



Cardinal MFA Update

Session 2 – March 3, 2026

9:30 am to 11:00 am



Objectives for Today

- Provide non-COV IT, HR, and Finance leadership with an update on additional MFA options available to users ahead of VITA's planned retirement of SMS/Voice **in early April**, with the goal of transitioning as many non-COV users as possible beforehand.
- Demonstrate the current MFA options and two additional options “coming soon” that do not require users to use a smartphone app.

Note: For organizations, interested in desktop-based Okta FastPass, additional targeted discussions may be needed for your IT groups to deploy and support installs of FastPass on your desktop image.



MFA Options

The table below shows the current and coming soon MFA options.

MFA Option	Status	Best for	Platform	Agency Effort/Support
Okta Verify	Available	Most users	Mobile Application (min. iOS 17.0/Android 13)	Low
Google Authenticator	Available	Users wanting a simple mobile code generator	Mobile Application (min. iOS 16.0/Android 11)	Low
Other TOTP Applications (Time-Based One-Time Password)	Available	Users with existing apps (Duo, Rapid Identity, Microsoft Authenticator, etc.)	Mobile Application (iOS/Android)	Low. Note: To enroll other TOTP apps, users must select the 'Google Authenticator' option and scan the QR code
Okta FastPass	Coming Soon (target Sunday 3/8)	Users who do not have a smartphone or prefer not to use a smartphone for authentication	Desktop	High – See information about agency responsibilities later in this deck.
Yubikey & Security keys	Coming Soon (target Sunday 3/8)	User requiring a physical hardware security key	Desktop/Mobile	High – Complex account configuration requirements. If used for Cardinal, cannot be used for other VITA Okta apps.

For more information from VITA, refer to [Okta Authentication Services | Virginia IT Agency](#)



Minor Look and Feel Differences Coming

When updates to the Cardinal sign-on page are deployed to support Okta FastPass and Security Keys for login, there will be minor changes to the overall look and feel of the authentication process for desktop-based logins. *There will be no changes for mobile logins to Cardinal.*

Change 1 – With the upcoming changes, the Cardinal login page will prompt for the username first, and the password field will appear only after the username is entered.

Currently

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.

Cardinal Username

Password

Sign In

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

To-Be

**Cardinal
NON-PRODUCTION**

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.

USER_NAME

Next

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

**Cardinal
NON-PRODUCTION**

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.

Enter Password

Verify

[Back to sign in](#)

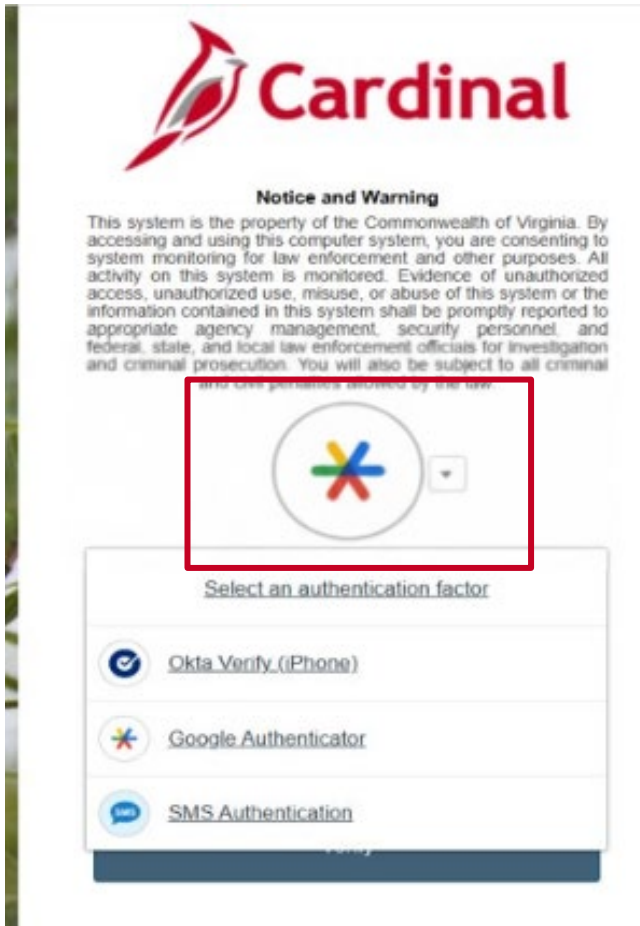
[Forgot Username](#) [Forgot Password](#)
[User Registration](#) [Sign-on Help](#)



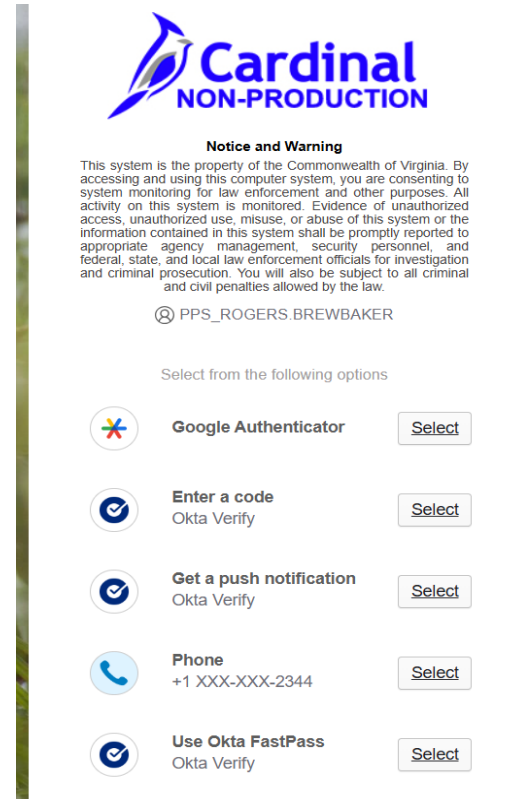
Minor Look and Feel Differences Coming

Change 2 – When MFA is required, MFA options will be displayed in a native Okta window as radio buttons versus a drop-down.

Currently



To-Be

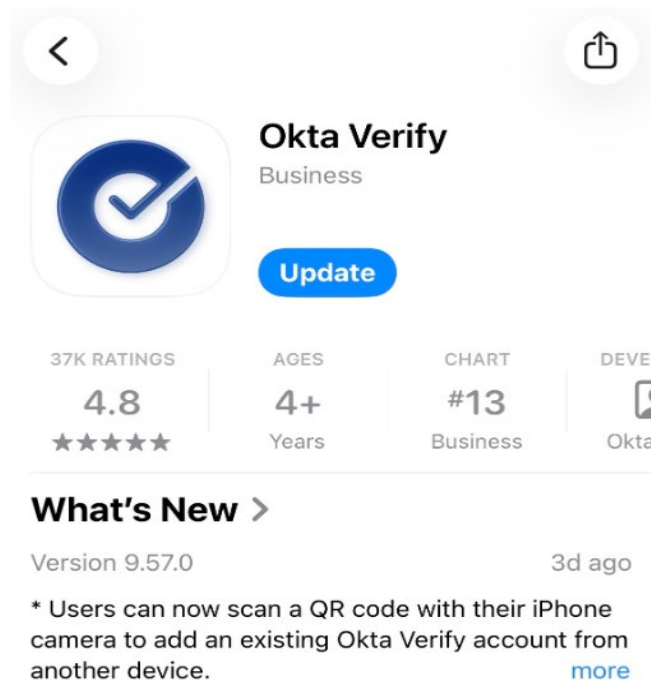


Demos – Okta Verify

Okta Verify is a smartphone app built by Okta to support MFA. Some older iPhones and Android models will not allow Okta Verify to be installed, as it frequently requires modern, security updates. Minimum requirement is iOS 17.0 / Android 13.

Setup and install instructions are located at the link below. More support is available from Cardinal help desk staff for Okta Verify than is available with some of the other authentication apps.

<https://www.cardinalproject.virginia.gov/oktaverify>

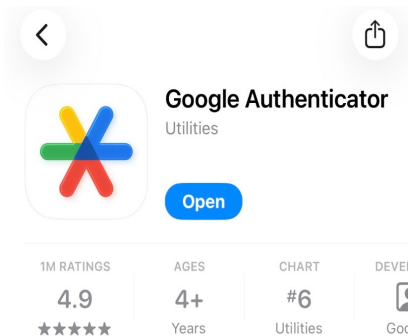


The screenshot shows the App Store page for the Okta Verify Business app. At the top, there is a back arrow on the left and a share icon on the right. The app icon is a blue circle with a white checkmark. The app name is "Okta Verify" and the category is "Business". Below the icon is a blue "Update" button. The app has 37K ratings with a 4.8 star rating, indicated by five stars. The age rating is "4+" (Years). The app is ranked #13 in the Business category. The developer is Okta. Below the app information is a "What's New" section with a right arrow. The latest update is Version 9.57.0, released 3 days ago. The update notes state: "* Users can now scan a QR code with their iPhone camera to add an existing Okta Verify account from another device." with a "more" link.

Demos – Google Authenticator and One-Time Password Apps

Google Authenticator and other TOTP Applications (Time-Based One-Time Password) are also current options. Users must select Google Authenticator to scan the QR code presented and setup the app. Google Auth and other Apps may work more efficiently in older smartphones than Okta Verify.

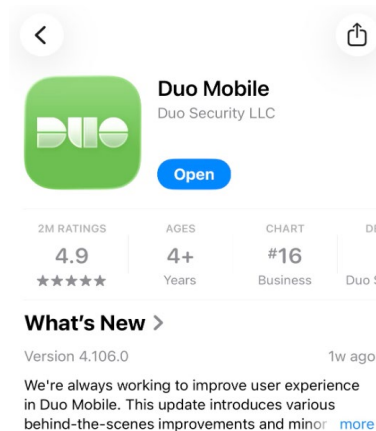
Cardinal help desk staff will only be able to provide users with limited support for these apps given the large number of possible options.



Google Authenticator
Utilities

Open

1M RATINGS	AGES	CHART	DEVELOPER
4.9 ★★★★★	4+ Years	#6 Utilities	Google



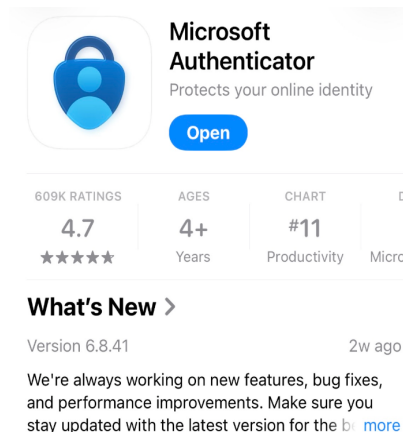
Duo Mobile
Duo Security LLC

Open

2M RATINGS	AGES	CHART	DEVELOPER
4.9 ★★★★★	4+ Years	#16 Business	Duo Security

What's New >
Version 4.106.0 1w ago

We're always working to improve user experience in Duo Mobile. This update introduces various behind-the-scenes improvements and minor [more](#)



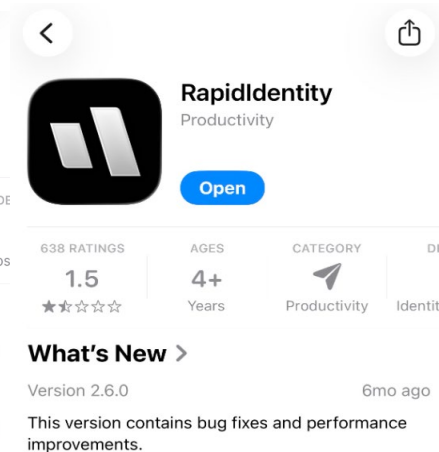
Microsoft Authenticator
Protects your online identity

Open

609K RATINGS	AGES	CHART	DEVELOPER
4.7 ★★★★★	4+ Years	#11 Productivity	Microsoft

What's New >
Version 6.8.41 2w ago

We're always working on new features, bug fixes, and performance improvements. Make sure you stay updated with the latest version for the best [more](#)



RapidIdentity
Productivity

Open

638 RATINGS	AGES	CATEGORY	DEVELOPER
1.5 ★☆☆☆☆	4+ Years	Productivity	Identit

What's New >
Version 2.6.0 6mo ago

This version contains bug fixes and performance improvements.



Demos – Okta FastPass

In response to feedback from a subset of users who either do not have a smartphone or prefer not to use one for authentication, over the past several months Cardinal has worked closely with VITA and Okta to provide alternatives to smartphone-based MFA options.

The primary and recommended non-smartphone solution is Okta Verify (FastPass) installed on a desktop; however, non-COV agencies will need to deploy and support the application within their own organizations.

Okta FastPass Agency Responsibilities

Agencies who elect to offer this option will be responsible for:

- Application deployment to agency Windows workstations – refer to [Public Articles - Deploying Okta Verify Desktop Client for Windows \(virginia.okta.com\)](#). For users on Apple Laptops, the install is more straight-forward and the user can download from the Apple App Store.
- End-user support and troubleshooting
- Ongoing maintenance and lifecycle management

If your agency plans to implement Okta FastPass, please submit a ticket to vccc@vita.virginia.gov with the subject line “Cardinal – Okta FastPass” by close of day Friday, March 6.

NOTE – There will be some adjustments required for the Cardinal Registration process for users who setup Okta FastPass as their MFA option.

Demos – Security Keys/YubiKeys

While FastPass is the recommended desktop-based solution, security keys and YubiKeys will also be an option for Cardinal logins, though with some limitations and added complexity.

To set up a security key, a user will first need to remove (or have the Cardinal Help Desk remove) all other MFA options. *In addition, security keys will work only for Cardinal logins and cannot be used to access other VITA Okta applications.*





Next Steps

- Additional MFA options are targeted for deployment this Sunday (3/8).
- Cardinal is updating relevant job aids and user help documentation.
- Communications and Cardinal message board updates outlining the look and feel changes will be published ahead of the sign-on page updates targeted for deployment.
- Additional user comms are planned throughout the month of March to encourage as many users as possible to move away from SMS/Voice before it is no longer an option.
- Organizations interested in Okta FastPass should submit a ticket by **Friday, March 6** to VCCC with “Cardinal FastPass” in the subject line, and additional guidance will be provided by the Cardinal and VITA teams.