

Innovate
Ohio
Platform

OHID MFA Job Aid

Updated: April 2024



**Department of
Administrative
Services**

MULTI-FACTOR AUTHENTICATION (MFA)

Setting up MFA enrollment

WHAT IS MFA?

Multifactor Authentication (MFA) is a security procedure that allows Ohioans to verify that they are who they claim to be. This is done by confirming additional identifying information from a secondary source.

KEY TERMS AND DEFINITIONS

Single Sign-On (SSO)



Single Sign On (SSO) refers to a sign on process which allows users to access multiple state agency resources through a single set of log in credentials (OHID and Password).

Multifactor Authentication (MFA)



Multifactor Authentication (MFA) is a second form of verification that the user logging in is who they claim they are. There will be multiple options available, including SMS text, phone call, email, and mobile app verification.

MFA REGISTRATION OPTIONS OVERVIEW

*There are four options available for MFA Registration. Please register for at least **two** MFA options.*



SMS Text Message

An SMS text with a PIN will be sent to the user's phone number.



Email

A PIN will be sent to the user's email associated with the OHID account.



Phone Call

An automated call will be made to the user's phone number.




IBM Verify App

User is given the option to authenticate through PIN displayed in app and an in-app push button option.

MFA REGISTRATION OPTIONS

*There are four options available for MFA Registration. Please register for at least **two** MFA options.*

It is recommended to choose a combination of phone-based and email options just in case you do not have multiple cell phones or lose your phone.




SMS Text Message

An SMS text with a PIN will be sent to the user's phone number.

Level of
Difficulty:

LOW

- The SMS verification option sends the user a one-time access code to their phone via text message.
- Users must select an active mobile phone number.
- For text message and phone call verification to be counted as separate methods, users cannot use the same phone number for both options.



Email

A PIN will be sent to the user's email associated with the OHID account.

LOW

- The Email verification option sends the user an email containing a one-time verification code to the email address they used to set up MFA.
- Users should use an active email account they have access to.

MFA REGISTRATION OPTIONS

*There are four options available for MFA Registration. Please register for at least **two** MFA options.*

It is recommended to choose a combination of phone-based and email options just in case you do not have multiple cell phones or lose your phone.



Phone Call

An automated call will be made to the user's phone number.

Level of
Difficulty:

LOW

- The Phone Call verification option places an automated phone call to the user's phone number.
- Users must select an active phone number.
- For text message and phone call verification to be counted as separate methods, users cannot use the same phone number for both options.



IBM Verify App

User is given the option to authenticate through PIN displayed in app and an in-app push button option.

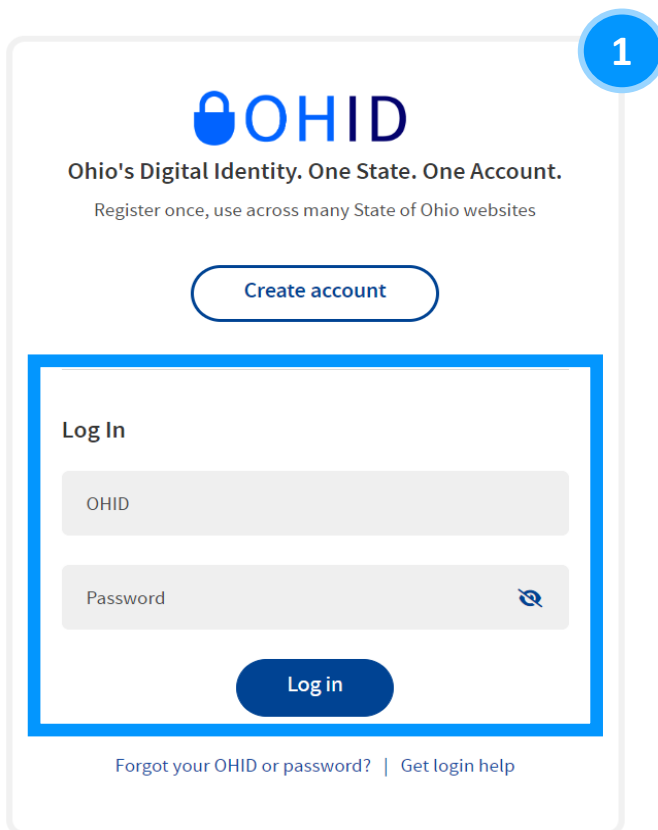
MEDIUM

- The IBM Verify verification app will send a push notification when selected as the MFA option.
- The IBM Verify app is free in both the Google Play and Apple App stores.

2-STEP VERIFICATION ENROLLMENT

- 1 Visit OHID.ohio.gov and log in using OHID and password.

Note: You can only enroll in 2-Step Verification options on the OHID website



OHID
Ohio's Digital Identity. One State. One Account.
Register once, use across many State of Ohio websites

Create account

Log In

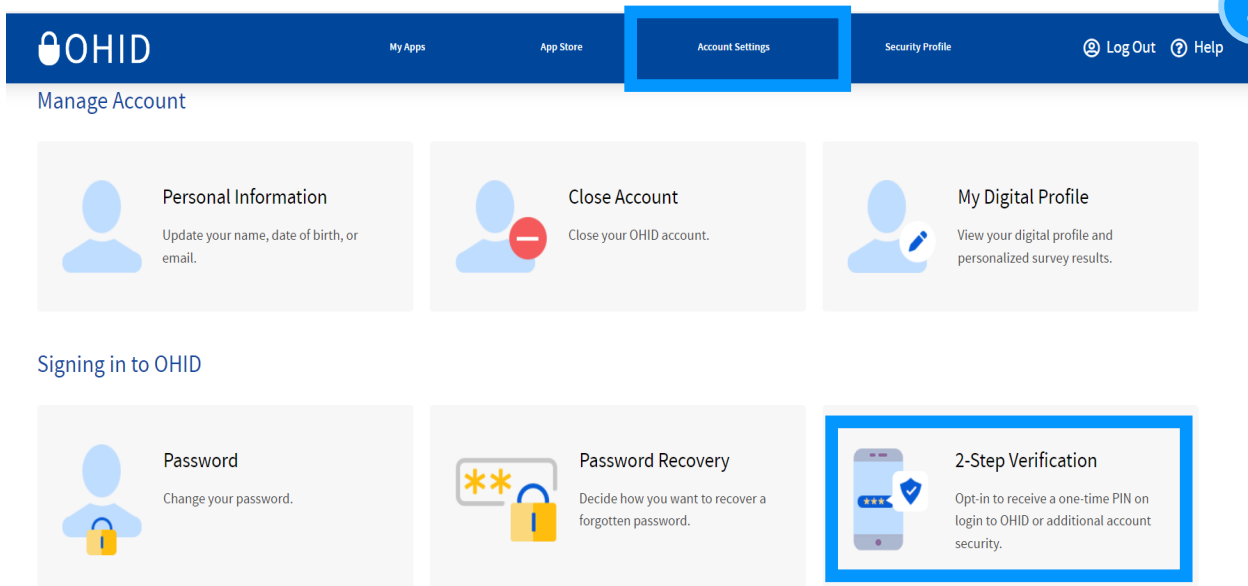
OHID

Password

Log in

Forgot your OHID or password? | Get login help

- 2 Select "Account Settings" then select "2-Step Verification."



OHID Manage Account

My Apps App Store Account Settings Security Profile Log Out Help

Personal Information
Update your name, date of birth, or email.

Close Account
Close your OHID account.

My Digital Profile
View your digital profile and personalized survey results.

Signing in to OHID

Password
Change your password.

Password Recovery
Decide how you want to recover a forgotten password.

2-Step Verification
Opt-in to receive a one-time PIN on login to OHID or additional account security.

2-STEP VERIFICATION ENROLLMENT

3 Select “Configure”.

[My Apps](#)[App Store](#)[Account Settings](#)[Security Profile](#)[Log Out](#) [Help](#)

3

Security Options

2-Step Verification

2-Step Verification provides an additional layer of security to verify your identity. In order to access certain agency applications, you must have your 2-Step Verification configured. Please note that setting up all identity verification methods will maximize your account security.



Configure 2-Step Verification for your OH|ID account

Click the configure button to be directed to the 2-Step Verification configure process. It is highly recommended that you configure all verification options.

[Configure](#)

4 Select “Add new method +”.

[IBM Security Verify](#)[App center](#)[My accesses](#)[My requests](#)

4

Profile & settings

[Profile](#)[Security](#)[Privacy](#)

Security

Protect your account access with a strong password plus an additional verification method as well as recovery options if you get locked out.



Verification methods

Manage your verification methods.

[Add new method +](#)

MDM managed devices

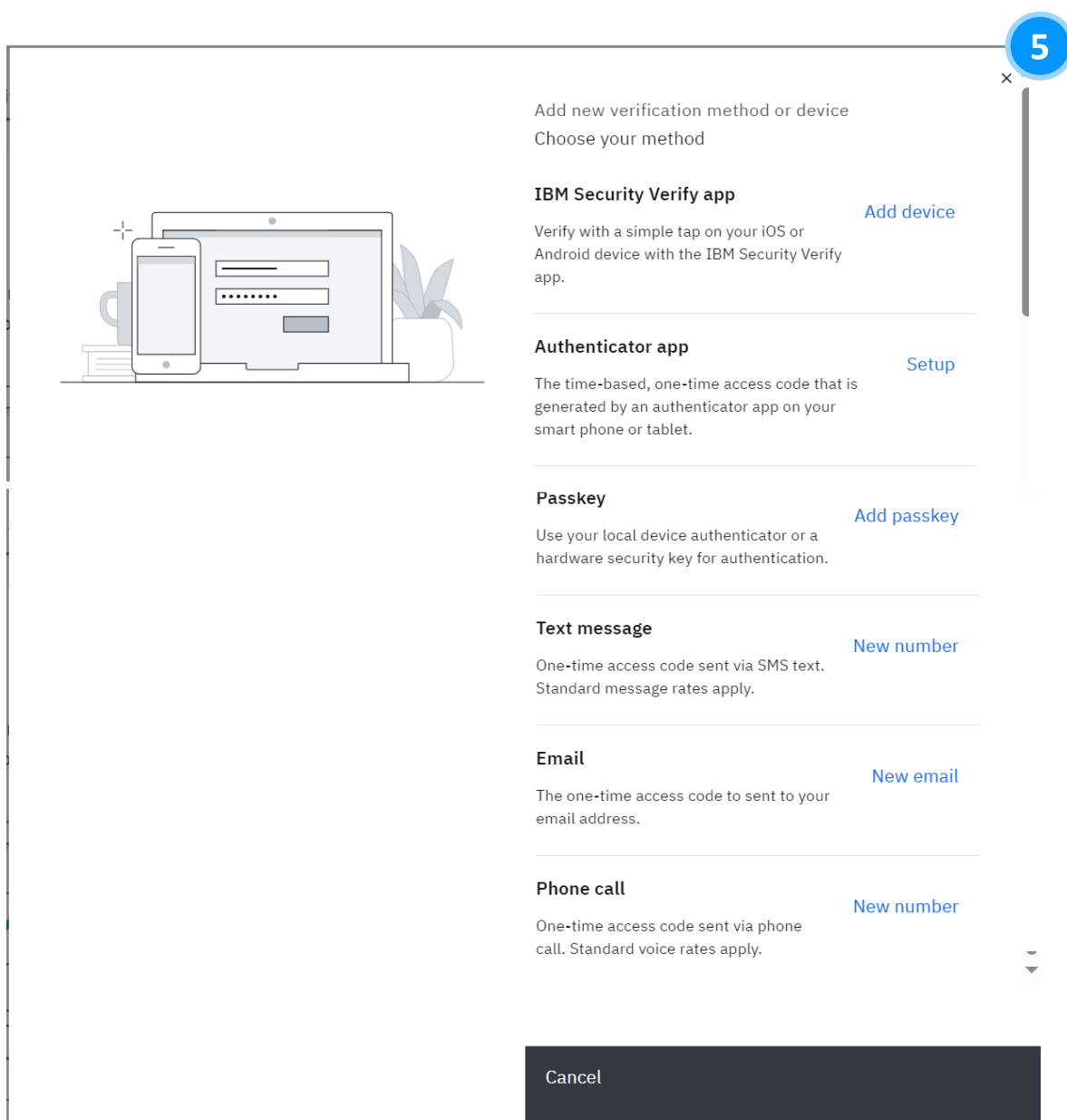
Manage your registered devices.

You do not have any registered devices.

2-STEP VERIFICATION ENROLLMENT

- 5 You will see all verification methods appear on the screen for selection.

Note: You will need to set up **2 methods** of verification. It is recommended that you select one phone-based option(Phone call or text) and one email option.



5

Add new verification method or device
Choose your method

IBM Security Verify app [Add device](#)
Verify with a simple tap on your iOS or Android device with the IBM Security Verify app.

Authenticator app [Setup](#)
The time-based, one-time access code that is generated by an authenticator app on your smart phone or tablet.

Passkey [Add passkey](#)
Use your local device authenticator or a hardware security key for authentication.

Text message [New number](#)
One-time access code sent via SMS text. Standard message rates apply.

Email [New email](#)
The one-time access code to sent to your email address.

Phone call [New number](#)
One-time access code sent via phone call. Standard voice rates apply.

Cancel

TEXT MESSAGE

2-Step Verification Enrollment Method

2-STEP VERIFICATION ENROLLMENT - TEXT MESSAGE

- 1 Select "New number" highlighted in blue.

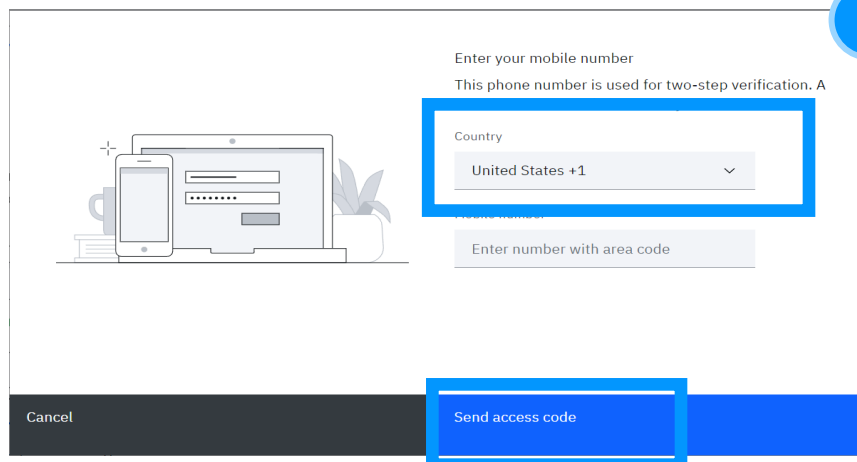
Text message

One-time access code sent via SMS text.
Standard message rates apply.

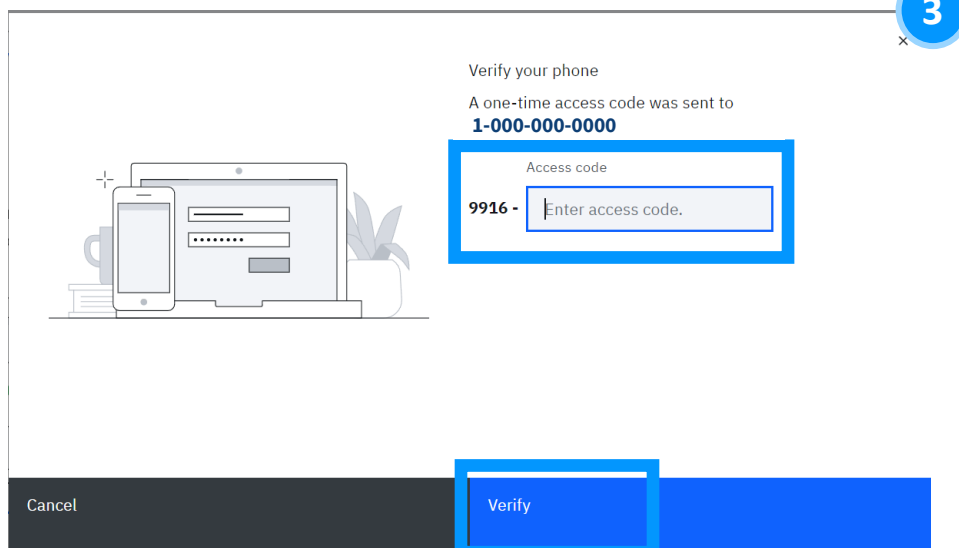
New number

- 2 Enter your Mobile number and select "Send access code".

Note: If the same phone number is entered for more than one 2-Step Verification options, you will be prompted to "Enroll another method"



- 3 Enter the access code that appears in the text message sent to you and select "Verify."



2-STEP VERIFICATION ENROLLMENT - TEXT MESSAGE

- 4 Once you enter and verify, you will see this page showing that you have successfully added the text message method of verification. You may select “Add additional method” if you have not yet enrolled in two methods or select “Done” if you have already done so.

4

Success!
The code was verified.



Add additional methods

Done

EMAIL

2-Step Verification Enrollment Method

2-STEP VERIFICATION ENROLLMENT - EMAIL

- 1 Select "New email" highlighted in blue.

Email

The one-time access code to sent to your email address.

New email

- 2 Enter your email address and select "Send access code"

Enter your email

This email is used for two-step verification. A one-time access code is sent to your email.

Email Address

Enter email address

Cancel

Send access code

- 3 Enter the access code that appears in the email that was sent to you and select "Verify."

Verify your email

Let's try it out

A one-time access code was sent to

Test@Gmail.com

8681 - Enter access code.

Cancel

Verify

2-STEP VERIFICATION ENROLLMENT - EMAIL

- 4 Once you enter and verify, you will see this page showing that you have successfully added the email method of verification. You may select “Add additional method” if you have not yet enrolled in two methods or select “Done” if you have already done so.



Success!

Your email is added

Test@Gmail.com

You can remove or add new two-step verification methods and devices in your account's Security Settings.

4
x

Add additional methods

Done

PHONE CALL

2-Step Verification Enrollment Method

2-STEP VERIFICATION ENROLLMENT - PHONE CALL

- 1 Select “New number” highlighted in blue.


Phone call

One-time access code sent via phone call. Standard voice rates apply.

New number

- 2 Enter your phone number and select “Call me”.

Note: If the same phone number is entered for more than one 2-Step Verification options, you will be prompted to "Enroll another method"



Enter your phone number

This phone number is used for two-step verification. A one-time verbal message with an access code is sent to your number.

Country

United States +1

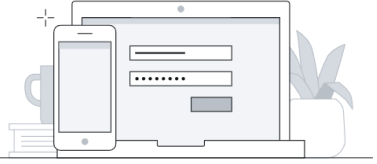
Phone number

Enter number with area code

Cancel

Call me

- 3 Pick up the phone call you receive and enter the access code that the automated messenger states to you and select “Verify.”



Verify your phone

A one-time access code was sent via phone call to
1-000-000-0000

Access code

9952 - Enter access code.

Cancel

Verify

2-STEP VERIFICATION ENROLLMENT - PHONE CALL

- 4 Once you enter and verify, you will see this page showing that you have successfully added the phone call method of verification. You may select “Add additional method” if you have not yet enrolled in two methods or select “Done” if you have already done so.



Success!

Your phone was added

1-000-000-0000

You can remove or add new two-step verification methods and devices in your account's Security Settings.

Add additional methods

Done

IBM VERIFY

2-Step Verification Enrollment Method

MFA ENROLLMENT: IBM VERIFY APP

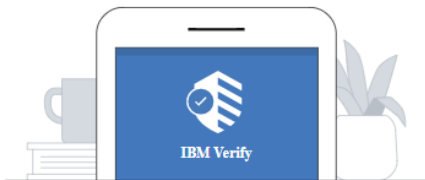
1

After selecting “Add Device” on the initial MFA enrollment page, you will download the IBM Verify App to your device and press “Connect Your Account”



Enroll with IBM Security Verify

Download the app



1

Follow these instructions or if IBM Security Verify is downloaded on your device, click "Connect your account".

1. Launch the App Store (iOS) or Google Play Store (Android) app.
2. Search for “IBM Security Verify”
3. Tap “Get” and “Install” to download the app.

[Use another method](#)

Connect your account

MFA ENROLLMENT: IBM VERIFY APP

- 2 After pressing “Connect your account” you will be met with the following screen and will need to access the IBM Verify app on your device to continue with registration.



Enroll with IBM Security Verify

Connect your account



2

Next, connect the app to your account. On your mobile device:

1. Launch the authenticator app.
2. Scan the QR code by using your device's camera.
3. Finally, follow the on-screen prompts and complete the registration process.

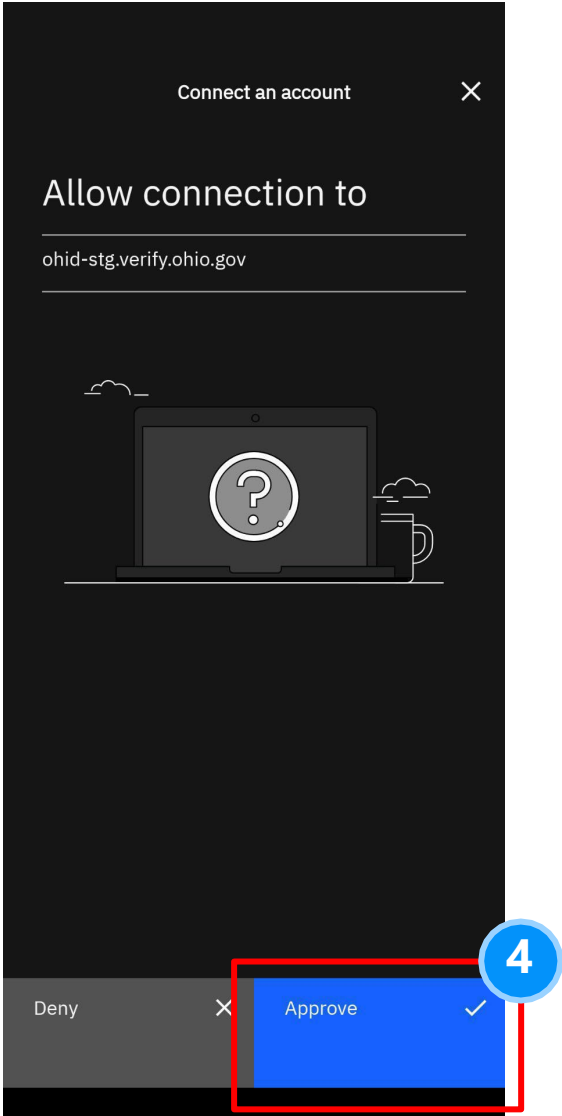
[Use another method](#)

Verify your device

MFA ENROLLMENT: IBM VERIFY APP

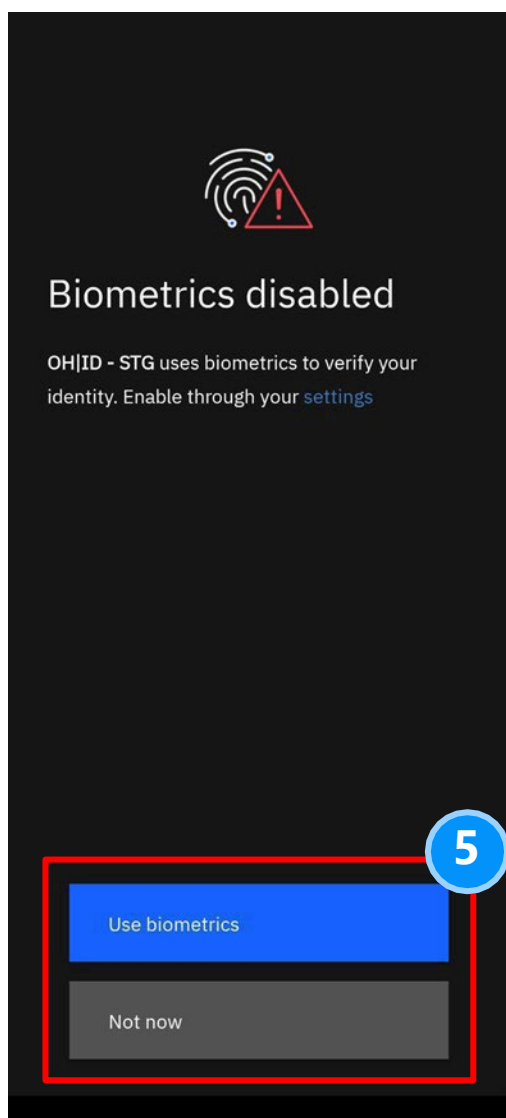
3 Scan the QR Code using the IBM app by opening the App's Camera.

4 Approve the connection after scanning the QR code.

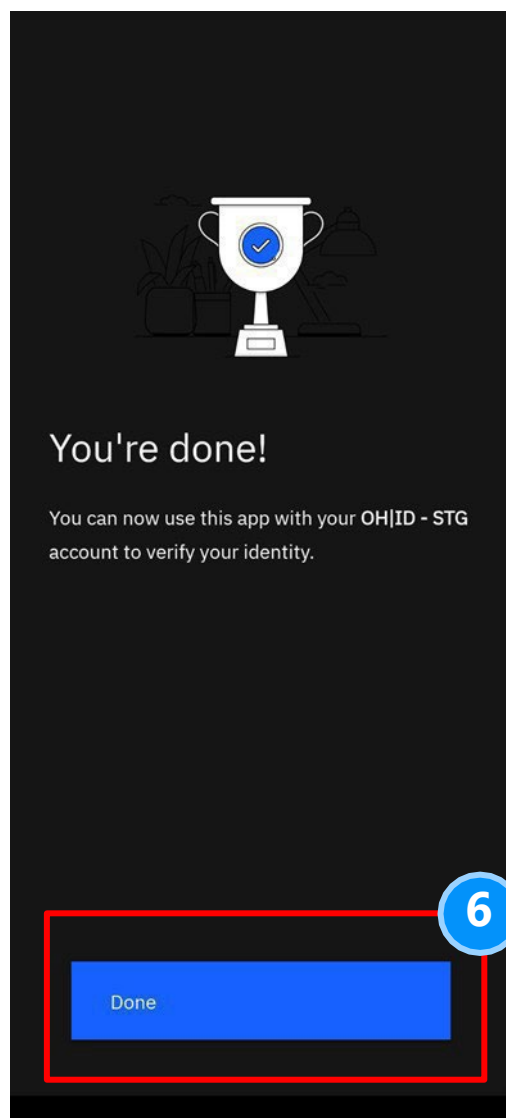


MFA ENROLLMENT: IBM VERIFY APP

- 5 Choose Biometrics preference. This has no bearing on linking the account to MFA.



- 6 Your account is now linked, press “Done”




MFA ENROLLMENT: IBM VERIFY APP

- 7 Select “Verify your device” to continue with IBM Verify Enrollment.

Enroll with IBM Security Verify

Connect your account



Next, connect the app to your account. On your mobile device:

1. Launch the authenticator app.
2. Scan the QR code by using your device's camera.
3. Finally, follow the on-screen prompts and complete the registration process.

[Use another method](#)

Verify your device

MFA ENROLLMENT: IBM VERIFY APP

8

You will now receive an “authentication challenge” to the IBM Verify app. To complete this, open the app, click the challenge, and approve the connection.

Note: The IBM Verify App does not allow screenshots for this step.



You have a pending authentication challenge on device Pixel 6 (Pixel 6)

Transaction: #ef76097e

[Use another method](#)

This system contains State of Ohio and United States government information and is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to and from this system is strictly prohibited, may be in violation of state and federal law, and may be subject to administrative action, civil and criminal penalties. Use of the system is governed by U.S. law and Ohio law and policies.

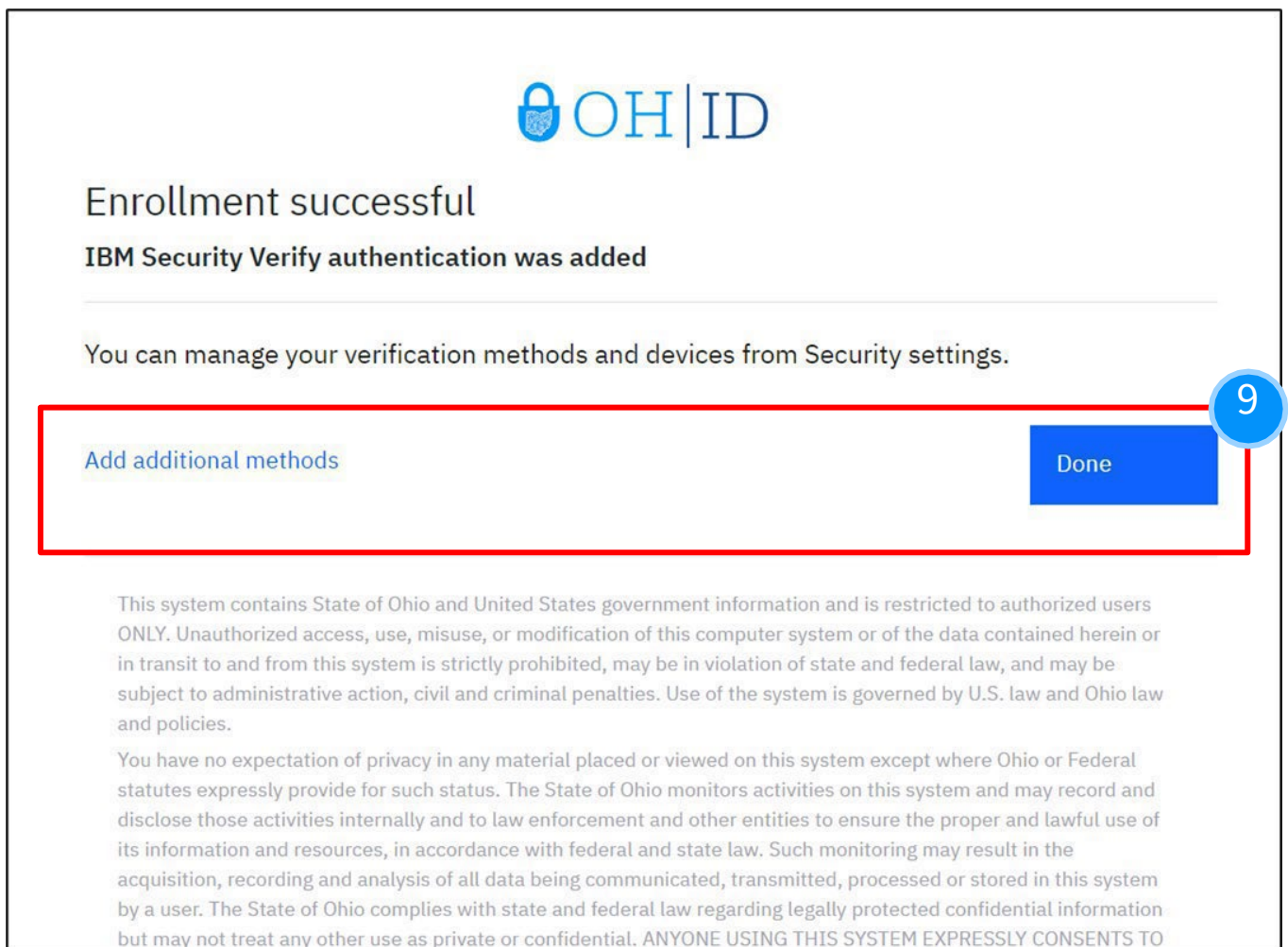
You have no expectation of privacy in any material placed or viewed on this system except where Ohio or Federal statutes expressly provide for such status. The State of Ohio monitors activities on this system and may record and disclose those activities internally and to law enforcement and other entities to ensure the proper and lawful use of its information and resources, in accordance with federal and state law. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. The State of Ohio complies with state and federal law regarding legally protected confidential information but may not treat any other use as private or confidential. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.


Ohio.gov

MFA ENROLLMENT: IBM VERIFY APP

9

After successfully completing the authentication challenge, you will be met with the following screen. From here you can select "Add Additional Methods" if you need another MFA option or "Done" if you are finished enrolling. Pressing "Done" will redirect you to the Application.





Enrollment successful

IBM Security Verify authentication was added

You can manage your verification methods and devices from Security settings.

[Add additional methods](#)

Done

This system contains State of Ohio and United States government information and is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to and from this system is strictly prohibited, may be in violation of state and federal law, and may be subject to administrative action, civil and criminal penalties. Use of the system is governed by U.S. law and Ohio law and policies.

You have no expectation of privacy in any material placed or viewed on this system except where Ohio or Federal statutes expressly provide for such status. The State of Ohio monitors activities on this system and may record and disclose those activities internally and to law enforcement and other entities to ensure the proper and lawful use of its information and resources, in accordance with federal and state law. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. The State of Ohio complies with state and federal law regarding legally protected confidential information but may not treat any other use as private or confidential. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO

9

2-STEP VERIFICATION ENROLLMENT: IBM VERIFY BEST PRACTICES

1. Before enrolling in the IBM Verify option, please download the IBM Verify application from the Apple App Store or the Google Play store.
2. The QR code provided to link your 2-Step Verification option to your device/application is for one-time use only. If you fail to connect the application the first time, you will need to return to the initial 2-Step Verification enrollment page, select add device, select “IBM Verify” and begin the process again.
3. The option for biometric login is dependent on your device capability.
 1. *E.g., If you have an iPhone with a “home” button (iPhone 8/8s) with TouchID activated, you can use the biometric confirmation. Any models without a “home” button and TouchID will be unable to confirm identity with biometrics. However, if you have FaceID enabled, you can select that option for biometric confirmation.*
4. Although IBM Verify is not a “phone-based option” like SMS Text and Phone Call, we still recommend choosing an email-based backup as your secondary 2-Step Verification option. If you do not have access to your registered phone number(s), you will not be able to complete 2-Step Verification with IBM Verify, SMS Text or Phone call, but will be able to complete 2-Step Verification via email.