# REFUGEE ARRIVALS DATA SYSTEM

## RADS RELEASE 3.4 LOGIN TRAINING

## FREQUENTLY ASKED QUESTIONS

### Q: What is the RADS URL? Did it change in this release?

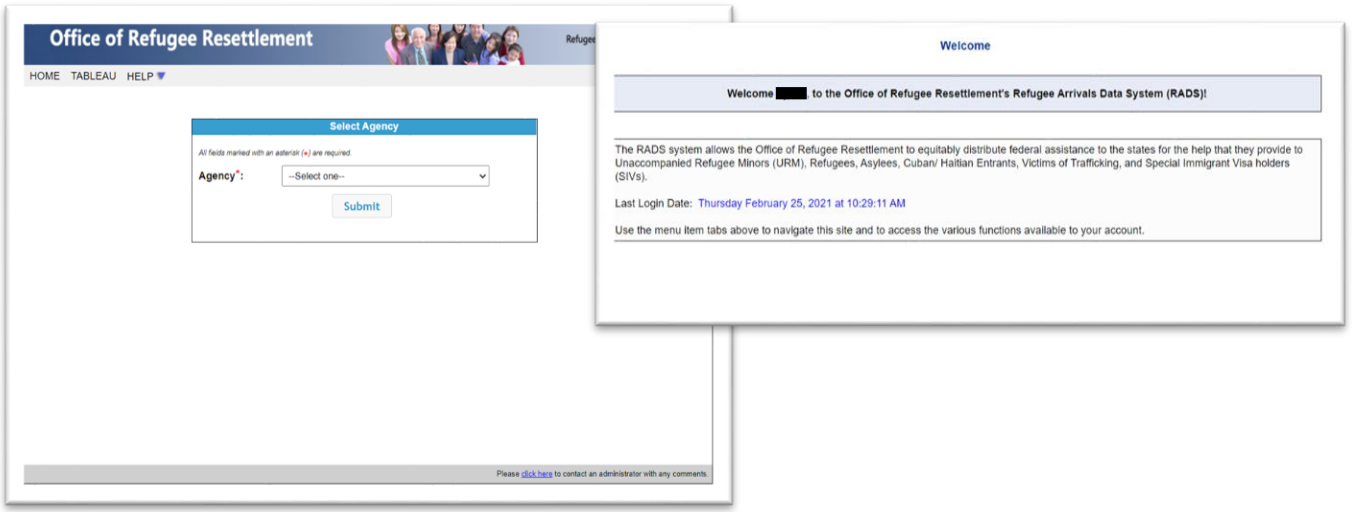
**A:** No, the RADS URL did not change in Release 3.4.

**RADS URL**: https://rads.acf.hhs.gov/rads/

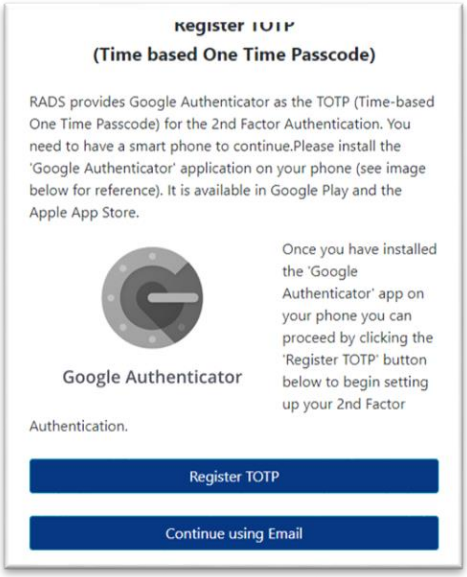
### Q: Am I a 'Verified' or 'Unverified' user?

**A:** Verified users, or ACF Network users, all access RADS from the verified ACF network. This network has an approved and certified IP address in RADS and does NOT require the user to complete a 2nd factor to login. Unverified users are everyone else- people who are not on the ACF network. Unverified users are required to complete a 2nd factor authentication (2FA) process. You will know what type of user you are by the prompts you receive after you log in to the system.

- If you see this screen you are a VERIFIED user and NO 2FA is needed:



- If you see this screen you are an UNVERIFIED user and must complete your 2FA process:




## Q: Do I have a choice between Register TOTP and Continue using Email?

**A:** Yes, there are the two options for 2FA. You must select one. The first option is: Register TOTP, which will take you through the steps to use Google Authenticator on your phone. This is the preferred option. The second option is to select Continue using Email, which follows the process of receiving a RADS generated PIN via email that has been existing functionality in RADS for a while.

## Q: What App do we need to download for the 2nd Factor Google Authenticator Token?

**A:** You will need to download the 'Google Authenticator' app on your smartphone. You can get this app for FREE on both the Google Play and Apple app stores. See the photo to the left, of the grey 'G' icon for reference.

*Note:* If you do not have the ability to download the app on your smartphone you should utilize the other 2nd factor authentication option of receiving a PIN via email.

## Q: I already have the Google Authenticator app on my smartphone. Can I use it?

**A:** Yes. You will just need to add the ORR-RADS account to the app to get the correct token code. Once you create your ORR-RADS account, it will show up on the Google Authenticator app with your other accounts as ORR-RADS-TOTP.

## Q: How do I register the Google Authenticator Token?

**A:** There is a detailed process of how to register your TOTP/ Google Token in Section Two of our User Guide. This should be a one-time process for most users. After the initial registration, users will then only need to open the Google Authenticator app on their smartphones to retrieve their Google token. Here is an overview of the registration process:

- ***Step 1:*** Download the App on your smartphone.
- ***Step 2:*** Login to RADS on your computer. Begin on the navigational landing page and select RADS. Then enter your login credentials on the login screen and select submit.
- ***Step 3:*** UNVERFIED users will need to select Register TOTP.
- ***Step 4****:* Once you have clicked, 'Register TOTP', you will then be given the Google Authenticator Registration prompt. There will be a QR code on the screen. Now you need to open the Google Authenticator app on your phone.
- ***Step 5:*** In the app, select 'Get Started', then select 'Scan QR Code'. Enable the app to access your camera. Then, on your computer, scan the QR code with your phone camera.
- ***Step 6:*** Once scanned, you will be sent TWO CODES.
    1. Activation code – sent to the email address associated with your RADS account
    2. Google Token – appears on the smartphone app as a 6 digit code (changing every 25 seconds)
- ***Step 7:*** Enter the two codes in their respective textboxes on the computer screen and select 'Submit'.

**You are registered successfully!**

Now, to login at the next visit, all you need is the Google token on your smartphone!

## Q: What email will the codes be sent to?

**A:** All emails will be sent to the email address that is associated with your RADS account.

**Q: How long does it take to get the verification emails?**

**A:** Emails are usually received within 5-10 minutes. However, due to a number of different factors, it can fluctuate.

**Q: If I am a verified user, can I still access RADS on an unverified network and use the 2FA?**

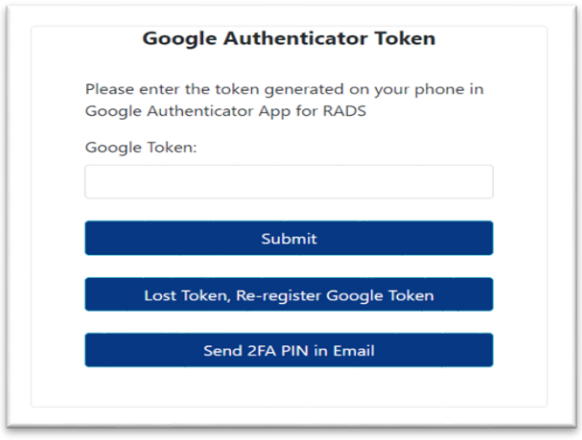
**A:** Yes, if you are logging in to the system off the ACF network, you will be considered an unverified user and will need to follow the 2FA process.

**Q: What do I do if I am not receiving the emails?**

**A:** The first thing you want to do if you do not receive the RADS emails is check your spam or junk folders. If it does not appear there, then you may want to check with your IT department. Some IT departments block RADS emails when they are not used to seeing them. If you have done this, and you still have not received the email, please reach out to the RADS system administrators via the link on the bottom of all RADS screens.

**Q: What if I lost my token/ got a new phone and need to re-register?**

**A:** If you need to re-register your Google Authenticator token you will select, 'Lost Token, Re-register Google Token' here and follow the steps in the previous question to register your TOTP/ Google token.




Once you have completed the initial registration, UNVERIFIED users will always be given this prompt after logging in with their username and password on the login screen. This is where users have the option to choose how they want to complete their 2nd factor. The three options are 1. To continue using their already registered google token. 2. Re-register their token. 3. Use the 2FA PIN generated by RADS and sent via email.

Users who have lost their token or need to re-register will need to select option 2 on the screen and repeat the process of registering their TOTP/ Google token. They will receive a new activation code and Google token.

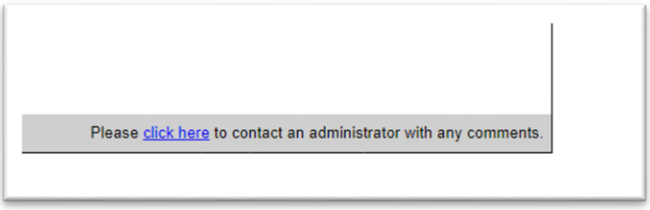
*Note:* Be sure to delete other ORR-RADS tokens in your Google Authenticator app. The RADS system will only accept the most recent token- therefore all other tokens will only cause confusion.

### Q: Can we access RADS via the earlier authentication method?

**A:** Yes, the RADS generated 2FA pin is still an option at this time. We are planning to move away from this functionality and are urging users to use the Google Authenticator Token as the preferred method moving forward.

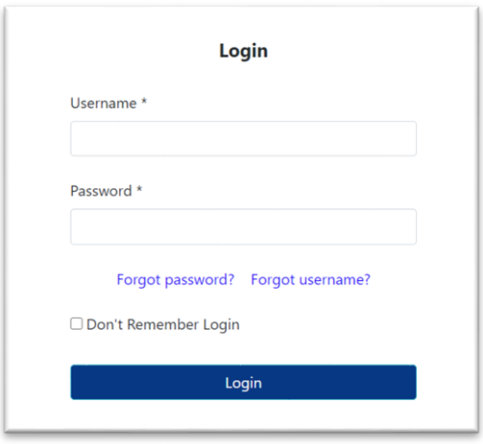
### Q: How do I request an account reset?

**A:** You can request an account reset by contacting the RADS system administrators via the link at the bottom of all RADS screens.




### Q: What if I forgot my Username or password?

**A:** If you have forgotten your username/ password you can utilize the links on the login screen.




Clicking 'Forgot Username' will prompt you to enter your email address associated with your RADS account in order to send you your username via email. Clicking 'Forgot Password' will prompt you to enter your username and send an email to your email address that is associated with your RADS account.