A Accessing One-e-App

The One-e-App system is shared by FAA, AHCCCS, and authorized facilities. To access One-e-App, a user account must be created for the specific agency. The user account defines which One-e-App screens the user has authorization to access, at both the agency and internal level.

Policy and procedures regarding accessing the One-e-App system are outlined as follows:

- One-e-App User Profiles
- One-e-App User Account Authorization
- One-e-App User Log in

.01 One-e-App User Profile

The levels of access to One-e-App for FAA are as follows:

- Administrative Profile

  This profile is defined in One-e-App as an "Agency Supervisor or Liaison." The Administrative Profile is reserved for authorized staff only, and is used for monitoring and security. The first screen to display for the Administrative Profile is the WORKLOAD SUMMARY screen.

  From the WORKLOAD SUMMARY screen, unassigned and assigned Health-e-Arizona applications at ALL FAA local offices can be monitored.

- Supervisor Profile

  This profile is defined in One-e-App as a "DES KidsCare, SSI Supervisor." The Supervisor Profile is used to monitor ALL Health-e-Arizona applications at the user's FAA local office. The first screen to display for the Supervisor Profile is the UNASSIGNED APPLICATIONS screen.

From this screen, unassigned Health-e-Arizona applications can be received and assigned to authorized EIs with an EI Profile, or transferred to AHCCCS or to another FAA local office.

NOTE The Supervisor Profile is not limited to FAA Supervisors. The local office may decide to activate this profile for OST staff, to allow the staff to assign and register applications.

- Eligibility Interviewer (EI) Profile

This profile is defined in One-e-App as a "DES, KidsCare, SSI Worker." The EI Profile is used to monitor ALL Health-e-Arizona applications assigned to the EI's workload. The first screen to display for the EI Profile is the ASSIGNED APPLICATIONS screen.

From this screen, the EI can monitor and work each assigned Health-e-Arizona application.

Authorize users to access One-e-App, see One-e-App User Account Authorization.

.02 One-e-App User Account Authorization

REVISION 08
(04/01/09 – 06/30/09)

Authorize user access to the One-e-App system as follows:

- Complete a J-125 form for the staff. Include the following on the J-125:

Staff’s d0 log in ID. The d0 log in ID is used to create the One-e-App User Name.

Staff’s site code location.

Staff’s One-e-App User Profile. This is necessary to assign the correct account profile in One-e-App.

Staff's e-mail address.

Both of the following:

- "HEALTH-E-ARIZONA"
- “TOPAZ USER" (TOPAZ is software that enables staff to view and print electronic signatures.)

A Supervisor forwards the J-125 to FAA Data Security. When the J-125 for the One-e-App User Account request is received, FAA Data Security completes the following:

- Adds the new user to One-e-App.
- Assigns the User Profile and site code location.
- Activates the One-e-App User Account.
- Contacts the staff by e-mail informing them the account has been authorized and is active, and providing the link to the One-e-App web site.

  The e-mail also informs the staff to log in to the new account on the One-e-App USER LOG IN screen for the first time, as follows:

  - Key the staff's d0 log in ID in the USER NAME field.
  - Key the temporary password provided by FAA Data Security in the PASSWORD field.

When staff log in for the first time, One-e-App prompts them to complete the following:

- Review and scroll to the bottom of the Click Agreements. Click on I AGREE.
- Change the temporary password provided by FAA Data Security to a new password by completing the following:
- Select a new password following the formatting requirements in Passwords to Secured Systems.
- Key the new password in the NEW PASSWORD field.
- Key the new password again to confirm in the CONFIRM PASSWORD field.
- Choose and answer a secret question.

WARNING

Do NOT use another staff's User Name and password to access the One-e-App system. Information returned through One-e-App is secured and confidential. Misuse of the authorized access to One-e-App is a security violation.

Once a user account is active, ensure that electronic signatures can be viewed. When the electronic signatures do not display, contact the FAA Information Technology (IT) Unit to determine whether the TOPAZ software must be installed.

One-e-App accounts expire and deactivate as follows:

- New accounts that have not been activated by the user within 30 calendar days of creation deactivate on the 30th day.
- Active accounts in which the user has not logged in within the past 60 calendar days deactivate on the 60th day.

To reactivate expired accounts, contact FAA Data Security.

To remove staff from the One e App system, see Deleting Security Profiles.

.03 One-e-App User Log in

REVISION 02
(10/01/07 - 12/31/07)

To log in and access the One-e-App system, complete the following:

- Access the One-e-App web site. The One-e-App USER LOG IN screen displays. Complete the following:

  Key the staff's d0 log in in the USER ID field.

  Key the account's password in the PASSWORD field.

  Click on NEXT, or press ENTER.
- The first One-e-App screen displays, based on the One-e-App User Profile.

WARNING

Do NOT use another staff's user ID and password to access the One-e-App system. Information returned through One-e-App is secured, and is confidential. Misuse of the authorized access to One-e-App is a security violation.

When staff are unable to remember their password, or their account is disabled after five unsuccessful attempts to log in, complete either of the following:

- Contact FAA Data Security to have the password reset.
- When a secret question was previously selected, complete the following:

  Click on CLICK HERE on the USER LOG IN screen.

  When the REACTIVATE YOUR ACCOUNT screen displays, key the answer to the selected secret question. Click on NEXT, or press ENTER.

  When the CHANGE PASSWORD screen displays, create a new password.

Staff are required to review and agree to One-e-App user license and confidentiality conditions, referred to as the Click Agreements. The Click Agreements are required when any of the following occur:

- A new user logs in to the One-e-App system for the first time
- The password expires, is changed, or reset
- The secret question is changed or used to log-in

The Click Agreements display on the following screens:

- USER LICENSE AGREEMENT FORM
- USER CONFIDENTIALITY AGREEMENT

Scroll to the bottom of the Click Agreement text to enable the agreement check boxes, and click on I AGREE.