



User Manual

PPM Version 2.0

FHA Connection Multi-Factor Authentication

U.S. Department of Housing and Urban Development

August 2023



Solution Information

	Information
Solution Name	FHA Connection Multi-Factor Authentication
Solution Acronym	FHA Connection (FHAC/F17C)
Version/Release Number	Version 1.0

Document History

Version No.	Date	Author	Revision Description
1.0	08/02/2023	Pyramid Systems, Inc.	Original Draft



Content

Solution Information	ii
Document History	ii
Contents	iii
1. Solution Summary	1
1.1 Features.....	1
1.2 Configuration.....	1
1.3 Data Flows.....	1
1.4 Contingencies and Alternate Modes of Operation	1
2. Getting Started	2
2.1 Software Version	2
2.2 Solution Requirements.....	3
2.3 Access Information.....	3
2.4 Logging On	4
2.5 Solution Menu.....	5
2.6 Changing User ID and Password.....	5
2.7 Exit Solution	5
3. Using the Solution (Online).....	6
3.1 FHA Connection MFA Start Page	6
3.1.1 Signing in with Password.....	6
3.1.2 Signing in with PIV / CAC Card	7
3.2 Setting Up Authentication Methods	8
3.2.1 Authenticating with Phone	9
3.2.2 Authenticating with Security Question	11
3.3 Optional Mobile App Authentication	12
3.3.1 Google Authenticator.....	13
3.3.2 Okta Verify	14
3.4 Special Instructions for Error Correction.....	14
3.5 Caveats and Exceptions.....	14
4. Using the Solution (Batch)	15
4.1 <Solution Function Name>.....	15
4.1.1 <Solution Sub-Function Name>	15



4.2	Special Instructions for Error Correction.....	15
4.3	Caveats and Exceptions.....	15
4.4	Input Procedures and Expected Output.....	15
5.1	Query Capabilities.....	15
5.2	Query Procedures.....	15
6.1	Report Capabilities.....	16
6.2	Report Procedures.....	16
7.1	Solutions to Common Problems.....	17
7.2	Getting More Help.....	17
7.3	Helpdesk.....	17
Appendix A: References.....		18
Appendix B: Key Terms.....		19



1. Solution Summary

FHA Connection Multi-Factor Authentication (MFA) is an added layer of security used to verify an end user's identity when they sign into the FHA Connection system. Implementing the MFA solution by Okta, Inc., reduces the risks of compromised passwords. This solution enables greater security without compromising the user experience for Single Family Housing lenders.

1.1 Features

1.1.1. Flexible Login

FHA Connection MFA enables users to sign in with either a user ID/password or PIV/CAC card. Users logging in with a user ID/password will be prompted for a 2nd authentication factor. The PIV/CAC card login is only available for HUD employees and contractors that were provided PIV cards by HUD.

1.1.2. Multi-Factor Authentication Options

FHA Connection MFA provides users with various access verification options. These include:

- One-time verification code sent to phone via text message (SMS)
- One-time verification code sent to phone via phone call (note: this option also works with a land line if no cell/smart phone is available)
- Using the Okta Verify phone application (iPhone or Android)
- Using the Google Authentication phone application (iPhone or Android)

In addition, users are prompted to set up a security question. This security question is not used for daily authentication, but it is used if needed to unlock a user's Okta account. For the security question, users can choose a security question from a list of 19 options or create their own security question.

1.2 Configuration

Users will continue to use the same login page as a starting point to enter the FHAC applications. There are no underlying changes to the applications. This only affects the login process to FHAC.

1.3 Data Flows

Not applicable.

1.4 Contingencies and Alternate Modes of Operation

During a pilot of the MFA capability, an alternate URL will be provided to login using the MFA capabilities. If issues arise during the pilot, the original FHAC sign-in URL can be used.



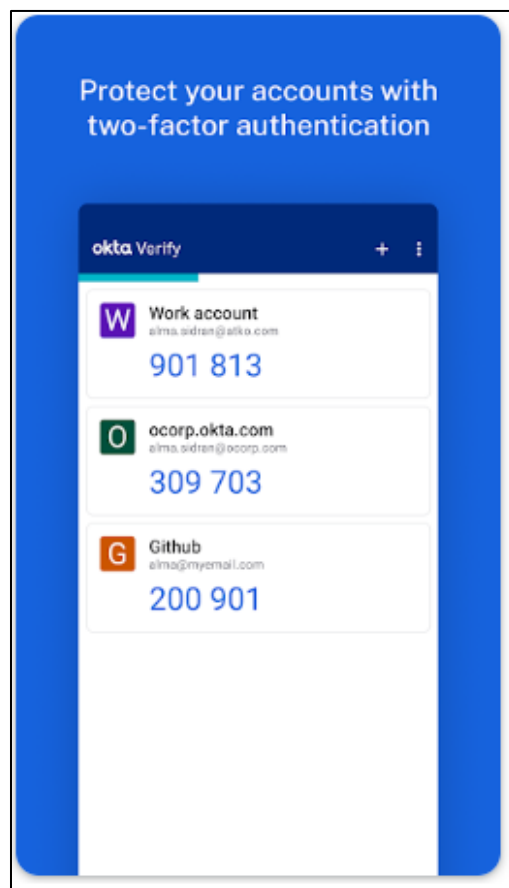
2. Getting Started

2.1 Software Version

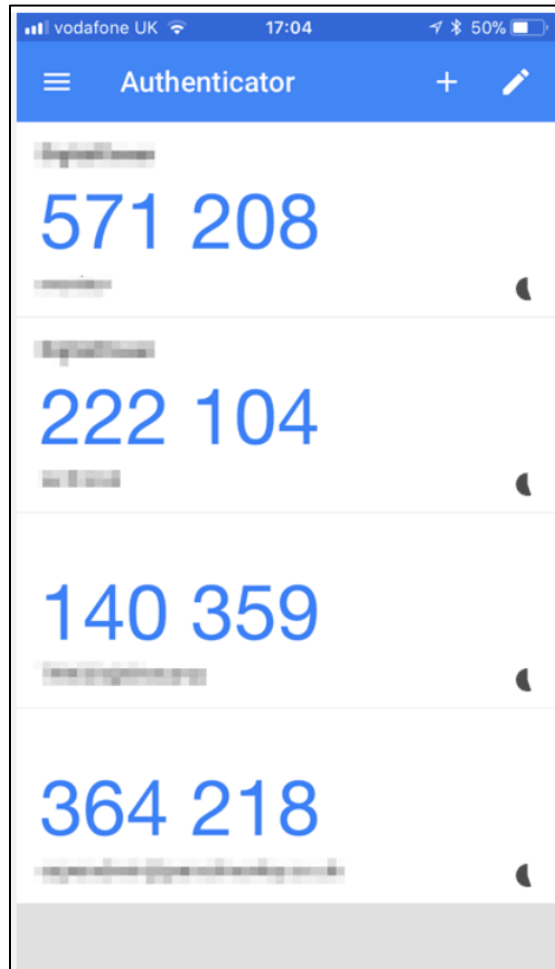
As preparation for using the Multi-Factor Authentication (MFA), FHAC users can download one of the free smart phone “authenticator” applications via the Apple App Store (iPhone) or the Google Play Store (Android).

If you are already using one of these two applications for other sites to authenticate, you can just use your existing application by adding another site to the authentication app by clicking the + sign and adding another account.

Okta Verify – This application is provided by Okta Inc. After setting up your account, the Okta Verify application will give you a verification number for your account that you will use to authenticate. This number changes every 30 seconds. If you sign in to FHAC with your user ID/password, you will be prompted to enter this rolling number.



Google Authenticator – The Google authenticator application works similarly to the Okta Verify application. If you choose this authenticator to use for FHAC, open the app and look for the HUD FHAC account (see setup later in this document), and enter your verification number.



2.2 Solution Requirements

HUD Employees and contractors that have a HUD PIV card can use the PIV card to login to FHAC. After the initial setup, additional authentication is not required when using the PIV card (and PIV card PIN).

Users signing into FHAC with the user ID/password will be prompted for another authentication method and will have to enter a one-time verification key obtained from one of text message (SMS), phone call, Okta Verify, or Google Authenticator.

2.3 Access Information

Users that do not have or do not wish to use a smart phone application can enter a land line telephone number during initial setup. When using this method, the user will receive a phone call with an automated record of the one-time verification number.



2.4 Logging On

Users should access FHA Connection using the same URLs/bookmarks they have always used. If the user goes to the FHA Connection Welcome Page (<https://entp.hud.gov/clas>) the user can click “Sign on” to access the MFA solution.

FHA Connection

Home Main Menu ID Maintenance E-mail Us Contact Us Sign Off

Welcome

The FHA Connection provides FHA-approved lenders and business partners with direct, secure, online access to computer systems of the U.S. Department of Housing and Urban Development (HUD).

[Sign on](#)

[Forgot Your Password?](#)
[Forgot Your User ID?](#)

Getting Started

- [About This Site](#)
- [Registering a New User](#)
- [Hours of Operation](#)
- [Contact Us](#)
- [OKTA Setup](#)


References

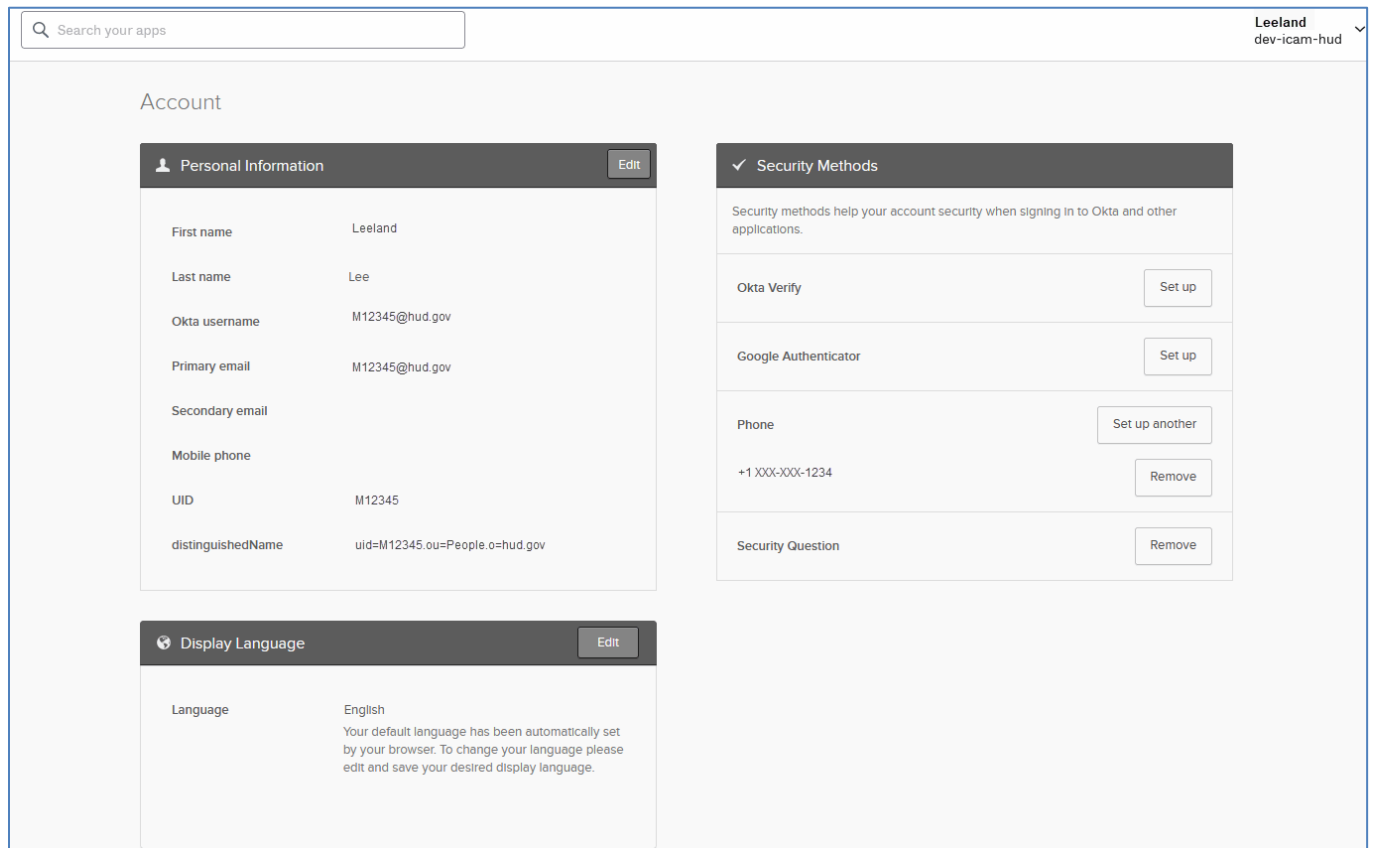
- [Frequently Asked Questions](#)
- [Quick Start Guide](#)
- [FHA Connection Guide](#)

All pilot participants are registered FHA Connection users; therefore, new user IDs are not required.



2.5 Solution Menu

Note the Okta Setup link on the page above. You can use this link to go to an Okta dashboard where you can edit your profile and set up additional authentication methods. Once on the dashboard, there is a dropdown box next to your name (or from the  icon) in the upper right corner of the screen. Choose Settings there to see additional authentication methods or to change your security question.



The screenshot shows the Okta user profile page. At the top left is a search bar labeled "Search your apps". At the top right, the user's name "Leeland" and email "dev-icam-hud" are displayed. The main content is divided into three sections:

- Personal Information** (with an "Edit" button):

First name	Leeland
Last name	Lee
Okta username	M12345@hud.gov
Primary email	M12345@hud.gov
Secondary email	
Mobile phone	
UID	M12345
distinguishedName	uid=M12345.ou=People.o=hud.gov
- Security Methods** (with a checkmark icon):

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

Okta Verify	Set up
Google Authenticator	Set up
Phone	Set up another
+1XXX-XXX-1234	Remove
Security Question	Remove
- Display Language** (with an "Edit" button):

Language	English
----------	---------

Your default language has been automatically set by your browser. To change your language please edit and save your desired display language.

2.6 Changing User ID and Password

The same password requirements will continue to exist under multi-factor authentication. Users will be required to change passwords every 90 days and following the password strength rules already in-place.

2.7 Exit Solution

Users can simply close out the browser.



3. Using the Solution (Online)

3.1 FHA Connection MFA Start Page

The sign-in process begins on the FHA Connection MFA Start page. First, users are required to enter their username, then presented the option to select “Keep me signed in.” Second, users are required to choose between selecting “Next” or selecting “Sign in with PIV / CAC card.”

3.1.1 Signing in with Password

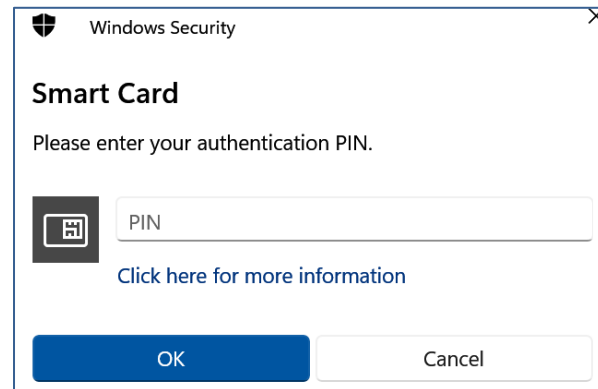
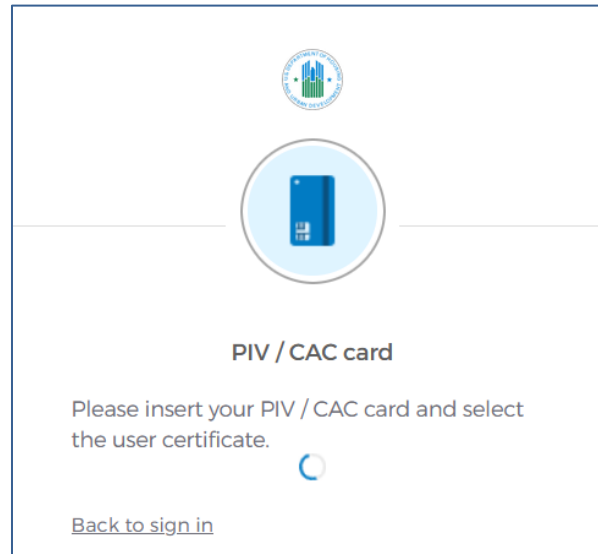
If the user opts not to sign in with a PIV / CAC card, they are prompted to enter a password.

A screenshot of the FHA Connection MFA Start Page sign-in form. The form is enclosed in a blue border and features the U.S. Department of Housing and Urban Development logo at the top center. Below the logo, the text "Sign In" is centered. A "Username" label is positioned above a text input field containing "M12345". Below the input field is a checkbox labeled "Keep me signed in". A dark blue button with the text "Next" is centered below the checkbox. Below the button, the word "OR" is centered between two horizontal lines. Below the lines is a blue-bordered button with the text "Sign in with PIV / CAC card". At the bottom of the form, there are two links: "Unlock account?" and "Help".



3.1.2 Signing in with PIV / CAC Card

If the user opts to sign in with a PIV / CAC card, they are prompted to insert their PIV / CAC card if not already inserted and then will be prompted to enter the PIV card PIN.







3.2 Setting Up Authentication Methods

After the user signs in, they are prompted to authenticate using a phone and a security question. These two methods are required. If you choose not to use a smart phone application (Okta Verify or Google Authenticator), you can enter a land line phone number to receive one-time verification keys via a phone call recorded message. If you choose to use text messages, enter your cell phone number here.

After setting up these two “required” authentication methods, the user will be prompted to add additional “optional” authentication methods. This is where you can choose the Okta Verify application, the Google Authenticator application, or both. (NOTE: We currently do not use the Microsoft Authenticator for FHAC).





Set up security methods

 M12345

Security methods help protect your Okta account by ensuring only you have access.

Set up required

-  **Phone**
Verify with a code sent to your phone
Used for access
[Set up](#)
-  **Security Question**
Choose a security question and answer that will be used for signing in
Used for recovery
[Set up](#)

[Back to sign in](#)



3.2.1 Authenticating with Phone

If the user opts to authenticate with a phone, they are prompted to choose between receiving a verification code via SMS or voice call. The default selection is SMS, and users are advised that carrier messaging charges may apply.

After a selection is made, the user will select the country associated with their phone number. The default country selection is “United States.” If the user selects a different country, then that country code will automatically update in the phone number field below.

The user is required to enter a complete phone number. If the user selected voice call instead of SMS, then the user will have the option to input an extension for the phone number. When all information is entered, the user will click “Receive a code via SMS” and/or “Receive a code via voice call.”

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Set up phone authentication

M12345

Enter your phone number to receive a verification code via SMS.

SMS

Voice call

Country

United States

Phone number

+1

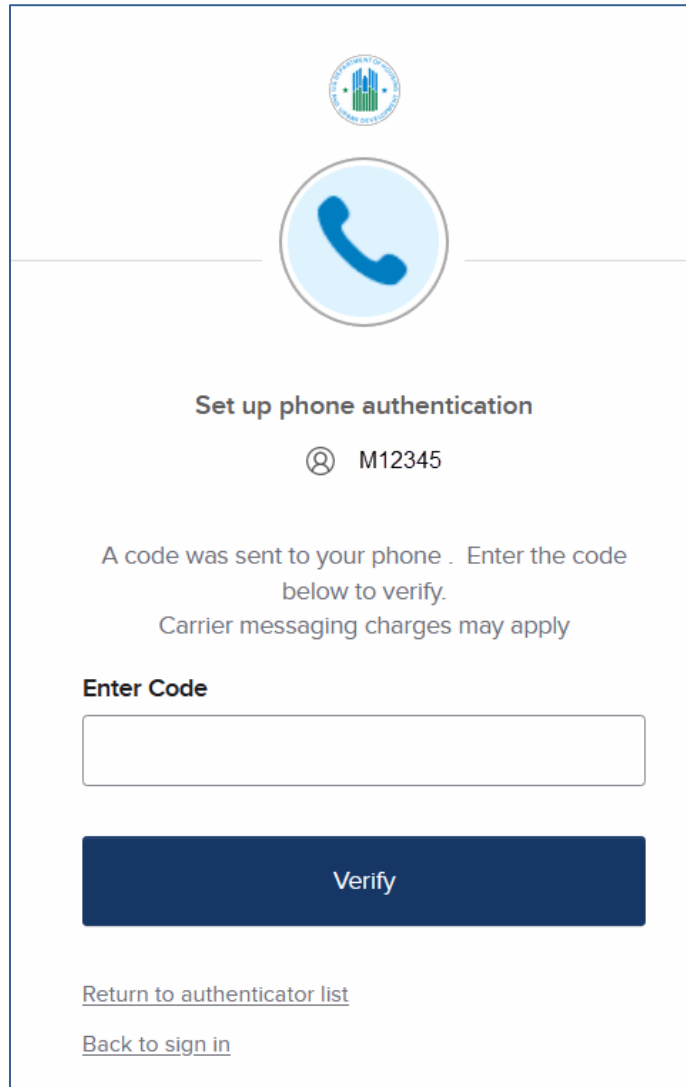
Receive a code via SMS



[Return to authenticator list](#)

[Back to sign in](#)




A new screen will prompt the user to enter the numeric verification code that was sent to their phone as either SMS or communicated via voice call. When the code is entered, the user will click “Verify.”

A screenshot of a mobile application screen for setting up phone authentication. At the top center is the U.S. Department of Housing and Urban Development logo. Below it is a large blue telephone handset icon inside a light blue circle. The main heading is "Set up phone authentication". Underneath, there is a phone number "M12345" with a small circular icon to its left. Below the number, there is explanatory text: "A code was sent to your phone . Enter the code below to verify." and "Carrier messaging charges may apply". A text input field labeled "Enter Code" is positioned below the text. At the bottom of the screen is a dark blue button with the word "Verify" in white. Two links are located at the very bottom: "Return to authenticator list" and "Back to sign in".

Set up phone authentication

 M12345

A code was sent to your phone . Enter the code below to verify.
Carrier messaging charges may apply

Enter Code

Verify

[Return to authenticator list](#)
[Back to sign in](#)



3.2.2 Authenticating with Security Question

The security question is not used for normal authentication to FHAC. The security question is only used if you need to unlock your account (self-service). If you click “Forgot Password” on the initial login screen, you will be prompted for the security question. To set-up your security question initially, you are prompted to choose a security question from a list of 19 options or create their own security question. The default selection is “Choose a security question.”


A screenshot of a web form titled "Set up security question". At the top center is a blue shield icon with a white question mark. Below the icon, the text "Set up security question" is displayed. Underneath, there is a user identifier "M12345" preceded by a person icon. Two radio buttons are present: the first is selected and labeled "Choose a security question", and the second is unselected and labeled "Create my own security question". Below these is a section titled "Choose a security question" containing a dropdown menu with the text "What is the food you least liked as a child?". Underneath the dropdown is an "Answer" field, which is a text input box with a small eye icon on the right side. At the bottom of the form is a large blue button labeled "Verify". Below the button are two links: "Return to authenticator list" and "Back to sign in".

After a selection is made, the user is required to enter an answer to the security question. When all information is entered, the user will click “Verify.”




3.3 Optional Mobile App Authentication

After the user verifies access using a phone or security question, they are offered a third way to authenticate: using a mobile app. If the user does not want to install and use a mobile app to authenticate, they can click “Set up later” to skip this step.




Set up security methods

 M12345


Security methods help protect your Okta account by ensuring only you have access.

Set up optional



Google Authenticator
Enter a temporary code generated from the Google Authenticator app.
Used for access

[Set up](#)



Okta Verify
Okta Verify is an authenticator app, installed on your phone, used to prove your identity
Used for access

[Set up](#)

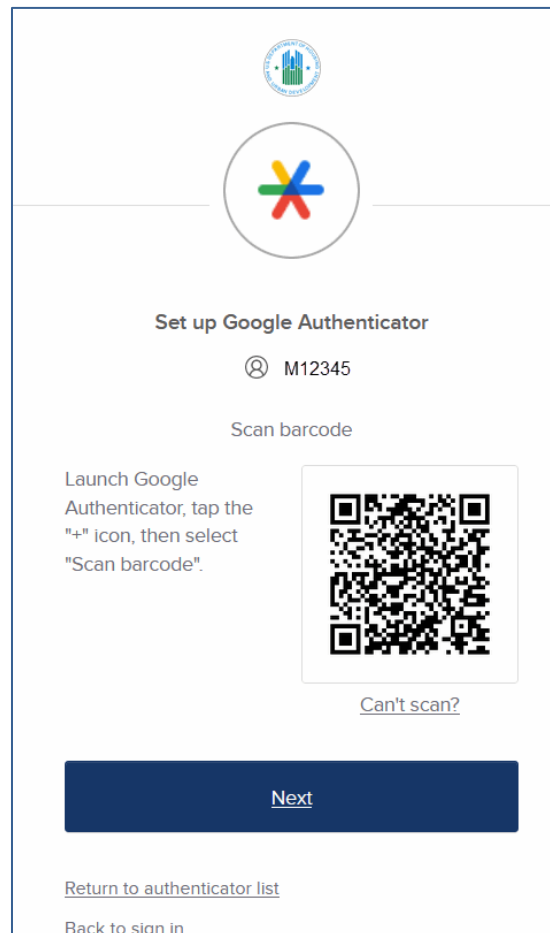
[Set up later](#)

[Back to sign in](#)



3.3.1 Google Authenticator

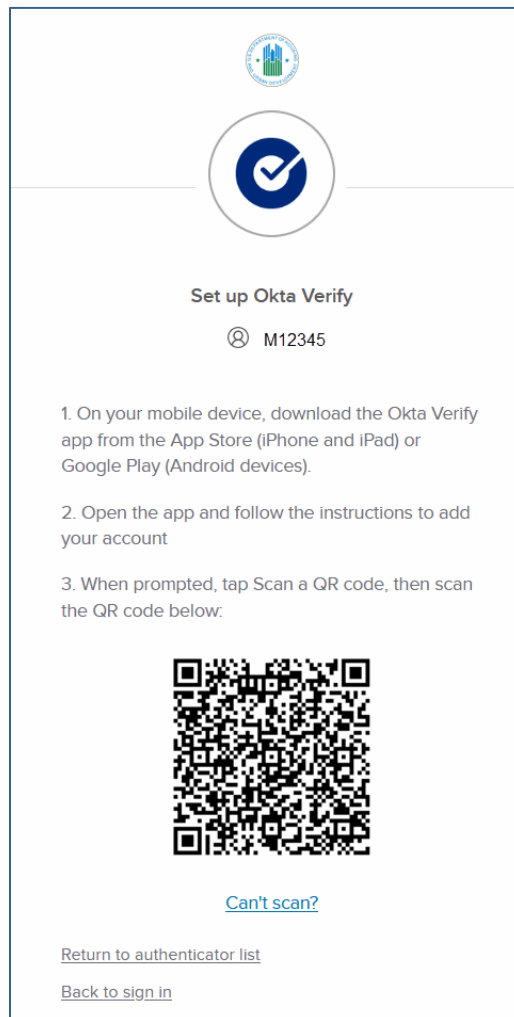
If the user opts to authenticate with Google Authenticator, they are prompted to scan a QR code, then enter a temporary code generated by the Google Authenticator mobile app. For future sign-ins, the user will not be required to authenticate using a phone or security question. Instead, they will be prompted to authenticate using Google Authenticator.





3.3.2 Okta Verify

If the user opts to authenticate with Okta Verify, they are prompted to scan a QR code, then enter a temporary code generated by the Okta Verify mobile app. For future sign-ins, the user will not be required to authenticate using a phone or security question. Instead, they will be prompted to authenticate using Okta Verify.



3.4 Special Instructions for Error Correction

If you chose to set these optional options up at a later time, you can set them up by clicking on the Okta Setup link on the FHAC sign-on page.

3.5 Caveats and Exceptions

Not applicable.



4. Using the Solution (Batch)

Not applicable.

4.1 <Solution Function Name>

Not applicable.

4.1.1 <Solution Sub-Function Name>

Not applicable.

4.2 Special Instructions for Error Correction

Not applicable.

4.3 Caveats and Exceptions

Not applicable.

4.4 Input Procedures and Expected Output

Not applicable.

5. Querying

Not applicable.

5.1 Query Capabilities

Not applicable.

5.2 Query Procedures

Not applicable.



6. Reporting

Not applicable.

6.1 Report Capabilities

Not applicable.

6.2 Report Procedures

Not applicable.



7. Getting Help

7.1 Solutions to Common Problems

Not applicable.

7.2 Getting More Help

Not applicable.

7.3 Helpdesk

Not applicable.



Appendix A: References

<Insert the name, version number, description, and physical location of any documents referenced in this document. Add rows to the table as necessary.>

Table 1 below summarizes the documents referenced in this document.

Document Name	Description	Location
<Document name and version number>	<Document description>	<URL to where document is located>

Table 1 - References



Appendix B: Key Terms

Table 2 below provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
<Insert Term>	<Provide definition of term and acronyms used in this document>

Table 2 - Key Terms