

LOGIN PROCEDURES

User Guide

August 2022

Contents

.....	1
Section 1: New User Account Creation & Set-up.....	3
<i>Annual Required Acknowledgements & Trainings</i>	3
Section 2: Account Login & Initial Registration	5
<i>2FA Option 1: 'Register TOTP' or Using the Google Authenticator App</i>	8
Section 3: Ongoing Account Login with 2FA.....	18
Section 4: RADS Tableau Navigation.....	19
Section 5: Signing out of RADS with Single Sign-on.....	19

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.

HHS Rules of Behavior and Security training certification

The *The Rules of Behavior for Use of HHS Information Resources*(HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. All new users of HHS information resources must read the HHS RoB and sign, by checking, the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB.

Please click the link below to review the RoB documentation and check the box to certify your adherence.

[Rules of Behavior](#)

☐ I have read the HHS Rules of Behavior for Use of Information Resources (HHS RoB), document number HHS-OCIO-2018-0004 and dated July 25, 2018 . I understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the Operating Division (OpDiv) Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

The security training requirement to Use of HHS Information Resources (HHS Security Training) provides the awareness of handling personally identifiable information (PII) and also other security aspect to avoid security breach and compromise of information. This training must be done yearly. The training can be done through your company or government agencies mandatory yearly training or by taking the two security training classes below.

Please click the link below to review the security training requirement to access HHS system

[Cybersecurity Awareness Training](#)
[Cybersecurity Essentials Training](#)

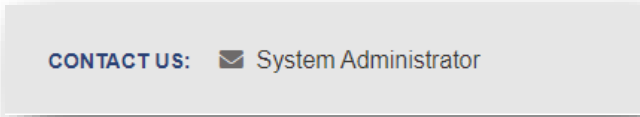
☐ I have read the HHS Security Training requirement and confirm that I have completed either (a) the two classes linked above or (b) a separate training through my employer's yearly requirement.

Submit

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.*



CONTACT US: ✉ System Administrator

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.

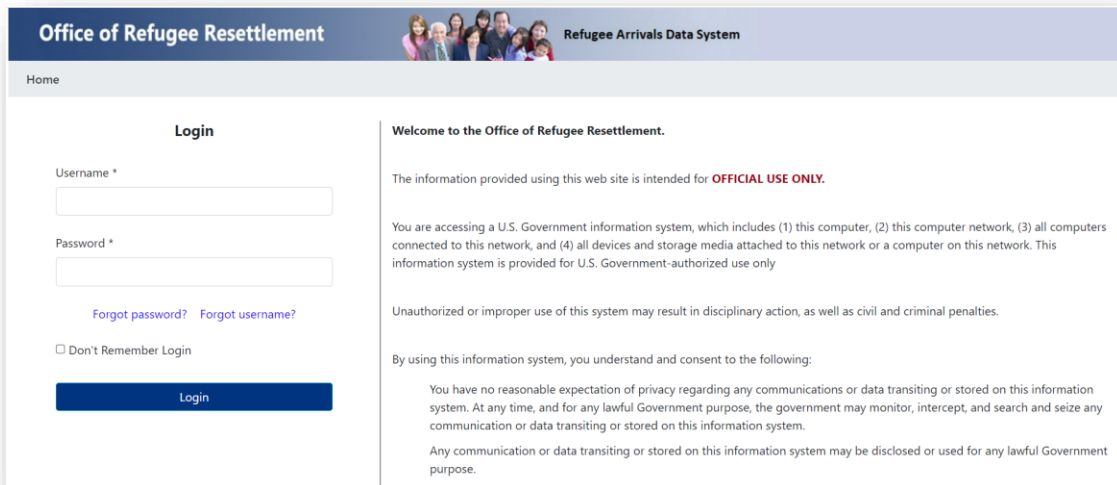
Section 2: Account Login & Initial Registration

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 put, 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.



The screenshot shows the login interface for the Refugee Arrivals Data System (RADS). The header includes the 'Office of Refugee Resettlement' logo and a group photo of diverse people. The main content area is divided into two columns. The left column, titled 'Login', contains fields for 'Username *' and 'Password *', with links for 'Forgot password?' and 'Forgot username?'. Below these is a checkbox for 'Don't Remember Login' and a blue 'Login' button. The right column contains a welcome message, a disclaimer about official use only, and a consent statement regarding privacy and data handling.

Office of Refugee Resettlement

Refugee Arrivals Data System

Home

Login

Username *

Password *

[Forgot password?](#) [Forgot username?](#)

☐ Don't Remember Login

Login

Welcome to the Office of Refugee Resettlement.

The information provided using this web site is intended for **OFFICIAL USE ONLY**.

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

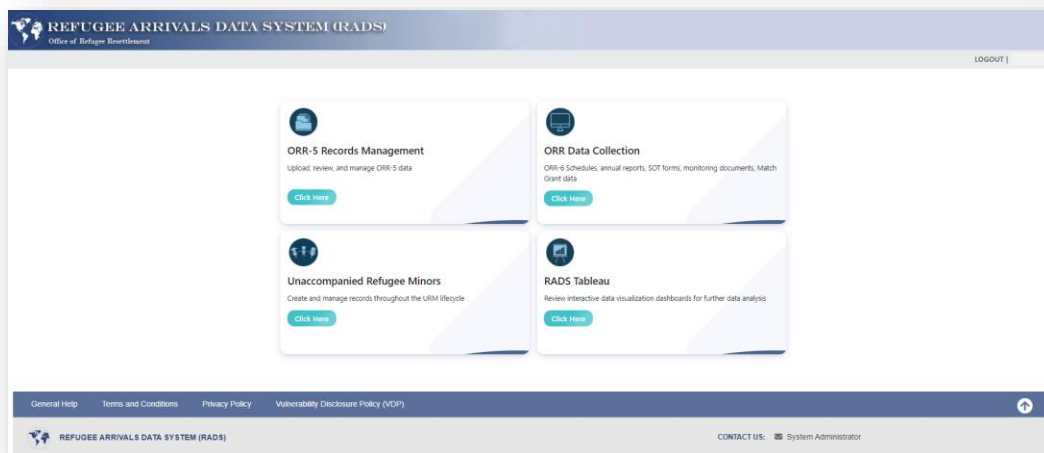
Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

- **Step 1:** Go to the RADS landing page via this URL: <https://rads.acf.hhs.gov/rads/>
- **Step 2:** Enter your assigned user ID in the textbox provided
- **Step 3:** Enter your temporary or personal password in the textbox provided
- **Step 4:** 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 this navigational landing page (pictured below) – you are on a VERIFIED network. You are not 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'.

Password Change

Current Password *

Password must be at least 8 characters, contains 1 number, 1 lowercase, 1 uppercase and 1 special character (!@#%\$^&*)

New Password *

Confirm New Password *

- ✓ 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'.

A screenshot of a web form titled "Security Questions". The form contains three identical sections for security questions. Each section consists of a dropdown menu labeled "Security Question 1 *" (or 2, or 3) with the text "-- Please select --" and a small downward arrow. Below each dropdown is a text input field labeled "Answer for security question 1 *" (or 2, or 3). At the bottom of the form is a dark blue button with the word "Submit" in white text.

Security Questions

Security Question 1 *

-- Please select --

Answer for security question 1 *

Security Question 2 *

-- Please select --

Answer for security question 2 *

Security Question 3 *

-- Please select --

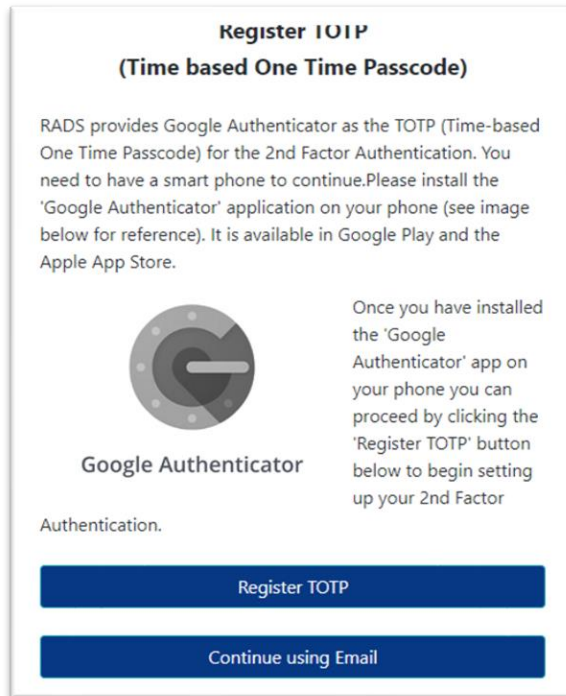
Answer for security question 3 *

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

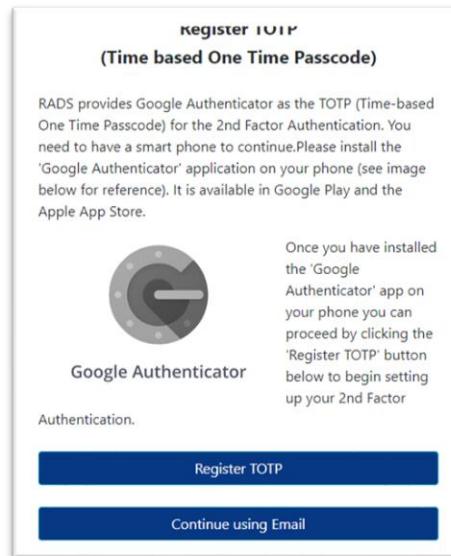


This following process is to register or sync the two (Google Authenticator app and RADS) by creating a RADS account (token) on the Google Authenticator app.

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.

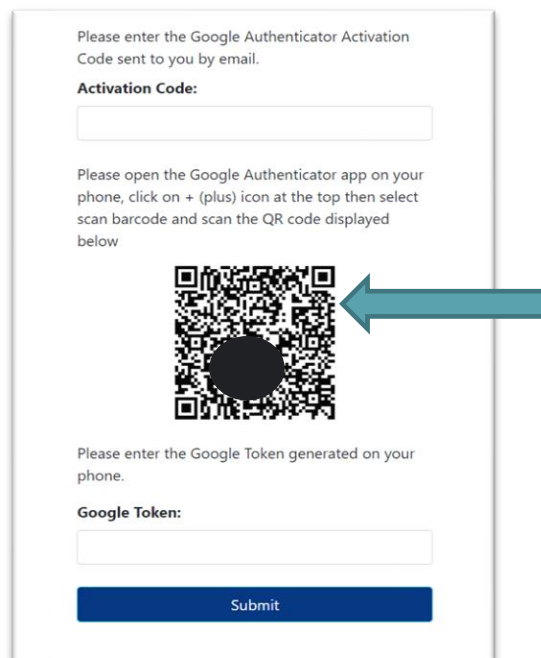
After you have downloaded the app, follow these steps:

- **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':



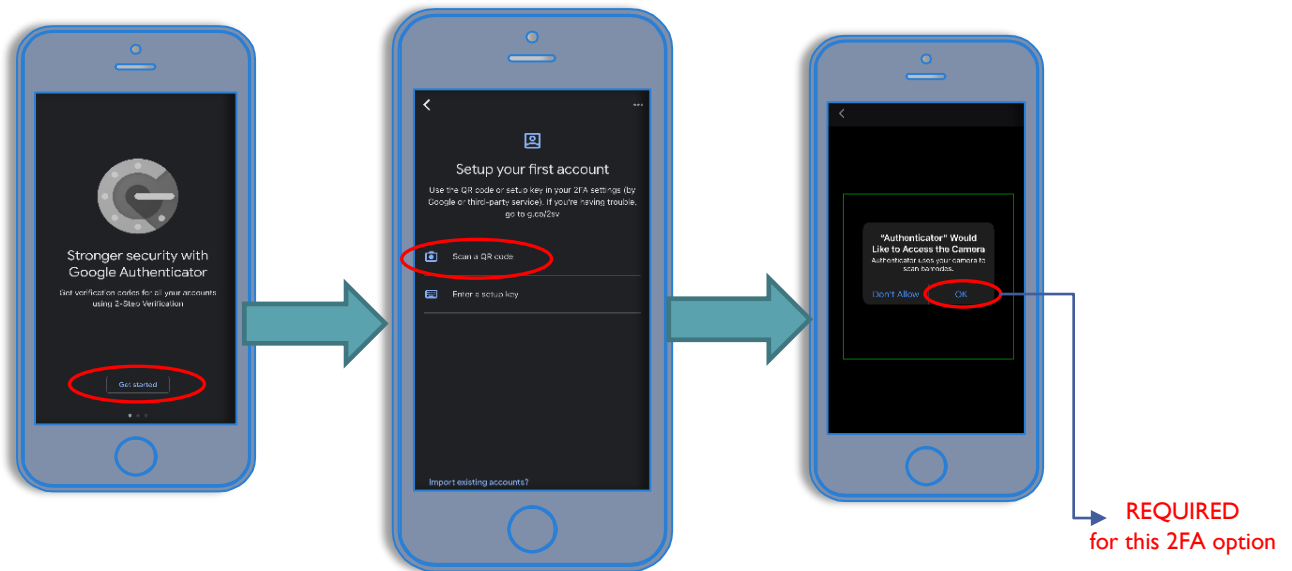
The screen is titled "register TOTP (Time based One Time Passcode)". It contains a paragraph explaining that RADS provides Google Authenticator as the TOTP for 2nd Factor Authentication and that a smart phone is needed. Below this is a circular icon for Google Authenticator. To the right of the icon, text instructs the user to install the app and click the 'Register TOTP' button. At the bottom, there are two blue buttons: "Register TOTP" and "Continue using Email".

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



The screen is titled "Please enter the Google Authenticator Activation Code sent to you by email." It has a text input field for the "Activation Code:". Below this, it says "Please open the Google Authenticator app on your phone, click on + (plus) icon at the top then select scan barcode and scan the QR code displayed below". In the center is a QR code with a large black circle in the middle. A blue arrow points from the right towards the QR code. Below the QR code, it says "Please enter the Google Token generated on your phone." and has a text input field for the "Google Token:". At the bottom is a blue "Submit" button.

- **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:

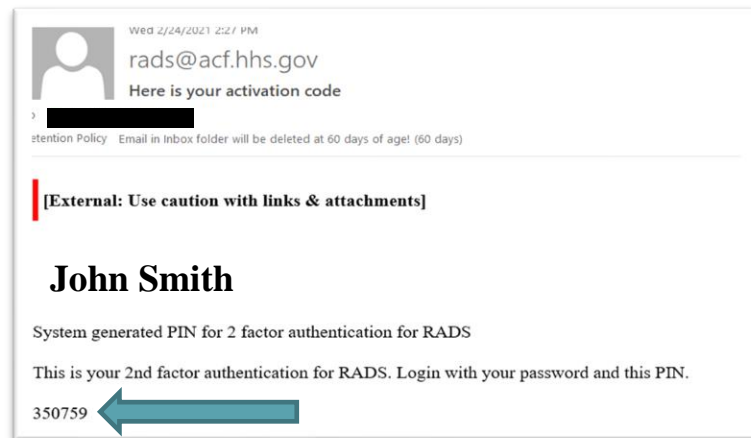


- **Step 4:** Snap a picture of the QR code via the app on your smartphone. You will then see a new box on your computer screen with prompts to enter two codes.

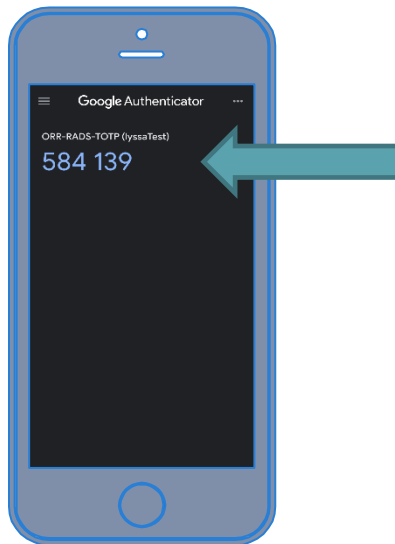
The image shows a computer screen with a form for activating Google Authenticator. The form contains the following elements:

- A heading: "Please enter the Google Authenticator Activation Code sent to you by email."
- A label "Activation Code:" with a red circle around it, followed by an empty input field.
- Instructions: "Please open the Google Authenticator app on your phone, click on + (plus) icon at the top then select scan barcode and scan the QR code displayed below"
- A QR code in the center of the form.
- Instructions: "Please enter the Google Token generated on your phone."
- A label "Google Token:" with a red circle around it, followed by an empty input field.
- A blue "Submit" button at the bottom.

- **Step 5: Activation code**
 - 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.**



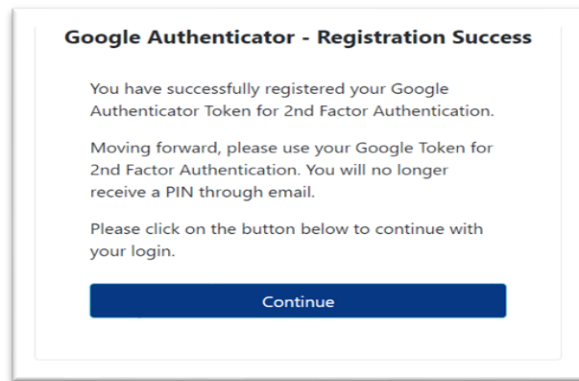
- **Step 6: Google Token Code (in the app)**
 - Once you scan the QR code, your smartphone will display your Google token number to enter in the box on the screen.



- **NOTE:** The Google token will always be a six-digit code in your app. However, be aware that *a new token is generated every 25 seconds* 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 the navigational landing page.

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.

Password Change

Current Password *

Password must be at least 8 characters, contains 1 number, 1 lowercase, 1 uppercase and 1 special character (!@#\$%^&*)

New Password *

Confirm New Password *

Submit

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'.

HHS Rules of Behavior and Security training certification

The *The Rules of Behavior for Use of HHS Information Resources* (HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. All new users of HHS information resources must read the HHS RoB and sign, by checking, the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB.

Please click the link below to review the RoB documentation and check the box to certify your adherence.

[Rules of Behavior](#)

☐ I have read the HHS Rules of Behavior for Use of Information Resources (HHS RoB), document number HHS-OCIO-2018-0004 and dated July 25, 2018. I understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the Operating Division (OpDiv) Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

The security training requirement to Use of HHS Information Resources (HHS Security Training) provides the awareness of handling personally identifiable information (PII) and also other security aspect to avoid security breach and compromise of information. This training must be done yearly. The training can be done through your company or government agencies mandatory yearly training or by taking the two security training classes below.


Please click the link below to review the security training requirement to access HHS system

[Cybersecurity Awareness Training](#)
[Cybersecurity Essentials Training](#)

☐ I have read the HHS Security Training requirement and confirm that I have completed either (a) the two classes linked above or (b) a separate training through my employer's yearly requirement.

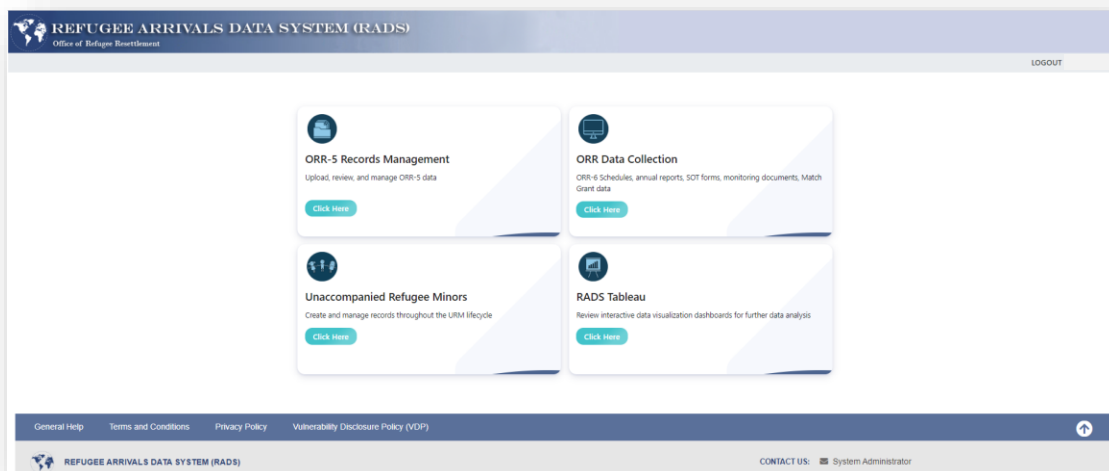
Submit

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



The image shows a 'Security Questions' form. It contains three identical sections for security questions. Each section has a dropdown menu for selecting a question (currently showing '-- Please select --') and a text input field for the answer. The questions are labeled 'Security Question 1 *', 'Security Question 2 *', and 'Security Question 3 *'. At the bottom of the form is a blue 'Submit' button.

After 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 this screen:



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.

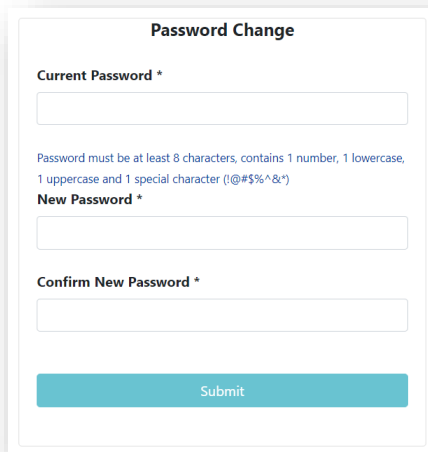
Once you have received the email, you will enter the PIN from the email into the provided textbox in RADS. Then Click 'Submit'.

A screenshot of a web form titled '2nd Factor Authentication (PIN)'. The form has a light gray border. Inside, there is a heading '2nd Factor Authentication (PIN)' in bold. Below the heading is a prompt: 'Please enter the PIN sent on the email address on the record'. Underneath the prompt is a text input field labeled 'PIN'. At the bottom of the form is a large blue button with the word 'Submit' in white text.

- **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.



Password Change

Current Password *

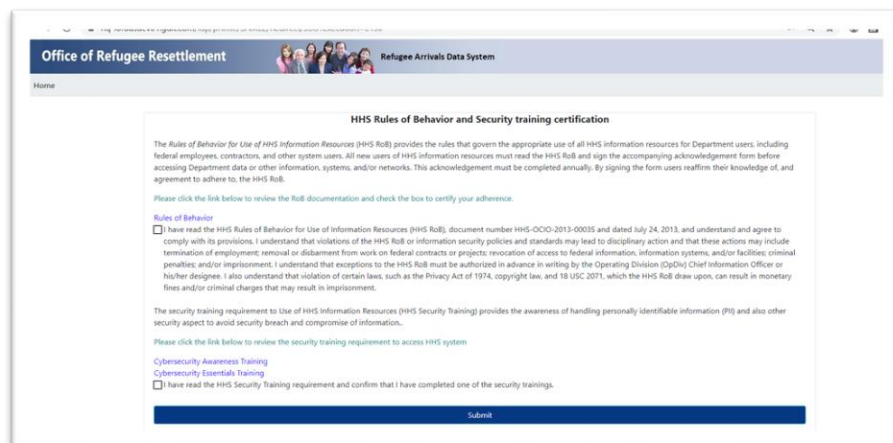
Password must be at least 8 characters, contains 1 number, 1 lowercase, 1 uppercase and 1 special character (!@#\$\$%^&*)

New Password *

Confirm New Password *

Submit

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'.



Office of Refugee Resettlement **Refugee Arrivals Data System**

Home

HHS Rules of Behavior and Security training certification

The Rules of Behavior for Use of HHS Information Resources (HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. All new users of HHS information resources must read the HHS RoB and sign the accompanying acknowledgment form before accessing Department data or other information, systems, and/or networks. This acknowledgment must be completed annually. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB.

Please click the link below to review the RoB documentation and check the box to certify your adherence.

[Rules of Behavior](#)

☐ I have read the HHS Rules of Behavior for Use of Information Resources (HHS RoB), document number HHS-OCIO-2013-00035 and dated July 24, 2013, and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment, removal or disbarment from work on federal contracts or projects, revocation of access to federal information, information systems, and/or facilities; criminal penalties, and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the Operating Division (OpDiv) Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

The security training requirement to Use of HHS Information Resources (HHS Security Training) provides the awareness of handling personally identifiable information (PII) and also other security aspect to avoid security breach and compromise of information.

Please click the link below to review the security training requirement to access HHS system

[Cybersecurity Awareness Training](#)
[Cybersecurity Essentials Training](#)

☐ I have read the HHS Security Training requirement and confirm that I have completed one of the security trainings.

Submit

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

Security Questions

Security Question 1 *

-- Please select --

Answer for security question 1 *

Security Question 2 *

-- Please select --

Answer for security question 2 *

Security Question 3 *

-- Please select --

Answer for security question 3 *

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. *Please note: Verified Users do not have to complete 2FA.*

- **Step 1:** Go to this RADS URL: <https://rads.acf.hhs.gov/rads/>

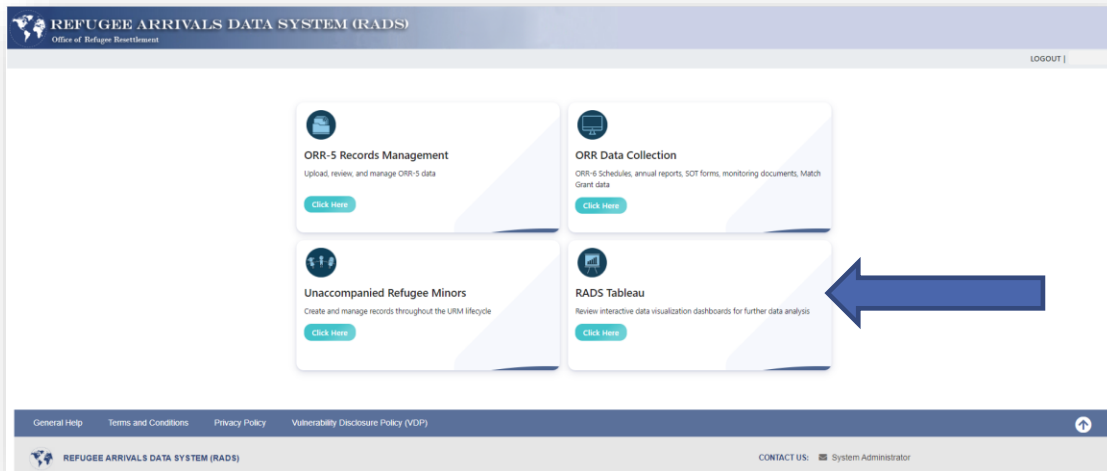
- **Step 2:** Enter your assigned user ID in the textbox provided
- **Step 3:** Enter your personal password in the textbox provided
- **Step 4:** Select 'Login'
- **Step 5:** Select one of the three options for your 2nd Factor Authentication

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, you will enter the 6-digit token that appears in your Google Authenticator app and select 'Submit'. <i>Note: This is the preferred method for 2FA.</i>	If you have 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 outlined 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, please take the time to delete any old ORR-RADS token accounts listed in your phone app. RADS will only accept 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.

To get to RADS Tableau, select the RADs Tableau module box after logging into RADS.



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 entire browser window, regardless of the browser you're using. Until a user closes the browser, they remain authenticated.

Logging out of Tableau	≡	✓ Logs you out of Tableau ✗ Does not log you out of RADS
Logging out of RADS	≡	✗ Does not log you out of Tableau ✓ Logs you out of RADS
Closing the browser	≡	✓ Logs you out of Tableau ✓ Logs you out of RADS