REFUGEE ARRIVALS DATA SYSTEM (RADS)

Office of Refugee Resettlement

LOGIN PROCEDURES

User Guide

March 2021

OFFICE OF REFUGEE RESETTLEMENT

An Office of the Administration for Children & Families

GENERAL DYNAMICS
Information Technology

Table of Contents

Introduction

In response to Release 3.4, we are pleased to provide a comprehensive guide outlining the procedures for logging into both RADS and RADS Tableau effective February 26, 2021.

RADS has implemented two important updates to login and navigational procedures:

1) Users with access to both RADS and RADS Tableau are now able to toggle between the two applications with a new single sign-on enhancement. This greatly enhances usability.

2) A new 2nd Factor Authentication (2FA) process using Google Authenticator is now in place to improve security.

Note: Users accessing RADS on the ACF network or VPN will have no change in their login procedures.

Section 1: New User Account Creation & Set-up

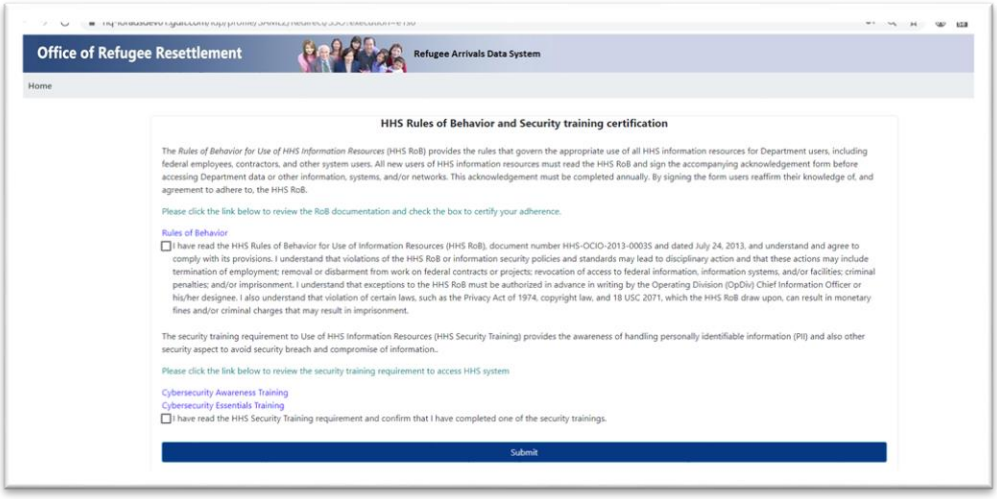
New user request forms are sent by an approved ACF employee to the RADS system administrator. If the request is approved, the system administrator will then complete your account creation. You are required to use your work email address for all accounts. Users should reach out to their supervisors and/or HHS/ACF/ORR contacts if a RADS account is needed.

Annual Required Acknowledgements & Trainings

All RADS and RADS Tableau users must have completed the following acknowledgements and trainings prior to accessing the system. These are annual requirements and are tracked from the date of RADS account creation.

- HHS Rules of Behavior
- HHS Required Cyber Security Training – this may be fulfilled by other cyber security training requirements; please check with your employer

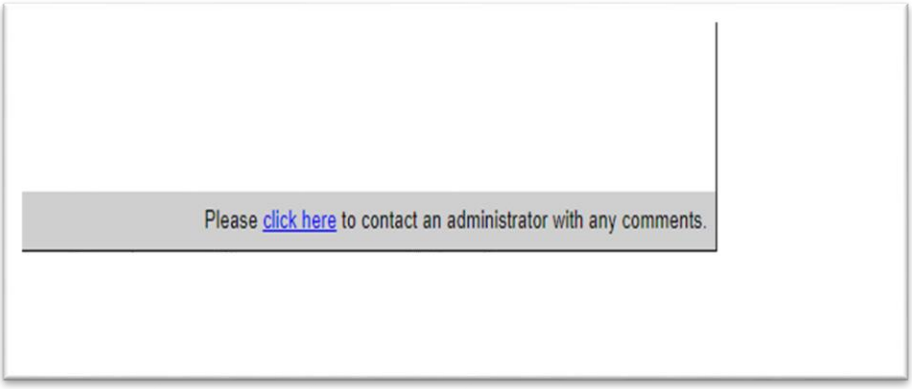
Links to these requirements are also available during the initial sign-on process. The acknowledgement page (shown below) will not show again until the next anniversary date of your account creation.



New User Account Set-up Information

Once your account has been created, you will receive two emails from rads@acf.hhs.gov. The first email will include your user ID and the second will have your temporary password.

NOTE: *The new account email access is only valid for 48 hours. If you do not activate the account, the invitation will expire. If this occurs, please contact the RADS system administrator. The contact information can be found at the bottom of any RADS screen and in the Troubleshooting section of this guide.*



Once you receive your account login credentials, you can begin your login process. This process is dependent on the network you use to access the system. RADS will prompt you through your login process. It is important to follow the instructions that appear on your screen and use this guide for supplemental support.

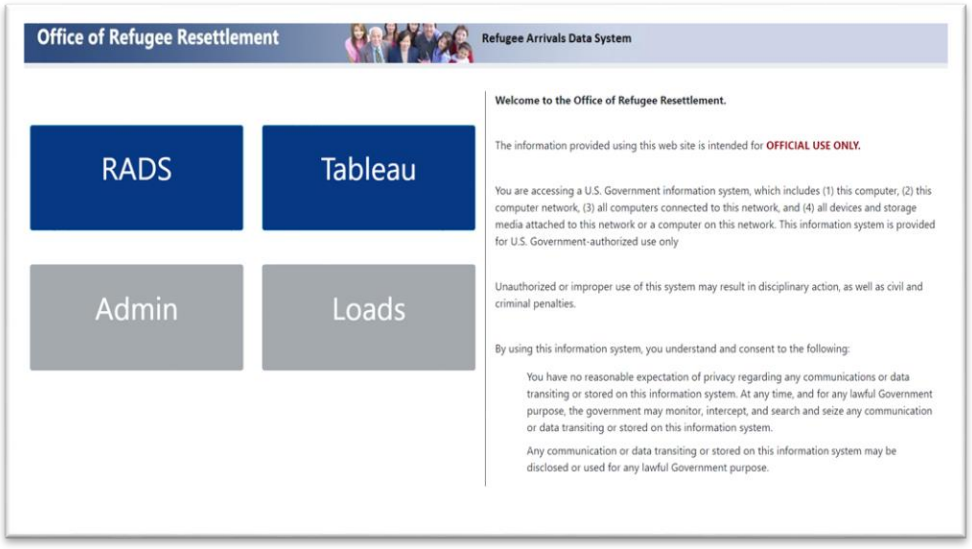
Section 2: Account Login & Initial Registration

The RADS and RADS Tableau systems are accessible on both *verified* and *unverified* networks, which is defined by the IP address you are using to access RADS. Simply, a *verified* network user is a person attempting to access RADS via a verified or approved IP address. An *unverified* network user is a person attempting to access RADS via an unverified/unknown IP address.

For RADS, the ONLY verified network users are ACF network users. These are users accessing RADS while on the ACF VPN. Therefore, if you are not on the ACF VPN, you are an *unverified* network user. All *unverified* network users must go through a verification process called 2nd Factor Authentication (2FA).

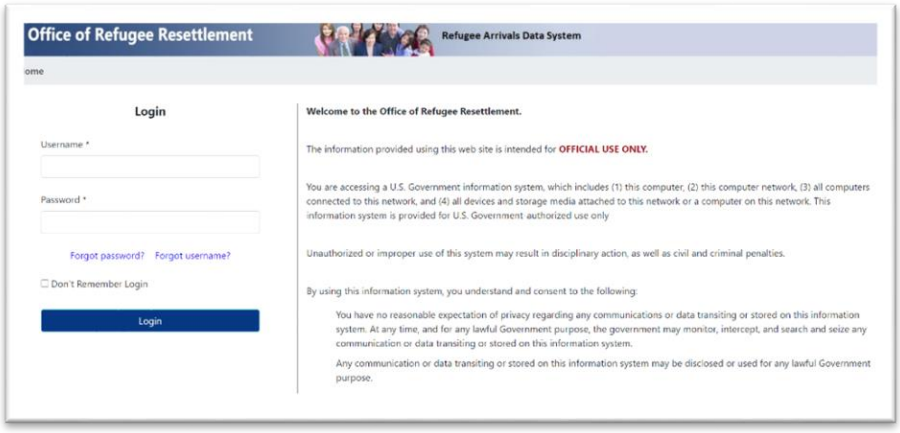
Accessing RADS

The system will guide your login regardless of your network. All users begin the login process on the same screen and with the same first few steps.



- ***Step 1:*** Go to the RADS landing page via this URL: www.rads.acf.hhs.gov
- ***Step 2:*** Select the blue RADS box to navigate to the RADS login screen
- ***Step 3:*** Enter your assigned user ID in the textbox provided
- ***Step 4*:** Enter your temporary or personal password in the textbox provided

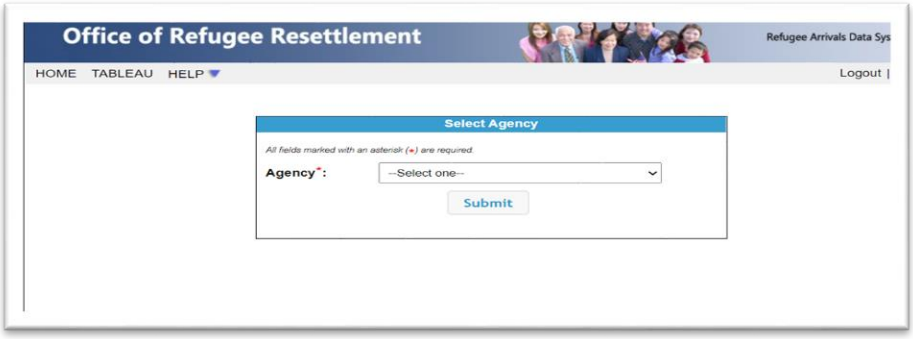
- ***Step 5:*** Select 'Login'

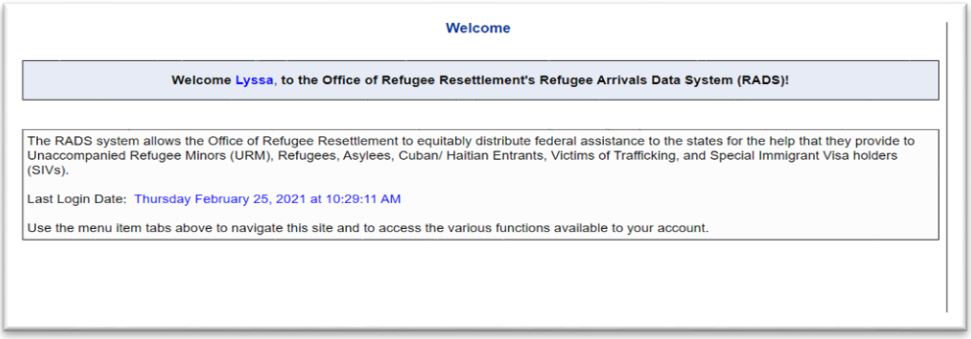


After clicking 'Login' on the screen pictured above, you will move to a new screen depending on the network access the RADS system detects.

RADS Login Process for Verified Network Users

If you have entered your user ID and password and are then taken to either of the screens below – the 'Select Agency' screen (users with numerous roles in RADS) or to the 'Welcome' screen (users with only one role in RADS) – you are on a VERIFIED network. You are <u>not</u> required to use the 2nd factor authentication. You are now ready to begin working in RADS.

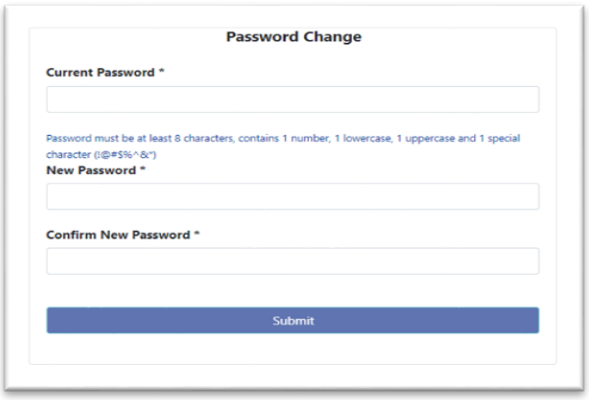




Verified Network NEW User Initial Login

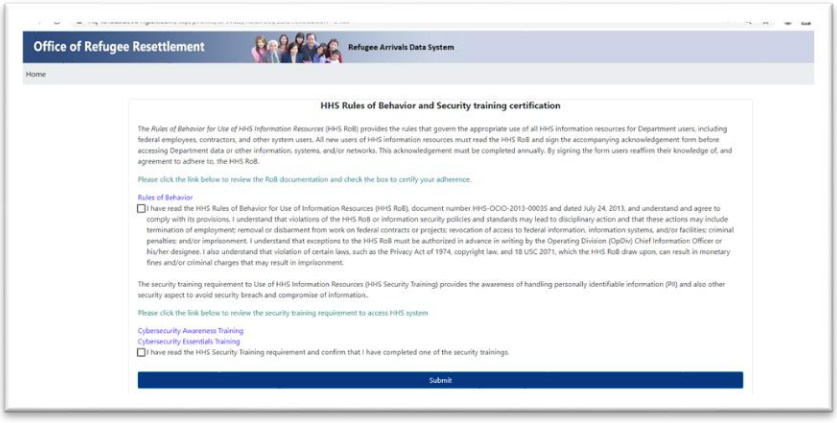
If you are on a verified network but a *new* user to RADS and/or Tableau, you will need to complete additional tasks for your first login.

First, you will be directed to change your password. Your new password must meet the requirements below. Once that is complete, select 'Submit'.

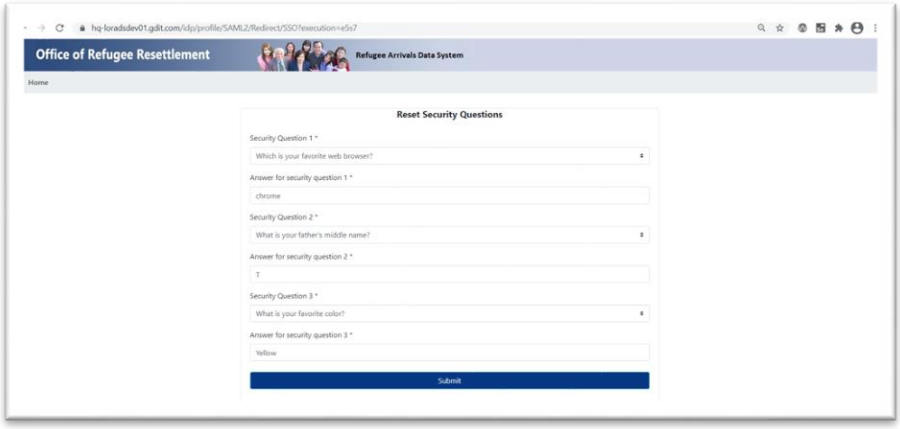


- ✓ At least 8 characters
- ✓ At least 1 number
- ✓ At least 1 lowercase letter
- ✓ At least 1 uppercase letter
- ✓ At least 1 special character (!@#$%^&*)

Next, you will acknowledge and certify the required HHS trainings and Rules of Behavior and select 'Submit'.



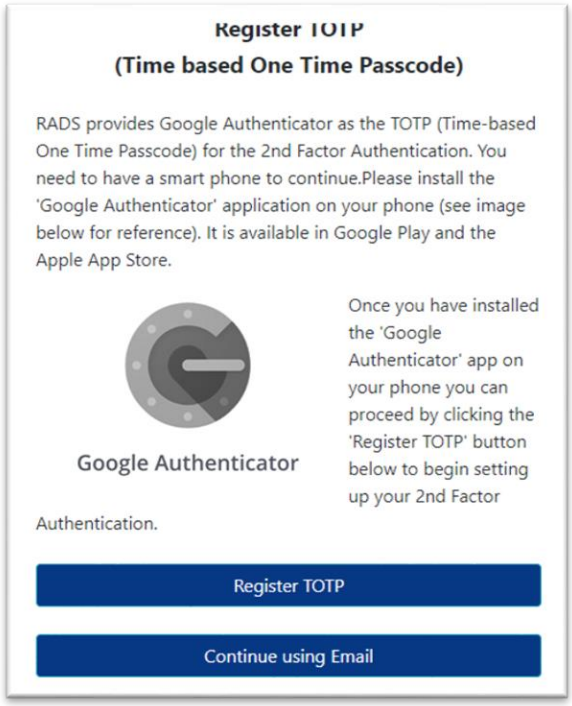
Then you will need to select, and answer, three security questions and click 'Submit'.



After completing these three steps, the new user account set-up is complete. You should be logged in to RADS and be taken to the welcome screen, as displayed in the previous page.

RADS Login Process for Unverified Network Users

If you have entered your user ID and password and are then taken to the 'Register TOTP' screen shown below– you are on an *UNVERIFIED* network. You are required to activate, or register, your 2nd Factor Authentication (2FA). It does not matter if you are a new or existing RADS user.



There are two options for your 2FA.

1. Register TOTP: This option allows you to use the Google Authenticator app on your smartphone to receive a Google token to login. This token will display as a 6 digit code on your phone that you will enter every time you login.

2. Continue using Email: This option allows you to use your email account to receive a PIN number to enter on the login screen. This must be done every time you login.

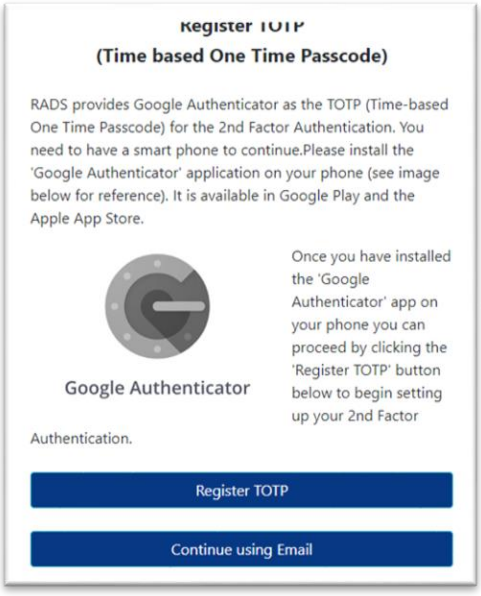
2FA Option 1: 'Register TOTP' or Using the Google Authenticator App

This following process is to register or sync the two (Google Authenticator app and RADS) by creating a RADS account (token) on the Google Authenticator app.

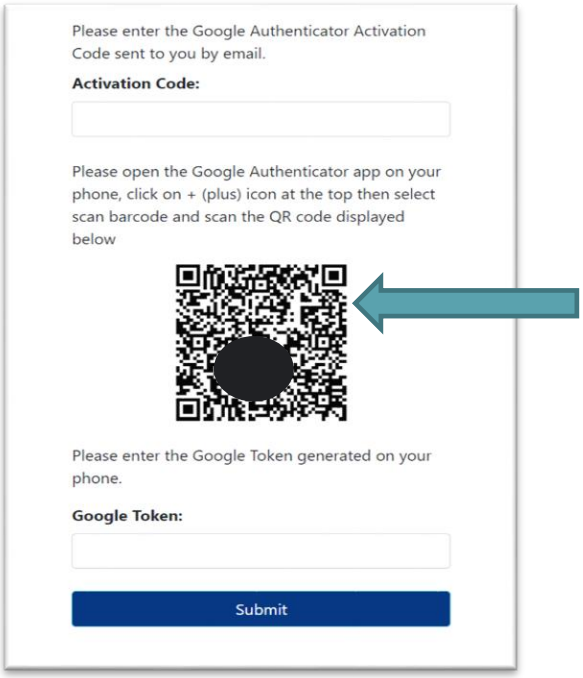
The first step is to download the app to your smartphone. This app is compatible with both iPhone and Android and can be found in both the Google Play and Apple app stores. Download the app *before* you attempt to sign on to the RADS system to save time.

After you have downloaded the app, follow these steps:

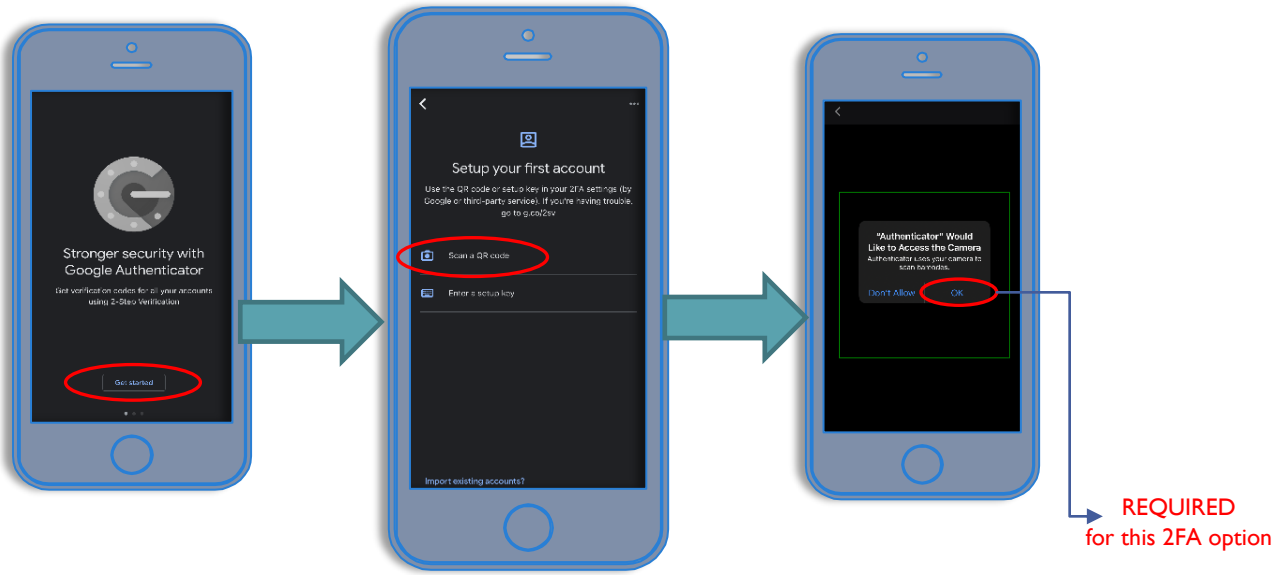
- ***Step 1:*** When you login to RADS on your computer using your user ID and temporary/personal password, all unverified users should see the 'Register TOTP' screen pictured below.
    - Select 'Register TOTP':



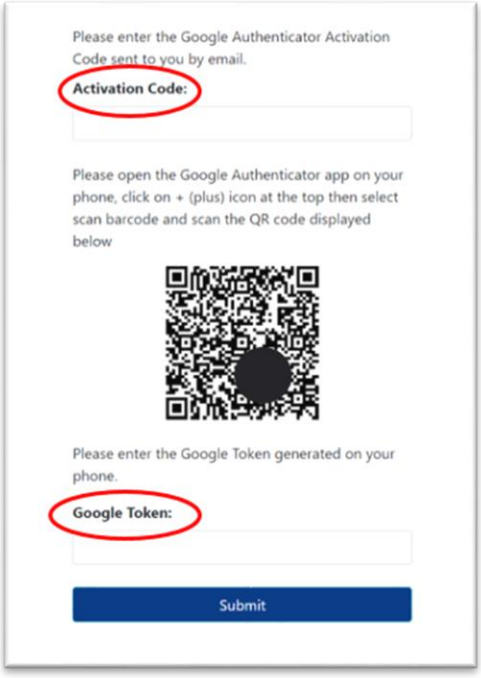
- ***Step 2:*** You should now see the 'Google Authenticator Registration' screen.
    - Here you will be provided with a QR code on your computer screen:



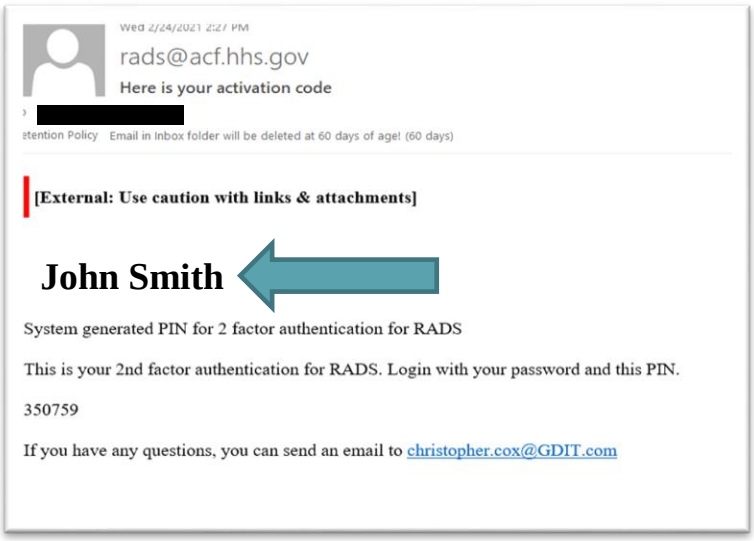
- ***Step 3:*** Now you will want to open the app on your smartphone.
    - Here you will follow the prompts on the screen in the app to scan the QR code on your computer:



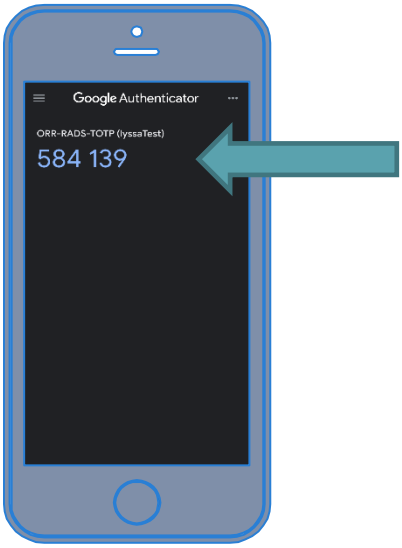
- ***Step 4:*** Snap a picture of the QR code via the app on your smartphone. You will then see a new box on your computer screen with prompts to enter two codes.



- ***Step 5:*** <u>Activation code</u>
  - You will receive an email to the email address associated with your RADS account. It will provide the initial PIN activation code. This code links your RADS/Tableau account to the Google Authenticator app and creates your unique account. **Enter this activation code in the box on the screen.**



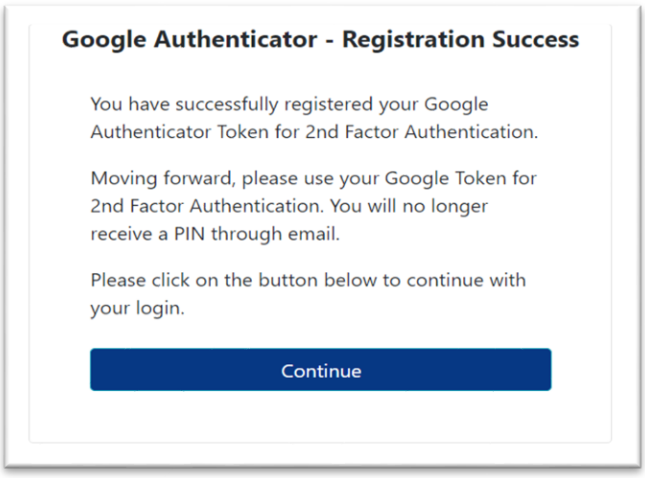
- ***Step 6:*** <u>Google Token Code (in the app)</u>
    - Once you scan the QR code, your smartphone will display your Google token number to enter in the box on the screen.



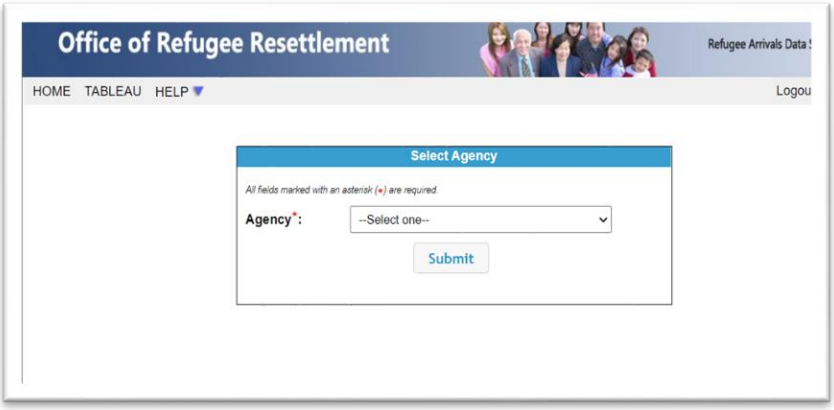
    - ***NOTE:*** *The Google token will always be a six-digit code in your app. However, be aware that this token changes every 25 second for* security purposes. The code will begin to turn red when it is about to expire so you need to click 'Submit' before it updates to a new code or wait until the new code appears.

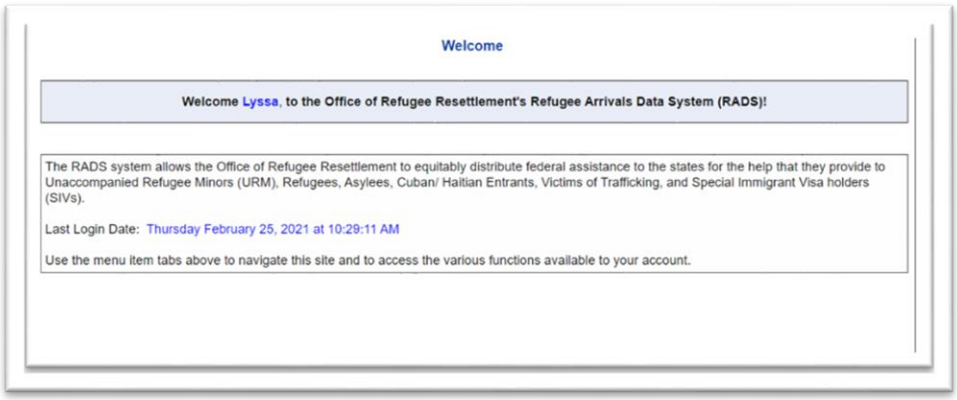
      **If you enter a code incorrectly or enter an expired code, you will get an error message and will need to enter the current code displayed in the app.

- ***Step 7:*** Once both codes are entered, click 'Submit.' That's it! You are registered.



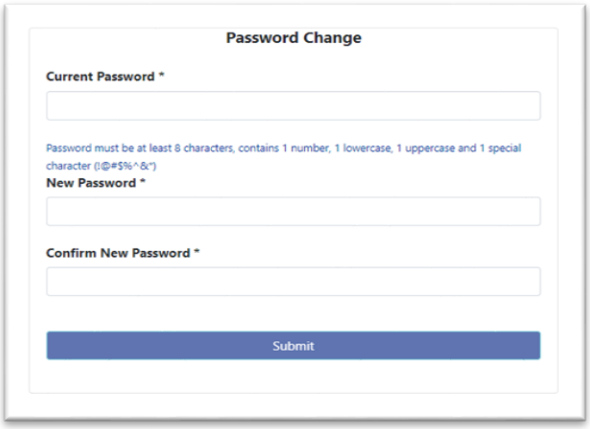
- ***Step 8:*** Click 'Continue' on the 'Registration Successful' screen to begin working in RADS and you will be brought to either the 'Select Agency Screen' or the 'RADS Welcome Screen'.





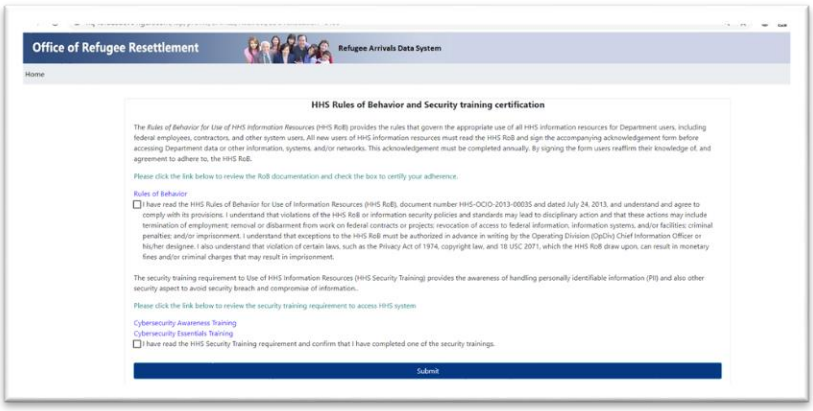
Unverified Network NEW User Initial Login

Once your login is complete, if you are new to the RADS/Tableau systems, you will need to complete a few additional steps to establish the account. First, you will be directed to change your password. Your new password must meet the requirements below. Once that is complete, select 'Submit'.

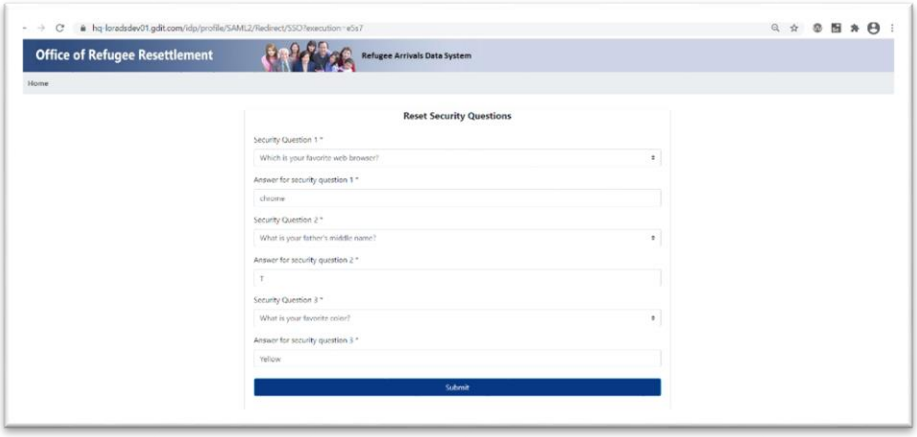


- ✓ At least 8 characters
- ✓ At least 1 number
- ✓ At least 1 lowercase letter
- ✓ At least 1 uppercase letter
- ✓ At least 1 special character (!@#$%^&*)

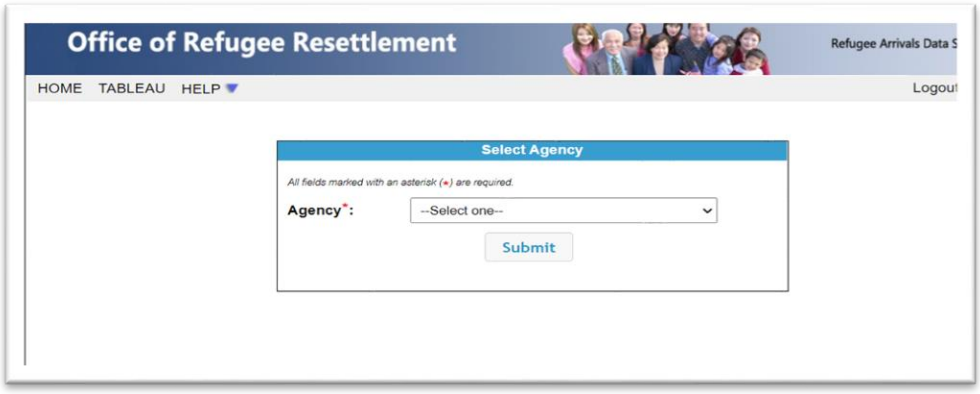
Next, you will acknowledge and certify the required HHS trainings and Rules of Behavior and select 'Submit'.

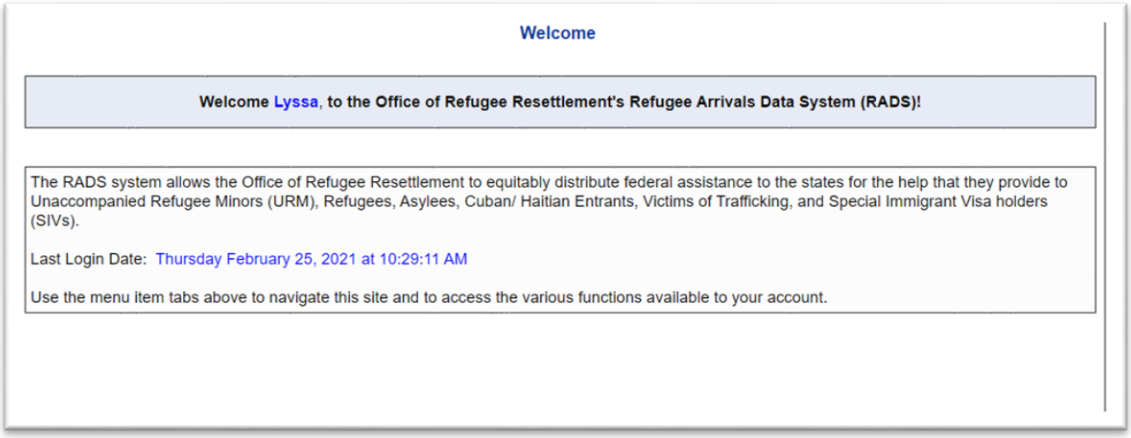


Then you will need to select, and answer, your three security questions and click 'Submit'.



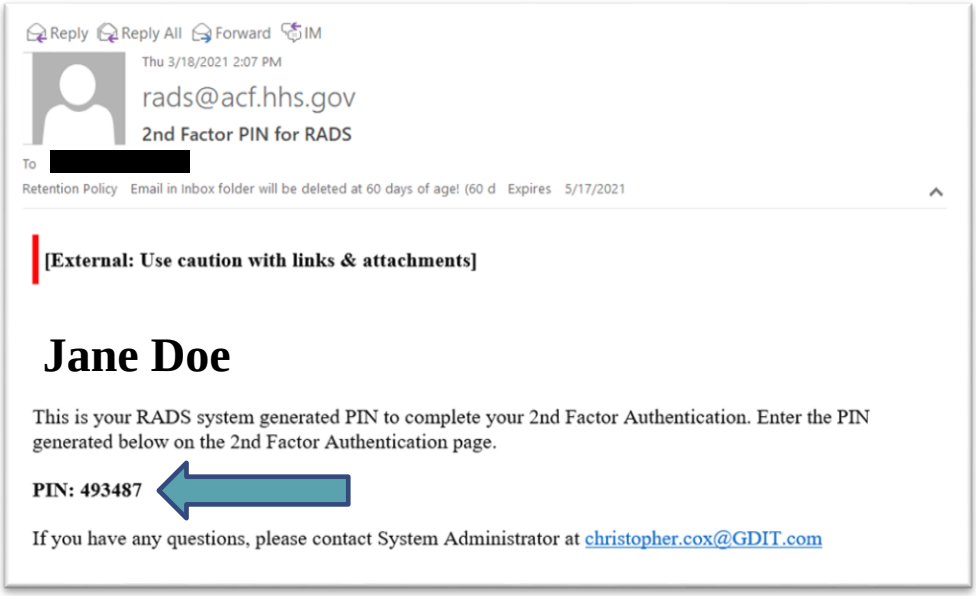
After completing these three additional tasks the new user account set-up is complete. Whether you are a new or existing user – at this point all unverified network users should be Registered with Google Authenticator and logged into RADS. You should see one of these two screens:





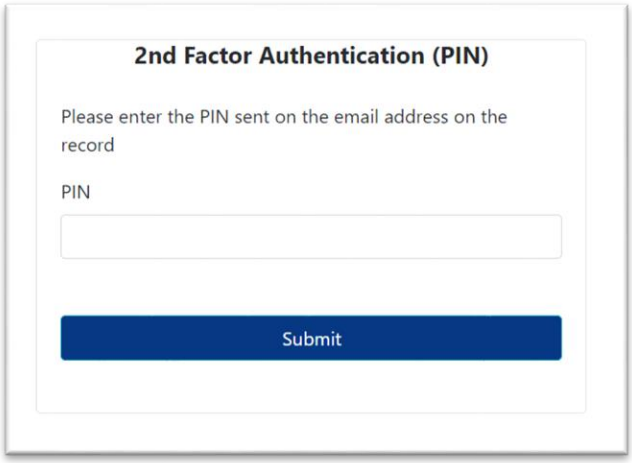
2FA Option 2: 'Continue using Email' or 2FA Pin via Email

If you select the 'Continue using Email' option – after entering/submitting your user ID and temporary/personal password on the login screen – you will need to request a RADS generated PIN. Once you have selected the email notification option, RADS will send you a PIN via email.



NOTE: *sometimes PIN emails are sent to junk or spam folders or blocked by your company's IT department. If you do not receive the PIN, you will want to check those two places first. If neither is the case, you should reach out to the RADS system administrators by clicking the link at the bottom of any RADS screen.*

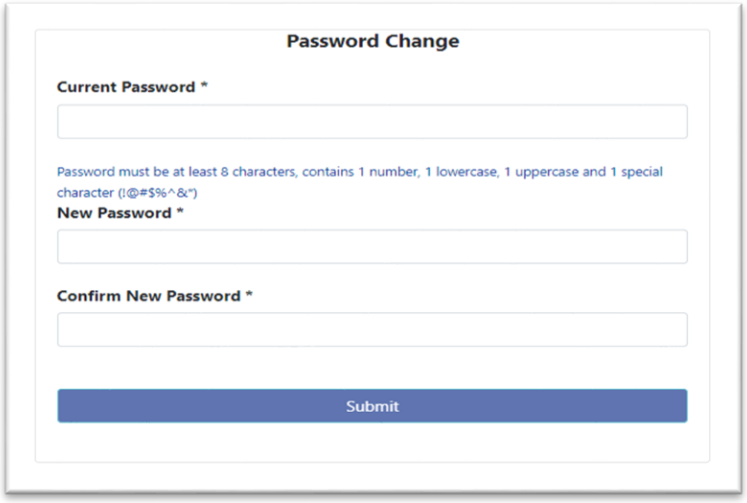
Once you have received the email, you will enter the PIN from the email into the provided textbox in RADS. Then Click 'Submit'.



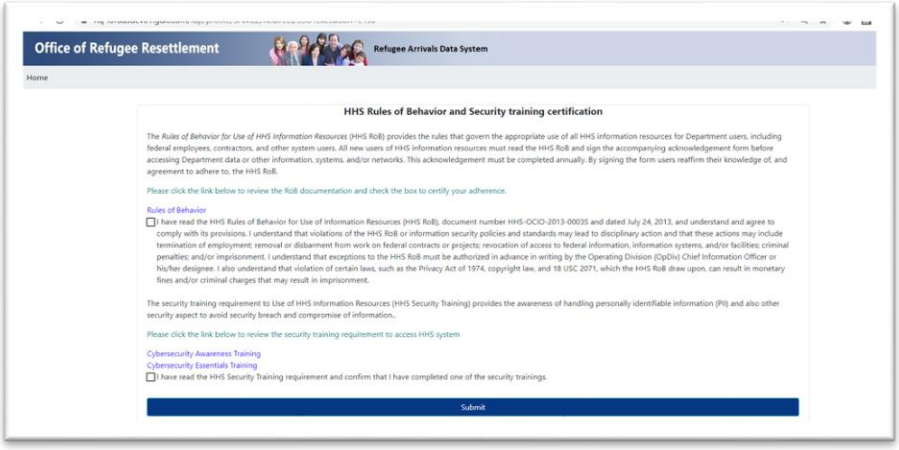
- Incorrect PIN: If you are receiving the below error after entering your PIN, double check the PIN you are entering or copying/pasting into the textbox. If the PIN entered appears to be correct, you will want to then try another PIN. In order to get a new PIN, you will need to begin the process again by logging in and selecting the '2FA PIN via email'
- Correct PIN: Once you enter the correct PIN, you will be taken to the next screen. If you are a user with numerous roles in the RADS system, you will see the 'Select Agency' screen. If you have only one role in RADS, who will see the 'Welcome' screen.

Unverified Network NEW User Initial Login

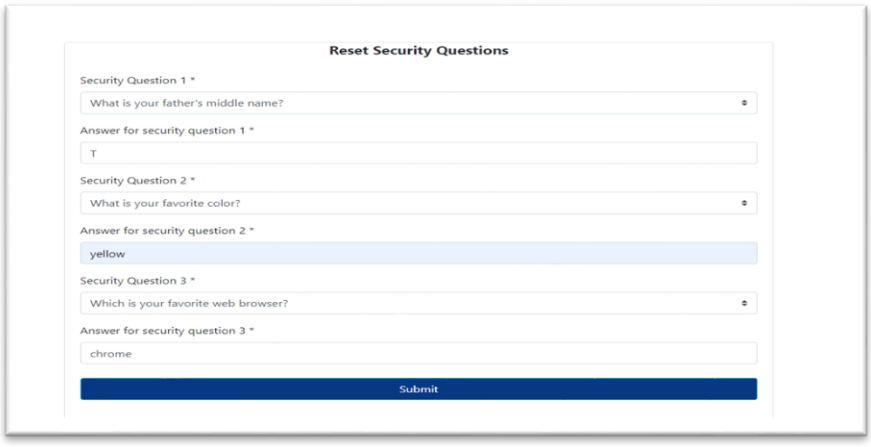
If you are a new user or need to reset/reinstate your account, you will need to change your password. Anytime you receive a temporary password from RADS your first prompt when you login to RADS will be to change it.



If you are new user, you will also be prompted to acknowledge and certify the required HHS trainings and Rules of Behavior and select 'Submit'.



Then you will need to select, and answer, three security questions and select ‘Submit’.

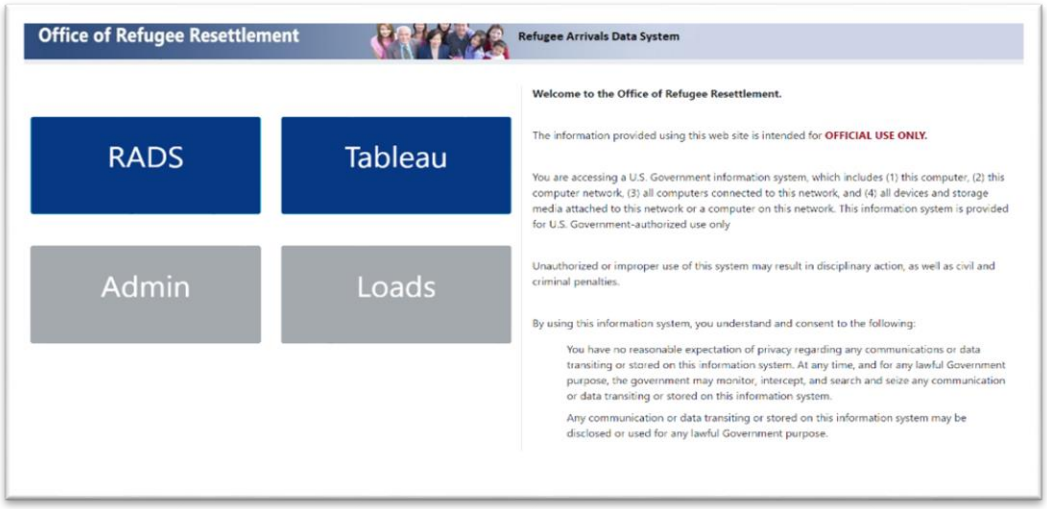


Section 3: Ongoing Account Login with 2FA

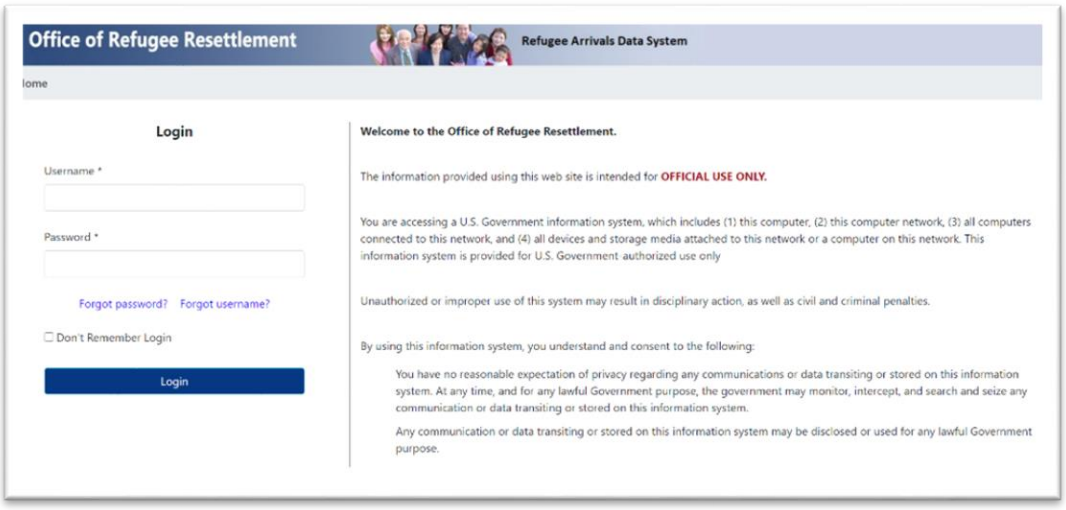
Once you have established your 2nd Factor Authentication, you will now use it to login to RADS every time.

Note: Verified users (ACF network) have no change in their login procedures. They do not need to establish their 2nd factor.

- ***Step 1:*** Go to the RADS landing page via this URL: www.rads.acf.hhs.gov



- ***Step 2:*** Select the blue RADS box to navigate to the RADS login screen



- ***Step 3:*** *Enter your assigned user ID in the textbox provided*
- ***Step 4*****:** Enter your personal password in the textbox provided
- ***Step 5:*** Select 'Login'
- ***Step 6:*** Select one of the three options for your 2nd Factor Authentication

Option 1	Option 2	Option 3
Submit Google Token	**Lost Token; Re-register Google Token**	**Send 2FA PIN in Email**
Continue with the use of the Google token you have already registered in your app. For this option, all you will need to do on this screen is enter that 6 digit token that appears in your Google Authenticator app and select 'Submit'. *Note: This is the preferred method for 2FA.*	If you have for some reason lost your previously registered token or gotten a new phone you will need to re-register your token. Here you will select 'Lost Token; Re-register Google Token' and continue on with the prompts following the directions listed out in section.	This method is also in section 2. Here you will select 'Send 2FA PIN in Email' and follow the steps listed in the previous section.
NOTICE: *Before re-registering any new tokens you should be sure and delete any ORR-RADS token accounts listed in your phone app. RADS will only except the most recent token created. There is also an ability to label the tokens in the app if you have numerous tokens for other work related accounts.*		

Section 4: RADS Tableau Navigation

For users with access to both RADS and RADS Tableau, we have added a single-sign-on enhancement. This new feature allows users of both systems to toggle between the two systems with ease. You no longer have to login to two separate systems to view your data because the single-sign-on feature is just that… one sign-on.

We have also added Tableau to your top bar menu once you have logged in. You can use the tabs at the top of your screen to jump from your work in RADS to view Tableau dashboards with minimal clicks.

Section 5: Signing out of RADS with Single Sign-on

It is critical to properly sign out of ***both*** RADS ***and*** Tableau. Logging out of RADS will only log you out of RADS. Logging out of RADS Tableau will only log you out of RADS Tableau.

To log out of both RADS and RADS Tableau you **must** CLOSE your browser. So if you are in Google Chrome you will need to completely close your window to log out of both systems. Until a user closes the browser they remain authenticated.