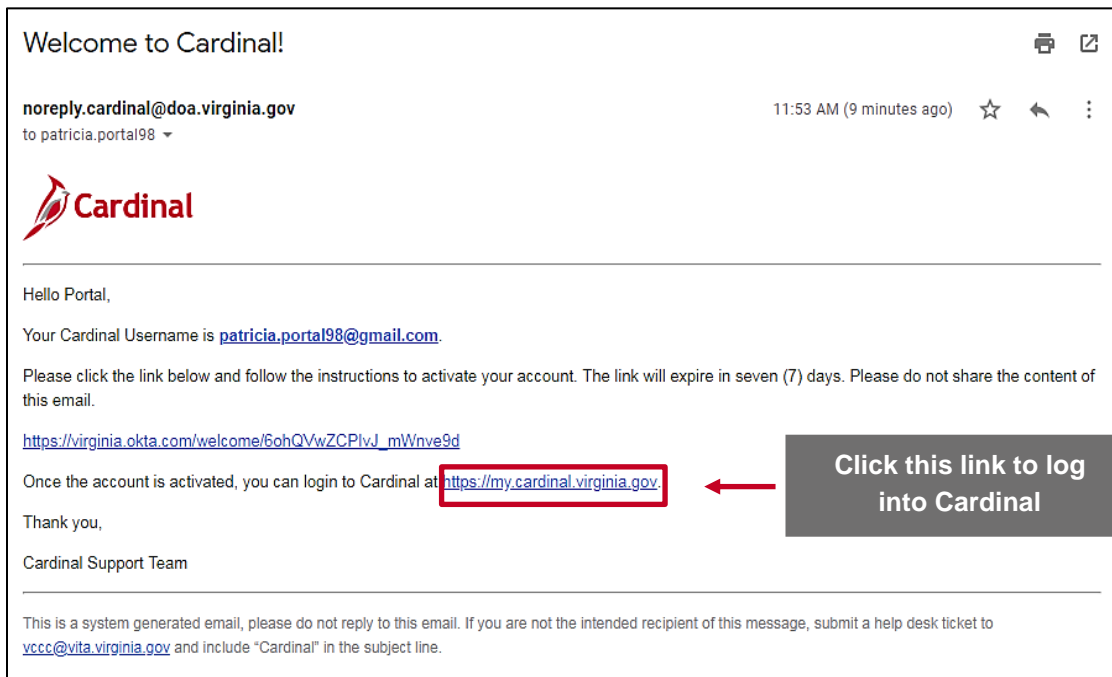


The screenshot displays a web form for creating an account. It is divided into two main sections. The first section, titled 'Choose a forgot password question', contains a dropdown menu with the selected option 'What is the food you least liked as a child?' and an empty text field labeled 'Answer'. The second section, titled 'Click a picture to choose a security Image', includes a descriptive text: 'Your security Image gives you additional assurance that you are logging into Okta, and not a fraudulent website.' Below this text is a 4x3 grid of 12 different images. At the bottom right of the form is a button labeled 'Create My Account'.

4. Under the **Choose a forgot password question** section, select a question from the drop-down list. This question will be used if you need to reset your password.
5. In the **Answer** field, enter the answer to the question you selected. This field is not case sensitive.
6. Under the **Click a picture to choose a security image** section, select a security image.
7. Click the **Create My Account** button.



8. The **VITA** page displays. No action is required on this page.
9. Click the **X** to close the web browser tab.



10. Now that your account has been activated, click the link from the **Welcome to Cardinal!** registration email or type the following URL in your web browser to access the **Cardinal Login** page (my.cardinal.virginia.gov).

Note: Bookmark my.cardinal.virginia.gov in your web browser.



Security and Access Job Aid

SW SEC: Cardinal System Access Guide

Cardinal

Notice and Warning

This system is the property of the Commonwealth of Virginia. By accessing and using this computer system, you are consenting to system monitoring for law enforcement and other purposes. All activity on this system is monitored. Evidence of unauthorized access, unauthorized use, misuse, or abuse of this system or the information contained in this system shall be promptly reported to appropriate agency management, security personnel, and federal, state, and local law enforcement officials for investigation and criminal prosecution. You will also be subject to all criminal and civil penalties allowed by the law.

patricia.portal98@gmail.com

Sign In

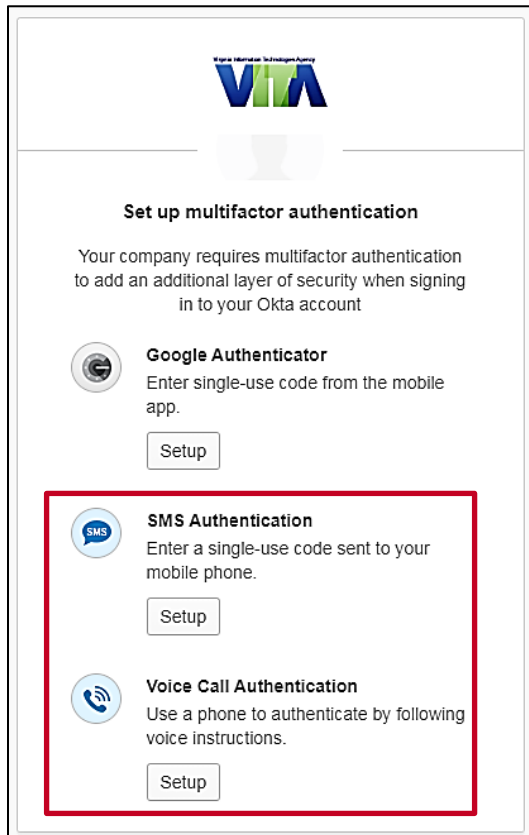
[Forgot Username](#) [Forgot Password](#)
[User Registration](#) [Sign-on Help](#)

11. The **Cardinal Login** page displays. In the **Cardinal Username** field, enter your Cardinal Username from the **Welcome to Cardinal!** email you received.
12. In the **Password** field, enter the password you created during the registration process.
13. Click the **Sign In** button.

Note: You will be required to setup multi-factor authentication (MFA) immediately after signing in the first time. This is a one-time only process. Follow the steps to set up MFA in the **Setting Up Multi-Factor Authentication** section.

Setting Up Multi-Factor Authentication (MFA)

Setting up MFA allows you to access the Cardinal Portal from outside the Commonwealth of Virginia (COV) network.



1. The VITA **Set up multifactor authentication** page displays. Cardinal recommends using one of the two options listed below.

SMS Authentication

- Requires a mobile phone registered in the United States or Canada.
- A text message is sent to your mobile phone, with an authentication code that you will need to enter on your computer/device.
- Standard text messaging rates apply.

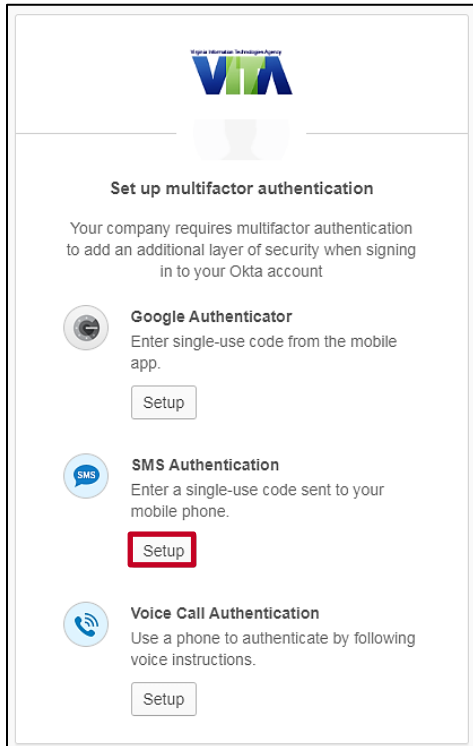
Voice Call Authentication

- Requires either a mobile phone or access to a land line phone.
- A phone call is placed to the phone number you enter. Once you answer the call, a code is verbally stated twice.
- Enter the code into your computer/device.

Google Authenticator is not recommended by Cardinal.

Setting up SMS Authentication

You will receive a random single-use code on your mobile phone (standard text messaging rates apply).



Set up multifactor authentication

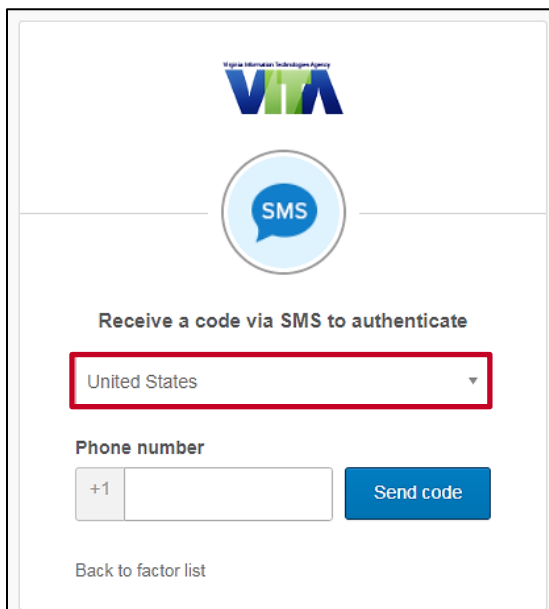
Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

Google Authenticator
Enter single-use code from the mobile app.

SMS Authentication
Enter a single-use code sent to your mobile phone.

Voice Call Authentication
Use a phone to authenticate by following voice instructions.

2. Click the **Setup** button under the **SMS Authentication** section of the page.

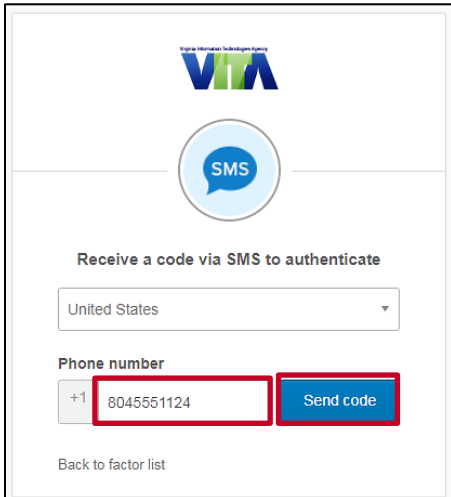


Receive a code via SMS to authenticate

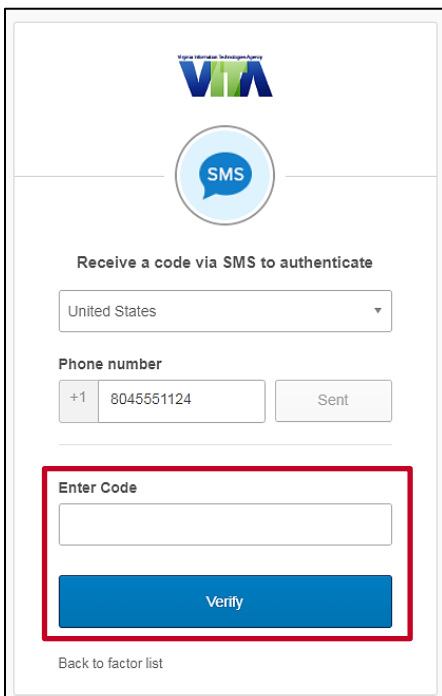
Phone number

[Back to factor list](#)

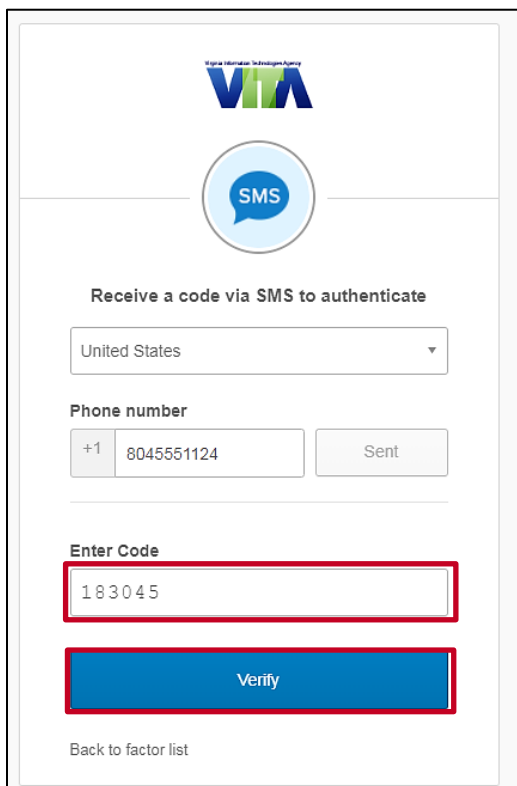
- The **SMS** page displays. Select **United States** or **Canada**, based on where your mobile phone is registered.



- Click in the **Phone number** field and enter your mobile phone number including area code.
- Click the **Send code** button.

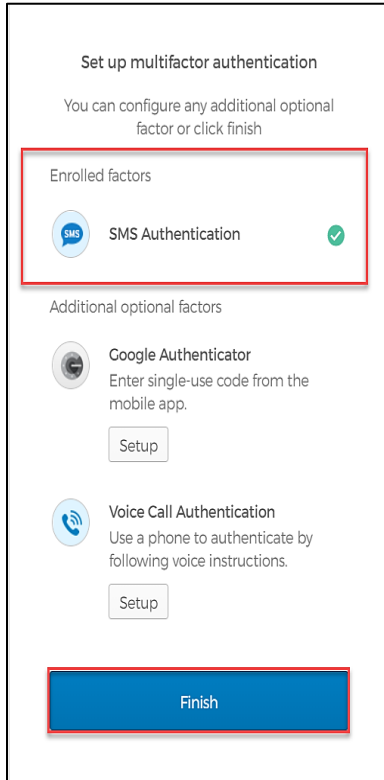


- An **Enter Code** field and **Verify** button display at the bottom of the page.
- A text message displays on your mobile phone with the authentication code.



The screenshot shows the VITA (Virtual Information Technology Assistant) interface for SMS authentication. At the top is the VITA logo and a blue circular icon with 'SMS' inside. 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 8045551124' and a 'Sent' button. The 'Enter Code' section has a text input field containing '183045', which is highlighted with a red border. Below the input field is a blue 'Verify' button, also highlighted with a red border. At the bottom, there is a link that says 'Back to factor list'.

8. Enter the authentication code in the **Enter Code** field on your computer/device.
9. Click the **Verify** button.



Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

- SMS Authentication ✓

Additional optional factors

- Google Authenticator
Enter single-use code from the mobile app.
Setup
- Voice Call Authentication
Use a phone to authenticate by following voice instructions.
Setup

Finish

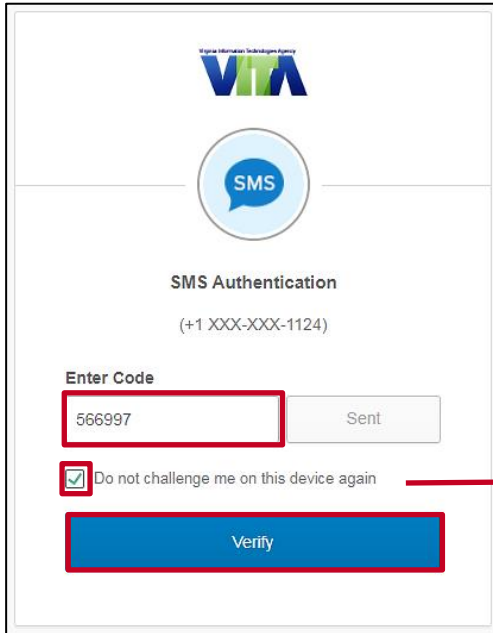
The **Set up multifactor authentication** page displays. A message indicates **You can configure any additional optional factor or click finish.**

- 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 factor.

- Click the **Finish** button.

Note: Now that you have completed your authentication setup, you will be required to authenticate in order to log into the **Cardinal Portal**.



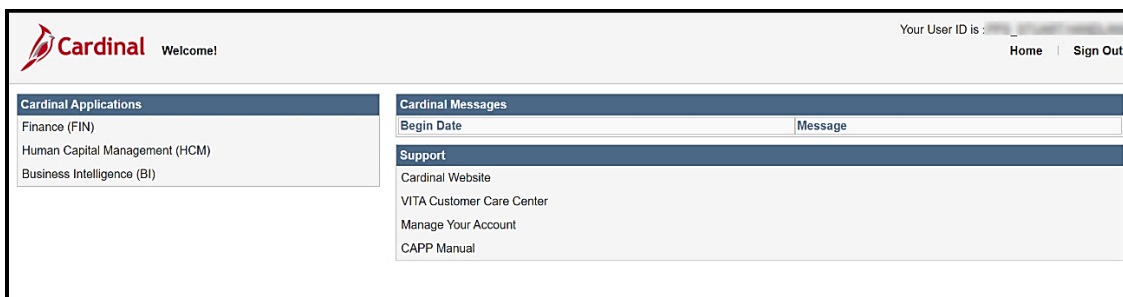
Do not select this option if this is a shared computer/device.

12. The **SMS Authentication** page displays. Click the **Send Code** button. The **Send Code** button changes to sent.
Note: After about 30 seconds, the **Sent** button changes to **Re-send Code**.
13. An authentication code is sent to your mobile device.
14. Enter the authentication code that displays on your mobile device in the **Enter Code** field on your computer/device.
15. To skip this step in the future, select the **Do not challenge me on this device again** check-box. Okta 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** check-box, after entering the authentication code, to have settings added back to the computer/device.
16. Click the **Verify** button to access the **Cardinal Portal**.



Security and Access Job Aid

SW SEC: Cardinal System Access Guide



17. The **Cardinal Portal** displays. Congratulations! You have completed the registration, activation, and authentication process for the Cardinal Portal.

See the [Cardinal Portal Layout](#) section for information about the Portal page.


Setting Up Voice Call Authentication

This additional authentication option allows you to use a mobile or land line to receive an authentication code.

1. 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.


Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account




Google Authenticator
Enter single-use code from the mobile app.

Setup



SMS Authentication
Enter a single-use code sent to your mobile phone.

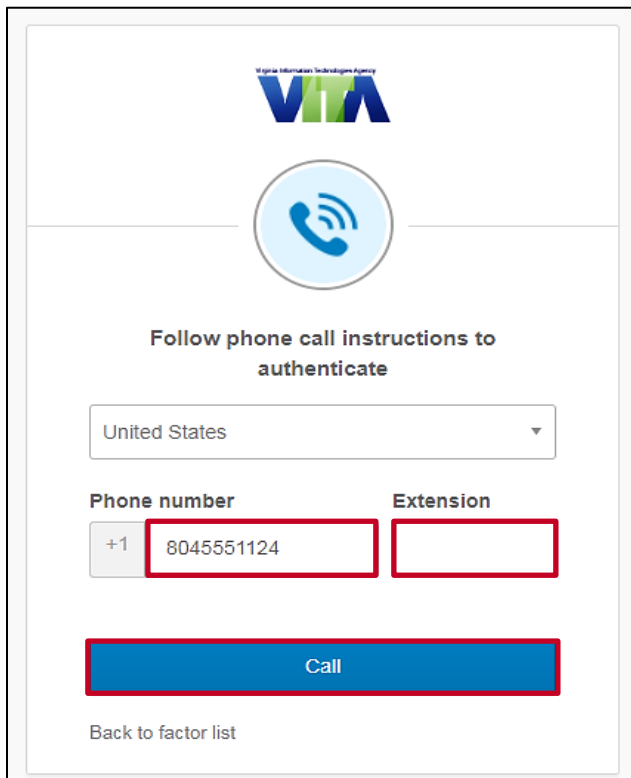
Setup





Voice Call Authentication
Use a phone to authenticate by following voice instructions.

Setup

2. Click the **Setup** button within the **Voice Call Authentication** section.



Follow phone call instructions to
authenticate

United States ▼

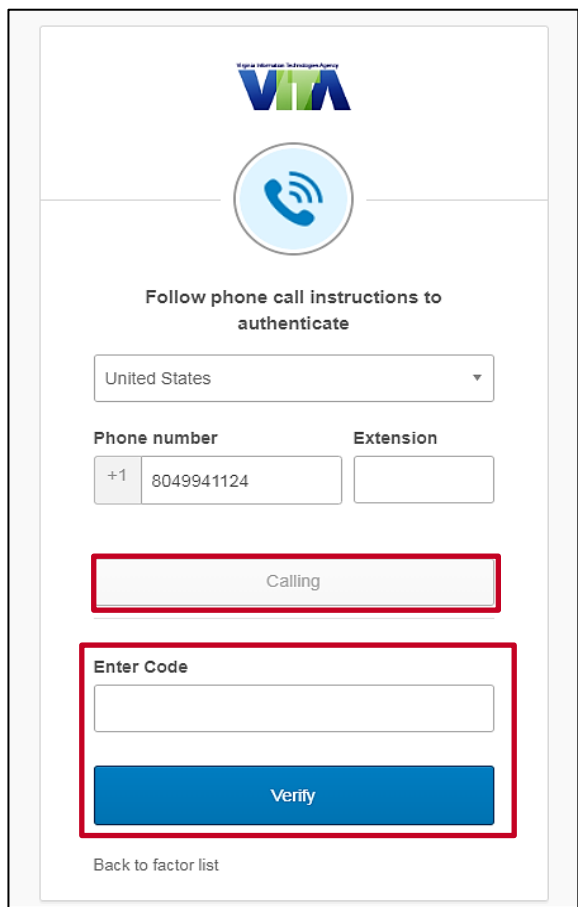
Phone number Extension

+1 8045551124

Call

[Back to factor list](#)

3. The **Follow phone call instructions to authenticate** page displays.
4. Enter the phone number you want to receive the call. The phone number can be either a land line or mobile, registered in the United States or Canada.
If the phone requires an extension, enter it in the **Extension** field.
5. Click the **Call** button.



Follow phone call instructions to authenticate

United States

Phone number Extension

+1 8049941124

Calling

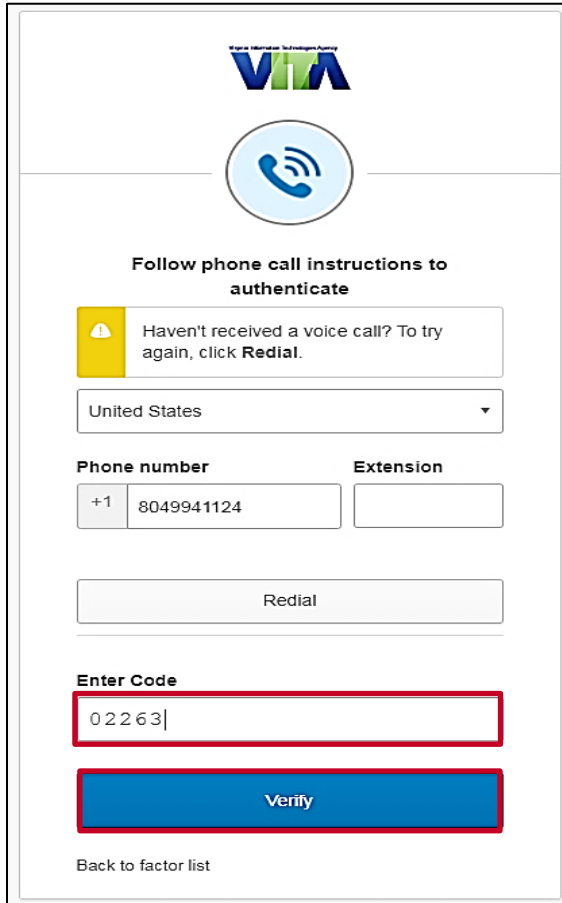
Enter Code

Verify

[Back to factor list](#)

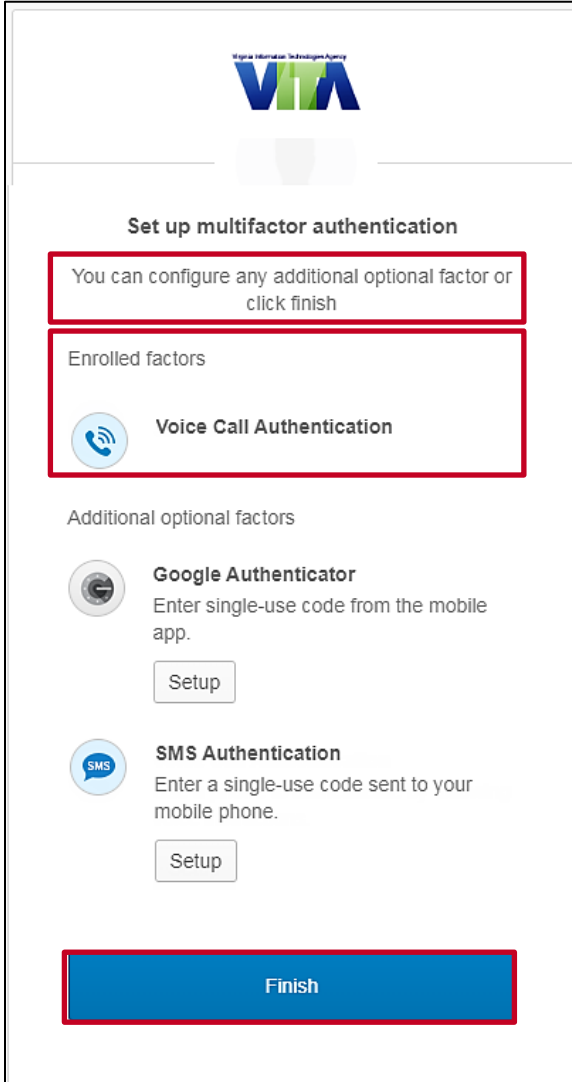
6. An **Enter Code** field and **Verify** button display on the page.

Note: The **Call** field changes to **Calling** when the call is in process. If you do not enter the code and click the **Verify** button, a few seconds after the call disconnects, the **Calling** option changes to **Redial**.



The screenshot shows a web-based interface for phone verification. At the top is the VITA logo and a phone icon. Below the icon, the text reads "Follow phone call instructions to authenticate". A yellow box with an exclamation mark icon contains the text: "Haven't received a voice call? To try again, click **Redial**." Below this is a dropdown menu showing "United States". Underneath are two input fields: "Phone number" with the value "+1 8049941124" and an empty "Extension" field. A "Redial" button is positioned below these fields. Further down is an "Enter Code" section with a text input field containing "02263" and a blue "Verify" button. At the bottom left is a link that says "Back to factor list".

7. 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.
8. Make note of the authentication code. Enter the authentication code in the **Enter Code** field on your computer/device.
9. Click the **Verify** button.



Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

Voice Call Authentication

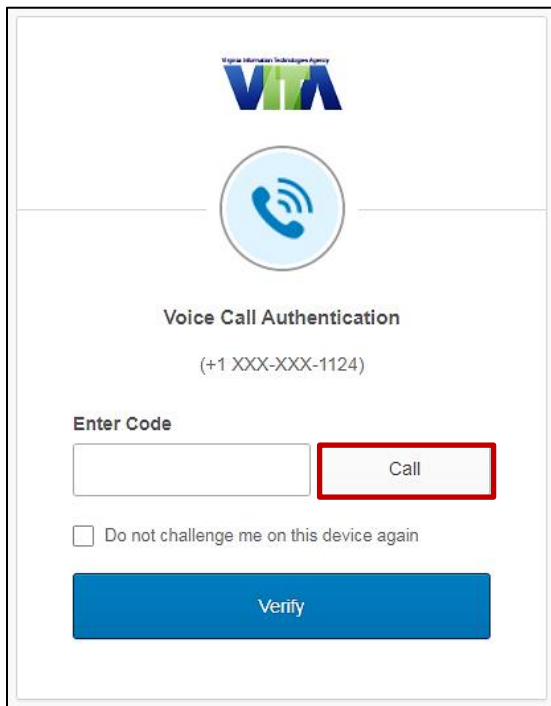
Additional optional factors

Google Authenticator
Enter single-use code from the mobile app.
Setup

SMS Authentication
Enter a single-use code sent to your mobile phone.
Setup

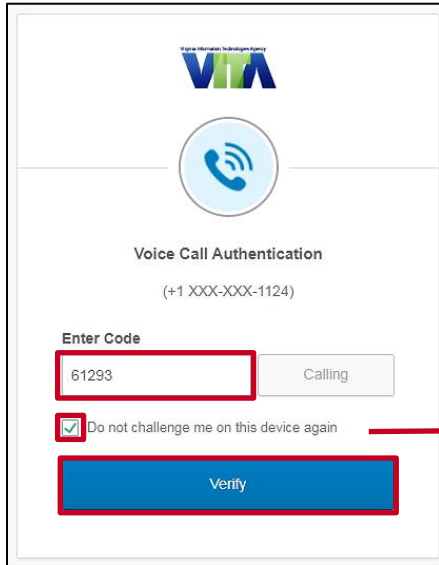
Finish

10. The **Set up multifactor authentication** page displays. A message indicates **You can configure additional optional options or click finish**.
11. 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.
12. 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 image shows a web-based interface for Voice Call Authentication. At the top, there is a logo for 'VITA' (Virginia Information Technologies Agency) and a circular icon containing a blue telephone handset with signal waves. Below the icon, the text 'Voice Call Authentication' is displayed, followed by the phone number '(+1 XXX-XXX-1124)'. There is a section labeled 'Enter Code' with a text input field and a 'Call' button highlighted with a red border. Below this is a checkbox labeled 'Do not challenge me on this device again'. At the bottom, there is a large blue button labeled 'Verify'.

13. The **Voice Call Authentication** page displays on your computer/device.
14. Click the **Call** button to receive a new authentication code.



VITA
Voice Information Technologies Agency

Voice Call Authentication
(+1 XXX-XXX-1124)

Enter Code
61293

Calling

☒ Do not challenge me on this device again

Verify

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

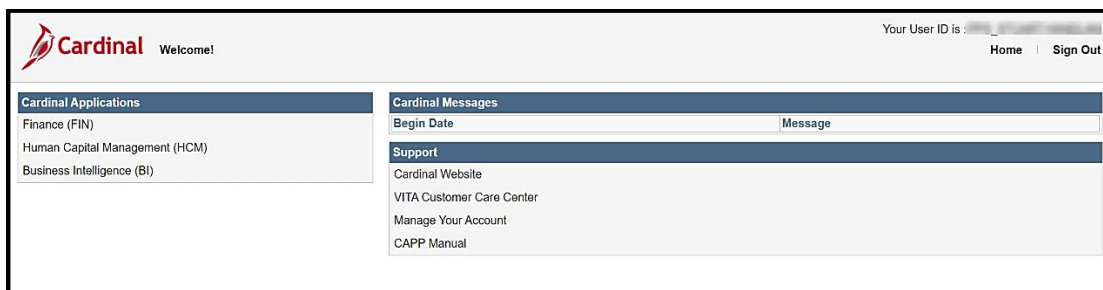
- Once you receive the call, enter the authentication code in the **Enter Code** field on your computer/device.

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

- To skip this step in the future, select the **Do not challenge me on this device again** checkbox. Okta remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, Okta 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.

- Click the **Verify** button to access the **Cardinal Portal**.



Cardinal Welcome! Your User ID is : [redacted] Home Sign Out

Cardinal Applications	Cardinal Messages
Finance (FIN) Human Capital Management (HCM) Business Intelligence (BI)	Begin Date [redacted] Message [redacted] Support Cardinal Website VITA Customer Care Center Manage Your Account CAPP Manual

The **Cardinal Portal** displays.

See the [Cardinal Portal Layout](#) section for information about the Portal page.