



Set Up Okta Verify for Cardinal Users

ACTION REQUIRED

The **Virginia IT Agency (VITA)** will stop supporting **SMS (text message)** and **phone call** logins through Okta. Soon, you will **no longer be able to receive a one-time code** via text or phone to log in to Cardinal. To ensure uninterrupted access, Cardinal recommends setting up the **Okta Verify mobile application**.

BEFORE YOU BEGIN

You will need the following information and devices:

- The **username/email and password** you use to sign in to Cardinal
- A **smartphone** and your Apple ID or Google account password (to download apps)
- Computer

Next

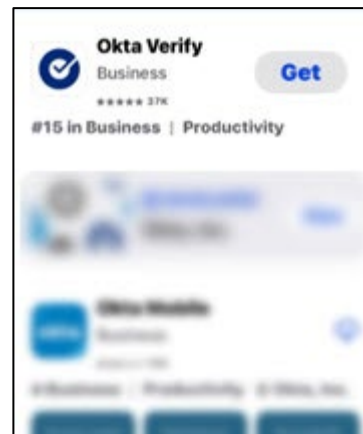
No computer? No Problem.

Click the button below to access smartphone-only setup instructions.

[Smartphone Only](#)

START HERE

[Phone] Download the Okta Verify App from the Apple App or Google Play store onto your smartphone.



ATTENTION COV USERS: The Cardinal system does not currently support the Okta Verify FastPass installed on workstations. Therefore, if you use Okta Verify FastPass on your desktop, you will still need to install Okta Verify on your smartphone to access Cardinal when off the COV network.



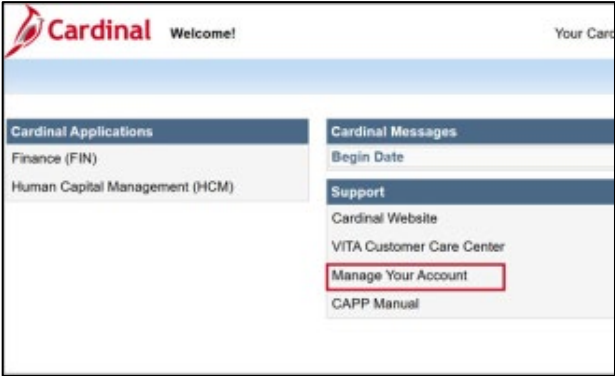
Set Up Okta Verify for Cardinal Users

ON YOUR COMPUTER

Access user account based on your user type shown in the table below.

Important: When signing in, be sure to use the **credentials associated with your Cardinal account**.

Using the correct credentials ensures you can successfully complete your Okta Verify setup for the Cardinal system login.

User Type	Who You Are	Link to Use
COV Agency User	You work at a VITA COV-Network agency and use an agency-provided email address to log in to Cardinal.	https://virginia.okta.com/enduser/settings Sign in using your Cardinal username and password .
All Others	You work at a Non-COV agency or Locality , or you use a personal email address to log in to Cardinal, or are a terminated/retired employee .	https://my.cardinal.virginia.gov • Sign in using your Cardinal username and password. • Don't get locked out! If you have entered your password incorrectly two times, stop immediately and click Forgot Password to easily reset it. • A third incorrect attempt will automatically lock your account for 30 minutes, forcing you to wait before you can reset your password. • Select Manage Your Account link. 
Confirmation of an agency's network status can be found in the Agency Network Status list.		

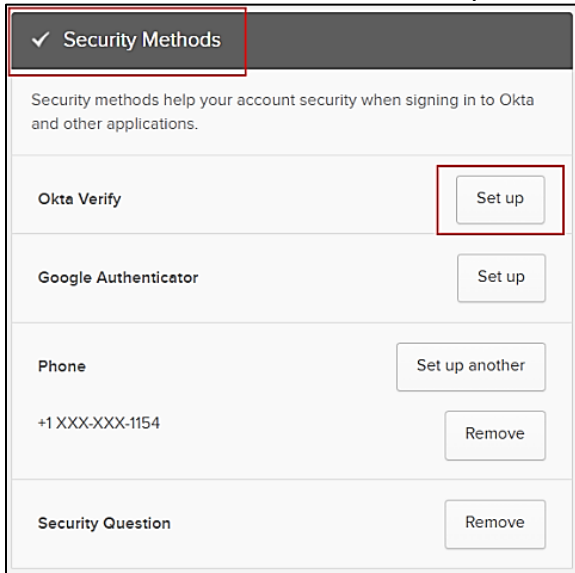
BEGIN OKTA VERIFY SETUP

Instruction Key:

- Steps you need to complete on your **smartphone** are labeled **[Phone]**
- Steps on your **computer** are labeled **[Computer]**

1. [Computer] On Settings page, scroll down to **Security Methods**. Click the **Set Up** button for **Okta Verify** or **Set up another**.

Non-COV users need to click Set Up

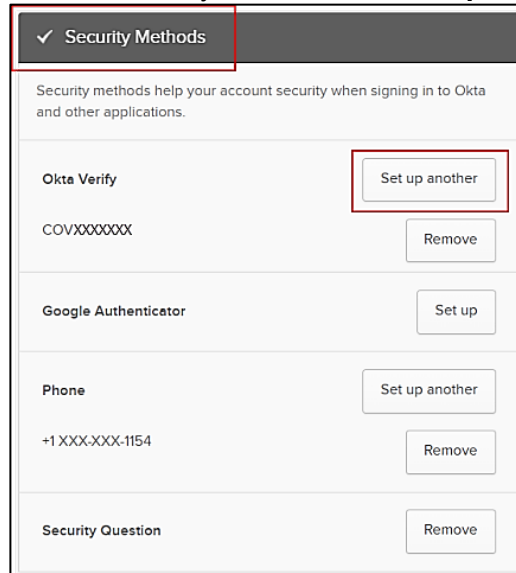


✓ Security Methods

Security methods help your account security when signing in to Okta and other applications.

Okta Verify	Set up
Google Authenticator	Set up
Phone +1 XXX-XXX-1154	Set up another Remove
Security Question	Remove

COV users may need to click **Set up another**



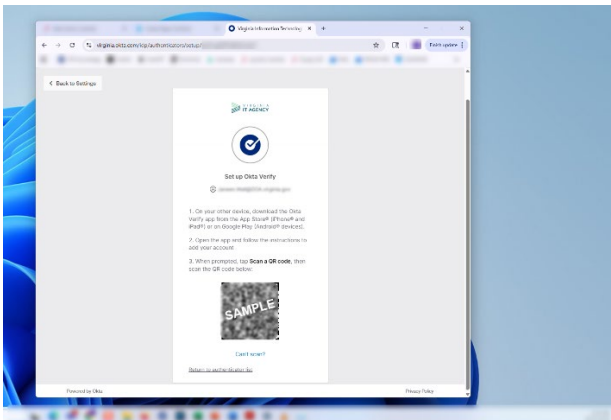
✓ Security Methods

Security methods help your account security when signing in to Okta and other applications.

Okta Verify COVXXXXXX	Set up another Remove
Google Authenticator	Set up
Phone +1 XXX-XXX-1154	Set up another Remove
Security Question	Remove

2. [Computer] You will first be guided through several screens on your computer prompting you to authenticate your identity, after which the Set up Okta Verify screen will display.

Once you successfully authenticate your identity using your Cardinal email and password, a QR code will display on your computer screen.

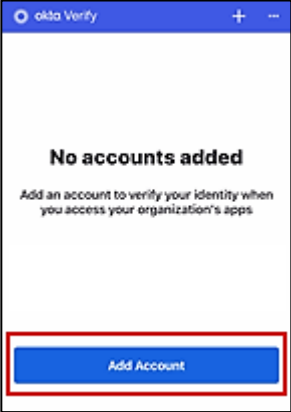
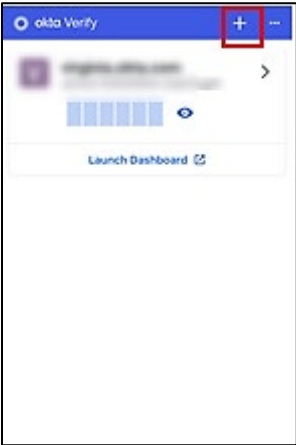
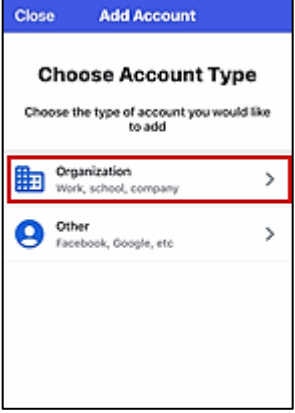


For the next step, switch to your smartphone
The Okta Verify app is needed in order to continue.



Set Up Okta Verify for Cardinal Users

3. [Phone] Open the Okta Verify app.

a. If this is the first time you are using the Okta Verify app, you will be prompted to Add Account. 	b. If you already use Okta Verify to access other accounts, tap the + (plus) symbol in the top right corner to proceed. 	c. On the Choose Account Type screen, tap Organization 
d. When prompted, tap Skip on the screen Add Account from Another Device to proceed to QR code option on next screen. 	e. Tap Yes, Ready to Scan 	f. Hold your smartphone up to the computer screen to scan the QR code. If your computer onscreen QR code has timed out, refresh the page on your computer. 

4. [Phone] Once the QR code is scanned, when prompted to enable passcode confirmation, choose **Enable**. Your smartphone will guide you through next steps. The app will show **Account Added** screen. Tap **Done** to complete smartphone setup. Proceed to next steps.



Set Up Okta Verify for Cardinal Users

Okta Verify	Okta Verify	Okta Verify
 Enable Face ID or Passcode Confirmation Protect your account by confirming your Face ID or passcode when you sign in using Okta Verify. Your organization requires Face ID or Passcode confirmation to be enabled for your account. Enable	 Enable Face ID or Passcode Confirmation Do you want to allow "Okta Verify" to use Face ID? Okta Verify uses Face ID to verify your identity. Don't Allow Allow Enable	 Account Added Janeen.Wall@DOA.virginia.gov You can now securely sign in to your organization's apps. Return to your organization's instructions to continue. Important: Keep this app installed on your device. You'll need it to sign in. Done



Set Up Okta Verify for Cardinal Users

TEST CARDINAL LOGIN WITH OKTA VERIFY

[Computer] or [Phone] Log in to Cardinal (my.cardinal.virginia.gov) using **Okta Verify** for authentication. To change your authentication method from the default displayed, click the drop-down arrow beside the icon and choose **Okta Verify**.

ATTENTION COV USERS: You will only be prompted for multifactor authentication (MFA) when you log into Cardinal while off the COV network and/or off VPN. Complete this step at your convenience.



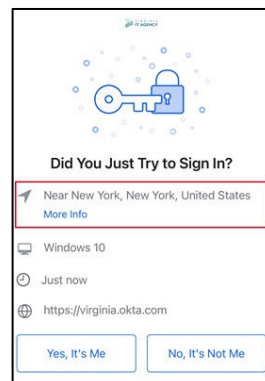
PUSH NOTIFICATIONS – LOCATION ALERTS

When using **Okta Verify push notifications** for authentication, it is very common for the login location displayed in the alert to not match your current physical location. It is OK to approve/authenticate **if you initiated the login**.

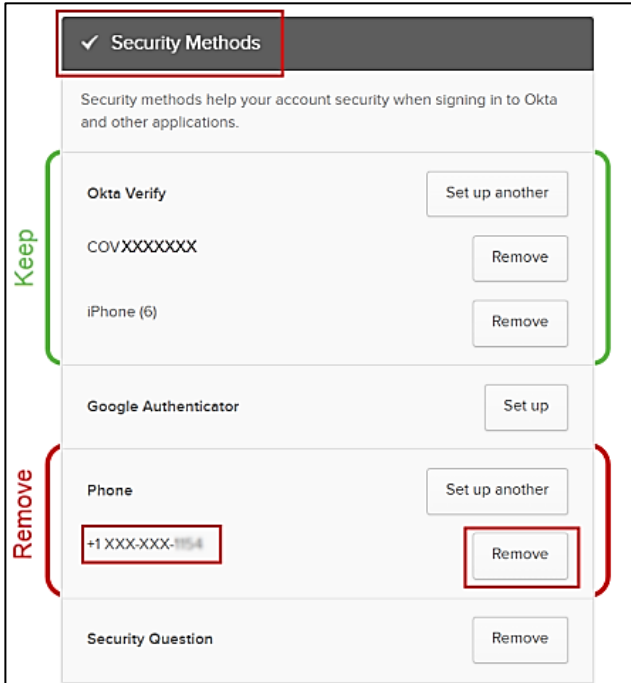
Why this happens:

This difference is typically a result of how cell phone networks or VPNs route connection traffic, and it is a normal occurrence

Example:



FINAL STEP – REMOVE SMS/PHONE



[Computer] Please read the details below carefully

Return

to <https://virginia.okta.com/enduser/settings> webpage.

Note: If the page has timed out, sign back in with your Cardinal username and password.

- Scroll down to the **Security Methods** section
- Locate the **Phone section** of Security Methods. You will see your phone number with the last 4 digits visible.
- **Do not make changes** to devices listed in the **Okta Verify section**.
- **Action Step:** Click the **Remove button next to the smartphone number** under **Phone** section of Security Methods, follow any on-screen prompts to confirm removal.