

This document lets **External users of UC Portal (i.e., non-government users)** users know how to setup Multi-Factor Authentication required to **access the application through Single Sign-on (ORR App Launcher)**.

- 1 Check your email for a message from ORRApplauncher@acf.hhs.gov. Click the "Confirm your email address" verification link.
- 2 Use the App Launcher link → <https://orr-uc-apps.acf.hhs.gov/s/login> to begin
- 3 Click the "Non-HHS User" button

Office of Refugee Resettlement (ORR)
App Launcher

Non HHS User

HHS User

This is a U.S. government service. Your use indicates your consent to monitoring, recording, and no expectation of privacy. Misuse is subject to criminal and civil penalties.
[Read more details.](#)

- 4 "Enter your email" and click Next

Office of Refugee Resettlement (ORR) App Launcher

Sign in as non-HHS User

Enter your email

Back Next

- 5 Enter the verification code received in the email here

Office of Refugee Resettlement (ORR) App Launcher

Sign in as non-HHS User

Enter verification code received via email

Back Verify

This document lets **External users of UC Portal (i.e., non-government users)** users know how to setup Multi-Factor Authentication required to **access the application through Single Sign-on (ORR App Launcher)**.

6a Set up your second layer of security.

As an added layer of protection, App Launcher requires you set up a secondary authentication method to keep your account secure. This is referred to as two-factor authentication (2FA).

We recommend using Salesforce Authenticator. **You could also use an Authenticator of your choice.** Download and install Salesforce Authenticator App on your mobile device from App Store or Google Play.

Enter Salesforce App, swipe through a brief tour and enter your mobile number.

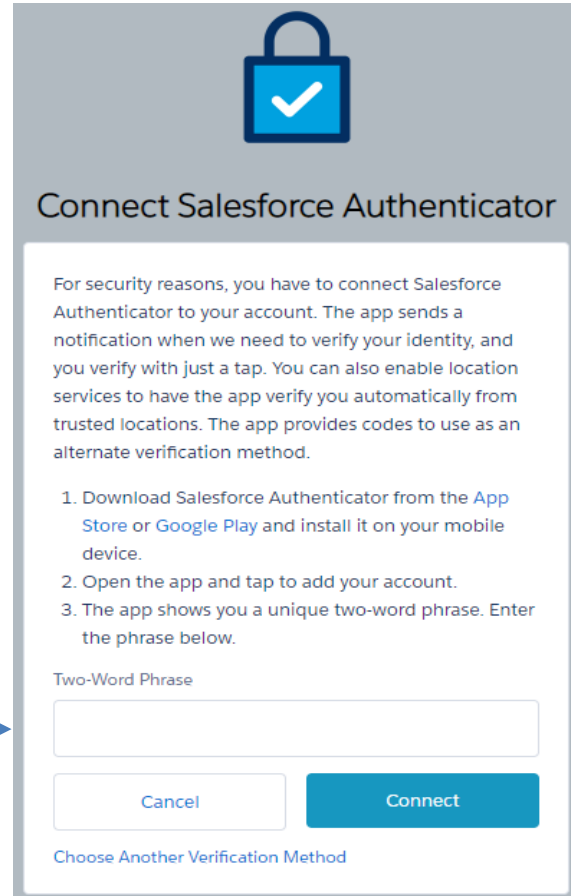
6b Verify your identity.

Authenticator sends you a link to verify your mobile number. When you get the text message, tap the link to open the Authenticator App.

6c Enter your Two-word Phrase. (for Salesforce Authenticator only)

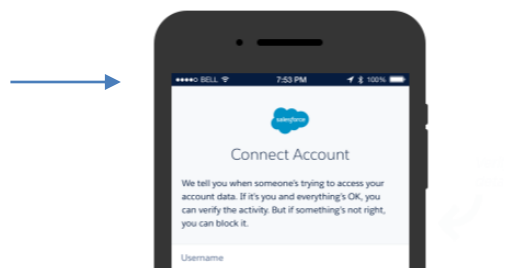
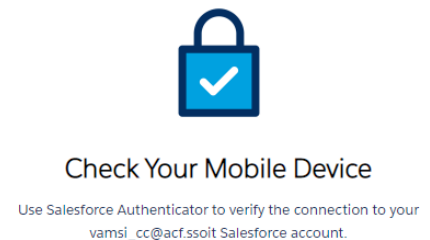
Click on Authenticator prompt to “connect your app”

A two-word Phrase will be displayed on your mobile device. Enter the phrase into the text box on your computer (you may need to click the “Add an Account” to get the 2-word phrase)



7 Verify your identity.

Approve the Salesforce Authenticator final step to verify your account



[Having Trouble?](#)

This document lets **External users of UC Portal (i.e., non-government users)** users know how to setup Multi-Factor Authentication required to **access the application through Single Sign-on (ORR App Launcher)**.

8 Setup a 8 to 10-digit PIN, your second layer of security.

You will be required to setup a 8 to 10 digit-PIN as an additional layer of your identity.

Note: DO NOT use the code from the Authenticator. This will be your personal PIN



vamsi_cc@acf.ssoit [Log Out](#)

As an added layer of security, you are required to setup 8 to 10 digit personal/secret PIN that you can easily remember.

Note: This is NOT the code that may show on your Authenticator App

* PIN

* Confirm PIN

[Continue](#)

9 Setup Challenge questions as backup in case you forget your PIN

Submit responses to at least 3 of the 5 questions



vamsi_cc@acf.ssoit [Log Out](#)

In the event you forget your Personal PIN, you will be prompted to answer challenge questions to reset it. Please submit responses to at least 3 of the following challenge questions.

In which city or town were you born?

What is the zip code of the first house you lived in?

What is your father's middle name?

What is your mother's birth month?

What is the Model of your first car?

[Continue](#)

This document lets **External users of UC Portal (i.e., non-government users)** users know how to setup Multi-Factor Authentication required to **access the application through Single Sign-on (ORR App Launcher)**.



vamsi_cc@acf.ssoit Log Out

10

You are required to complete the two compliance trainings.

You are required to complete these steps.  Click Continue

You are required to complete the **Cyber Security Awareness Training** and **Rules of Behavior** to access the ORR App launcher.

- Complete Cyber Security Awareness Training
- Upload the Completion Certificate below
- Review Rules of Behavior Document and Sign

Please click the Continue button to start the process

Continue

11

Mandatory Compliance Training

Follow the prompts, to complete/upload the Cyber security training, acknowledge the ROB and continue to App Launcher

NOTICE

You are required to complete the **Cyber Security Awareness Training** and **Rules of Behavior** to access the ORR App launcher.

- Complete Cyber Security Awareness Training
- Upload the Completion Certificate below
- Review Rules of Behavior Document and Sign

[Complete Cyber Security Training](#)

Upload Cyber Security Training Completion Certificate here

 Upload Files Or drop files

Continue

Rules of Behavior for General Users v. 2.2

These *Rules of Behavior (RoB)* for General Users apply to all Department of Health and Human Services (HHS) employees, contractors, and other personnel who have access to HHS Information resources and information technology (IT) systems. Users of HHS Information and Information systems shall read, acknowledge, and adhere to the following rules prior to accessing data and using HHS information and systems.

A. HHS Information Systems

When using and accessing HHS information resources and systems, I understand that I must:

1. Comply with federal laws, regulations, and HHS Operating Division (OpDiv) policies, standards, and procedures and that I must not violate, direct or encourage others to violate HHS policies, standards or procedures;
2. Not allow unauthorized use and access to HHS information and information systems;
3. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing;
4. Limit personal use of information and IT Resources to the extent that it does not:
 - a. disrupt my productivity;
 - b. interfere with the mission or operations of HHS; and
 - c. violate HHS security and privacy policies;
5. Have no expectation of privacy while using and accessing HHS information resources and assets at any time, and I understand that any actions and activities are subject to HHS monitoring, recording, and auditing;

ORR App Launcher ACF Rules of Behavior for Privileged User Accounts Signature

I have read the ACF Rules of Behavior for Privileged User Accounts and understand and agree to comply with its provisions.

I understand that violations of the ACF Rules of Behavior for Privileged User Accounts 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 facilities, criminal penalties, and imprisonment.

I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the ACF Rules of Behavior for Privileged User Accounts draws upon, may result in monetary fines and criminal charges that may result in imprisonment.

☐ Accept

Continue

This document lets **External users of UC Portal (i.e., non-government users)** users know how to setup Multi-Factor Authentication required to **access the application through Single Sign-on (ORR App Launcher)**.

12

Welcome to App Launcher!!

