FTA Access Control and Entry System (FACES)

User Guide

Version: 6.4.7
As of 8 April 2024

Prepared for:

Prepared by:

Federal Transit Administration

Table of Contents

Revision History

Date	Version	Description	Author
08/08/2021	6.3.0	Updated with Login.gov instructions.	C. Palencia
10/29/2021	6.3.1	Updated OTrak user roles table.	C. Palencia
11/15/2021	6.3.2	Updated section 7.1.	C. Palencia
12/07/2021	6.3.3	Updated Sections 6.3 and 7.3.	C. Palencia
12/17/2021	6.3.4	Updated Screenshots to 6.3.4.	C. Palencia
01/10/2022	6.3.5	Updated email screenshots throughout.	C. Palencia
02/25/2022	6.3.6	Updated Sections 6.2.1, 6.2.2, 6.2.3, 6.3.2.	C. Palencia
03/28/2022	6.3.7	Added Section 3.3.1.	C. Palencia
01/12/2023	6.3.8	Removed references to Justification Documents being required.	B. Anderson
04/07/2023	6.4.0	Updated Sections 4.2,6.2.1, 6.2.2, 7.1, Appendix B, C.	B. Anderson
04/20/2023	6.4.1	Updates	A. Burnett
04/27/2023	6.4.2	Updated formatting and layout.	G. Nesburg
10/30/2023	6.4.3	Updates – Template changed, any direct reference to “you” changed to “users” or “the user”.	G. Nesburg
12/05/2023	6.4.4	Updated sections to add NTD Non-FTA User Category and External Read Only role	
02/20/2024	6.4.5	Updated DOT User Role Category for Otrak to External Read ONLY	B. Khan
03/01/2024	6.4.6	Updated sections of recertifying users, add/update users, and review role requests regarding comment section in FACES	B. Khan
04/08/2024	6.4.7	Added new header (6.4 **Reviewing Monthly User Comparison Report**) and added details to **Recertification.** Edited **User Management** Section. Edited **Reviewing Monthly User Comparison Report**	B. Khan

1. Introduction

1.1. What is FACES?

The Federal Transit Administration (FTA) maintains several web-based software systems that reside on the same FTA platform. The FTA platform is accessed via the website, https://faces.fta.dot.gov/suite/. The systems on this FTA platform include the Transit Award Management System (TrAMS), the National Transit Database (NTD), FTA Discretionary Grant System (DGS), the Joint Procurement Clearinghouse (JPC), and the FTA Access Control and Entry System (FACES). TrAMS is FTA's system for awarding and managing federal grants. NTD is FTA's system for tracking transit statistics on American transit systems. The JPC is available to FTA grant recipients for communicating about procurement needs and soliciting partners for a joint purchase. DGS is FTA's system for approving or rejecting grant applications and preparing funding scenarios. FACES is the user creation and management system for each user on the FTA platform. All other software systems on the FTA platform rely on FACES for user management functions. Within FACES, each software system has its own set of user roles access privileges.

2. User Access

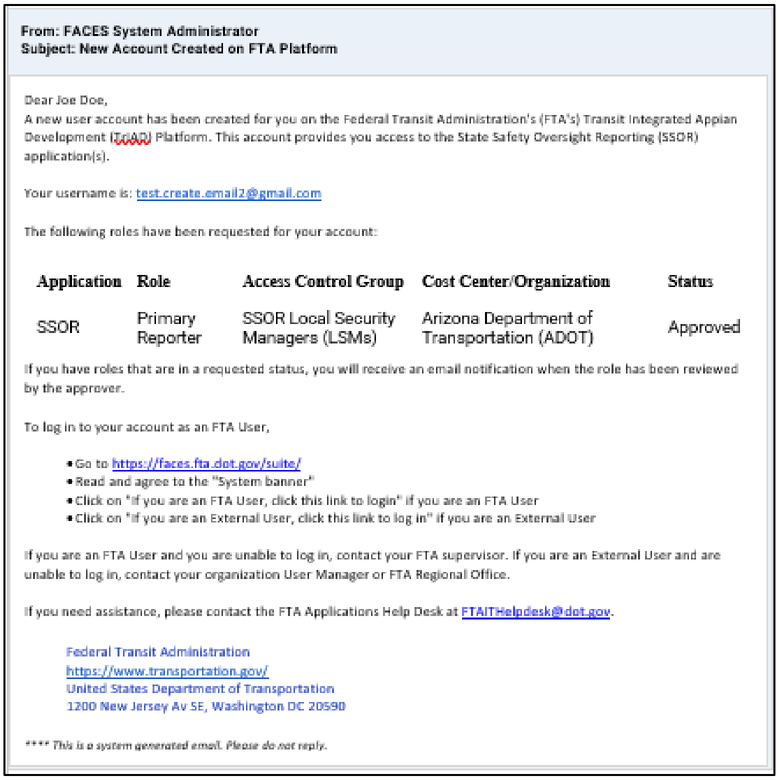
2.1. New User Account Creation

User access to each of the FTA software systems on the FTA platform, https://faces.fta.dot.gov/, is granted by either an organizational User Manager (UM), Local Security Manager (LSM), or Global Security Manager (GSM) within the appropriate system. An individual with one of those roles can create user accounts and assign users an initial suite of roles. Once an account has been created, the user will receive an automated email notification containing their username and access/login instructions,

- **Username** – all usernames are initially set to the email address associated with the user's account. The username cannot be changed. If a user needs to update their email address, they will need to contact FTAITHelpdesk@dot.gov for assistance.

2.1.1 Non-FTA User Setup

New non-FTA users will receive an automatic email notification from FACES once their account is created. It will look like the one below. If you need an account on the TrIAD platform, then reach out to your User Manager or Local Security Manager.



From: FACES System Administrator
Subject: New Account Created on FTA Platform

Dear Joe Doe,
A new user account has been created for you on the Federal Transit Administration's (FTA's) Transit Integrated Appian Development (TriAD) Platform. This account provides you access to the State Safety Oversight Reporting (SSOR) application(s).

Your username is: test.create.email2@gmail.com

The following roles have been requested for your account:

Application	Role	Access Control Group	Cost Center/Organization	Status
SSOR	Primary Reporter	SSOR Local Security Managers (LSMs)	Arizona Department of Transportation (ADOT)	Approved

If you have roles that are in a requested status, you will receive an email notification when the role has been reviewed by the approver.

To log in to your account as an FTA User,

- Go to https://faces.fta.dot.gov/suite/
- Read and agree to the "System banner"
- Click on "If you are an FTA User, click this link to login" if you are an FTA User
- Click on "If you are an External User, click this link to log in" if you are an External User

If you are an FTA User and you are unable to log in, contact your FTA supervisor. If you are an External User and are unable to log in, contact your organization User Manager or FTA Regional Office.

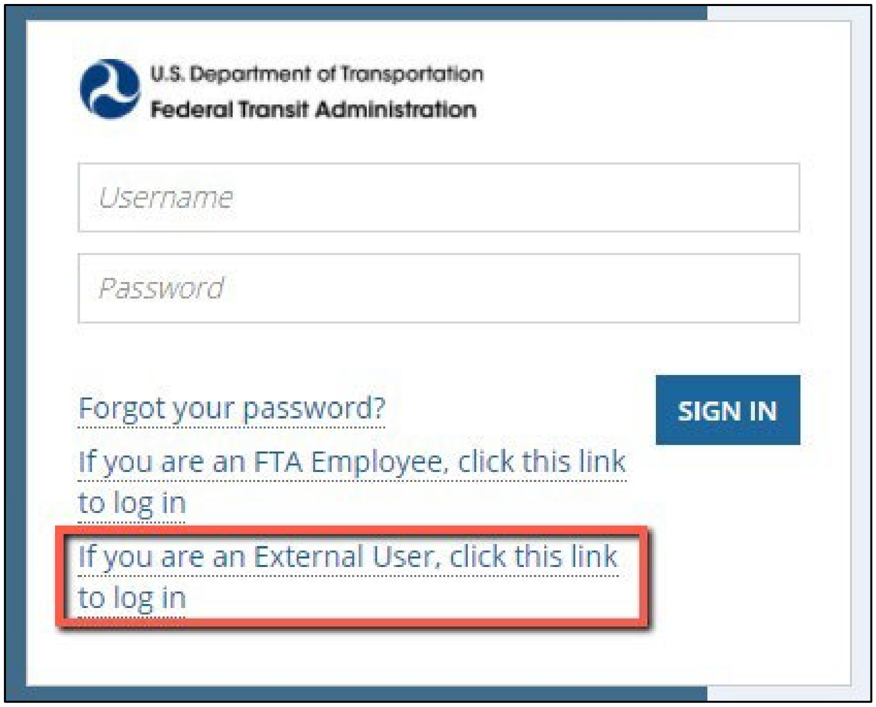
If you need assistance, please contact the FTA Applications Help Desk at FTAITHelpdesk@dot.gov.

Federal Transit Administration
https://www.transportation.gov/
United States Department of Transportation
1200 New Jersey Av SE, Washington DC 20590

***** This is a system generated email. Please do not reply.*

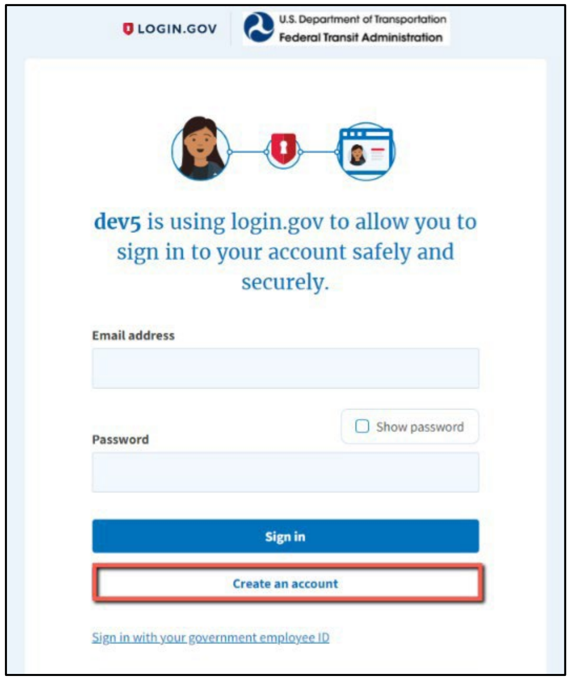
1) Using the email, select the URL (internet link) to access the site, [https://faces.fta.dot.gov/.](https://faces.fta.dot.gov/)
2) Read the security policy and select ***I AGREE.***

3) On the login page, select the ***If you are an External User, click this link to log in*** link next to ***Sign In***.

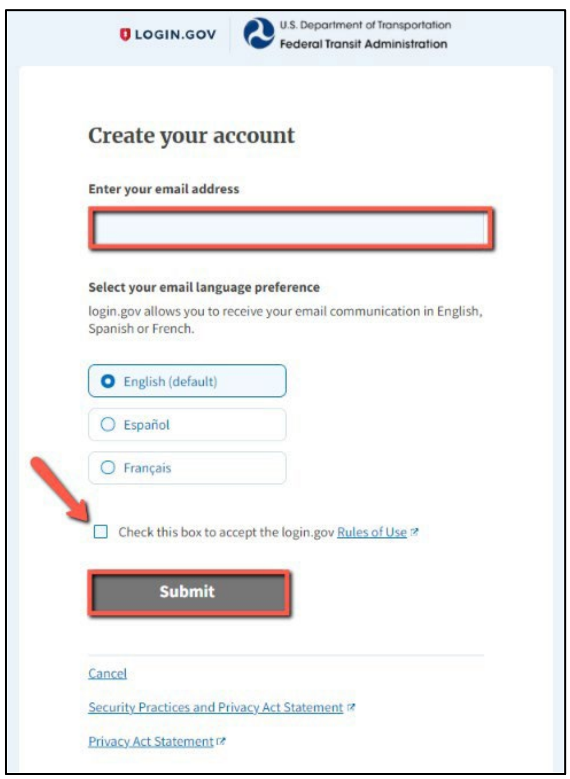


4) Users will be redirected to Login.gov where all External users will need to initially create and register an account.

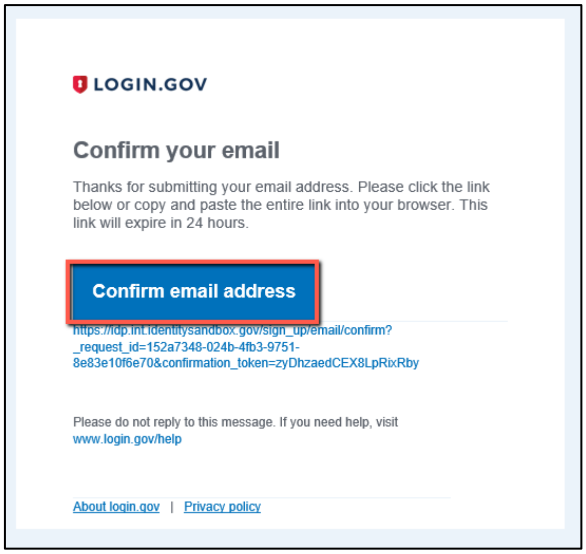
5) If this is the first-time using Login.gov the user will need to Click on ***Create an account***.



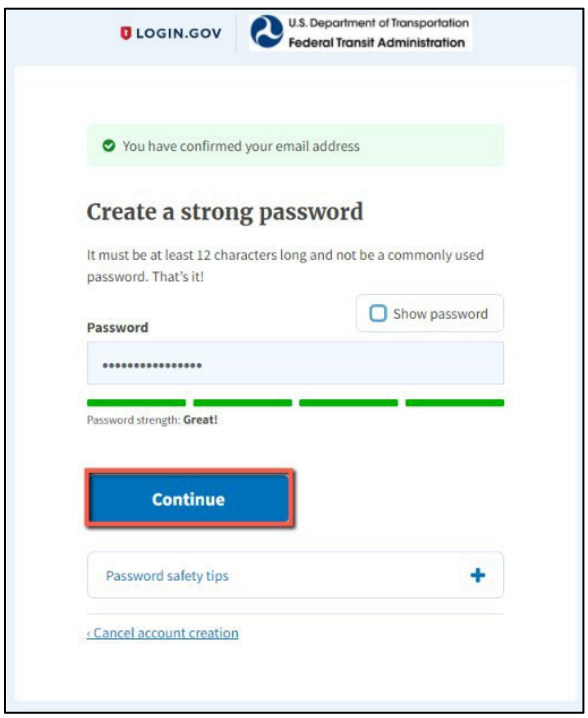
6) Enter your email and check off the box accepting login.gov ***Rules of Use***.



7) Login.gov will send you a "Confirm Your Email" email. In that email, click on "Confirm email address".



8) The user is redirected back to login.gov and is asked to create a strong password and click Continue.



9) Select one of the five authentication method options and follow the setup instructions.

   1) **Security Key** - A security key is typically an external physical device, like a USB, that you plug into your computer. The key is linked to your accounts and will only grant access to those

accounts once the key is plugged in and activated. Login.gov requires security keys that meet the FIDO (Fast Identity Online) standards.

2) **Government Employee ID** - Physical PIV (personal identity verification) cards or CACs (common access cards) are secure options for federal government employees and military personnel. These cards, with encrypted chip technology, are resistant to phishing and difficult to hack if stolen.

3) **Authentication Application** - Authentication applications are downloaded to your device and generate secure, six-digit codes you use to sign into your accounts.

   i. Google Authenticator

   ii. Authy

   iii. LastPass

   iv. 1Password

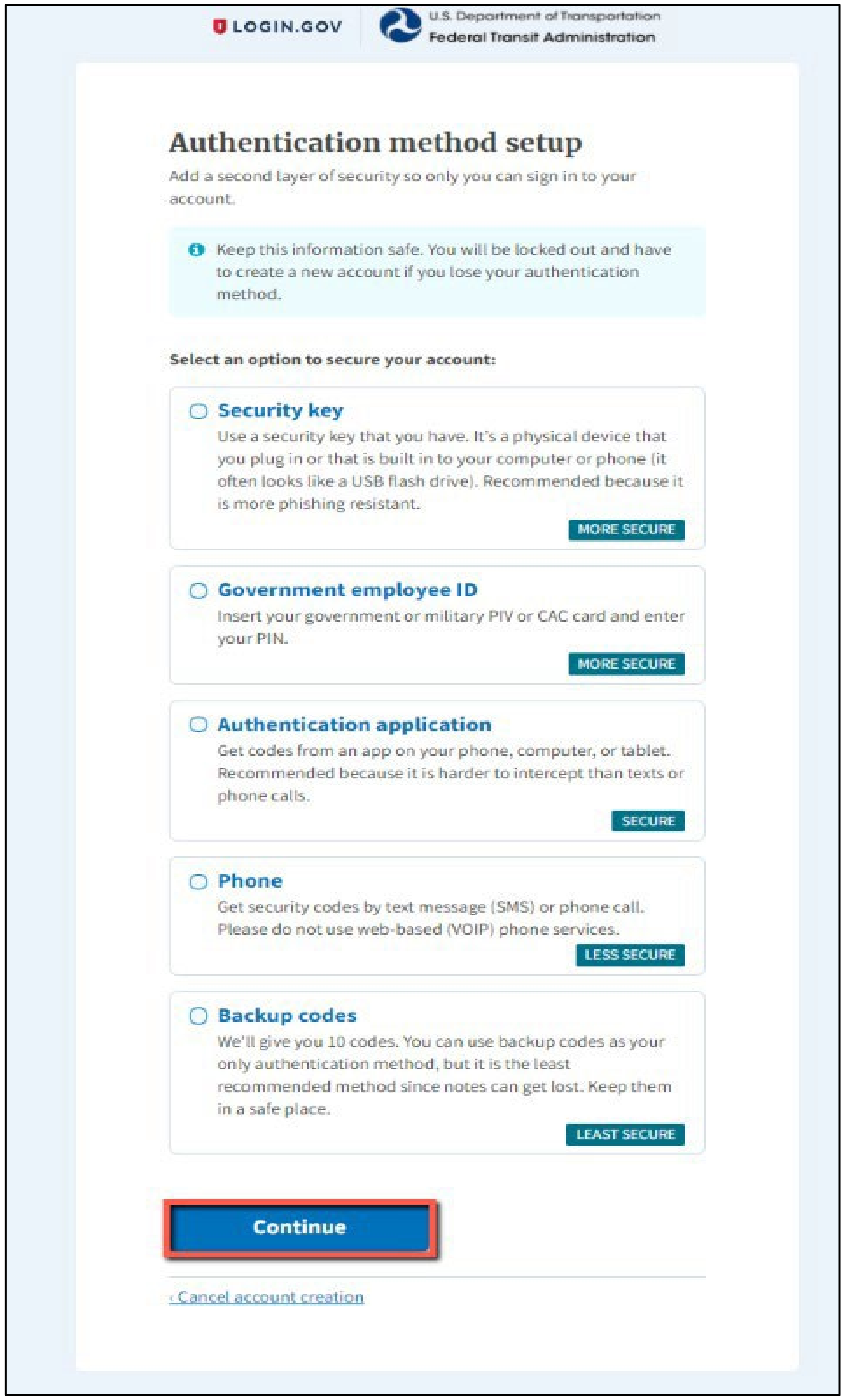
   v. OTP Manager

   vi. Authenticator

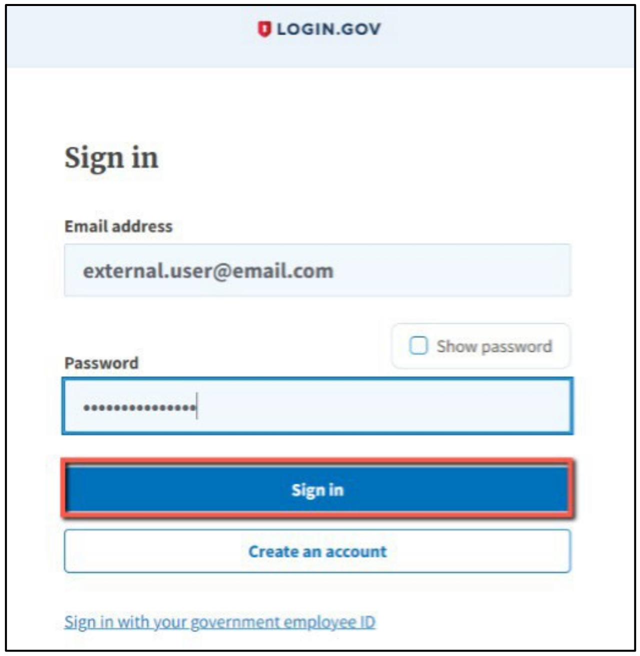
   This method offers more security than phone calls or text messaging against phishing, hacking, or interception. A one-time passcode is generated by the application each time you sign in to login.gov.

4) **Phone** - A unique security code is sent to that phone number via SMS or phone call each time you sign in to your login.gov account. Each security code expires after ten minutes and can only be used once. You will receive a new security code each time you sign in to your login.gov account.

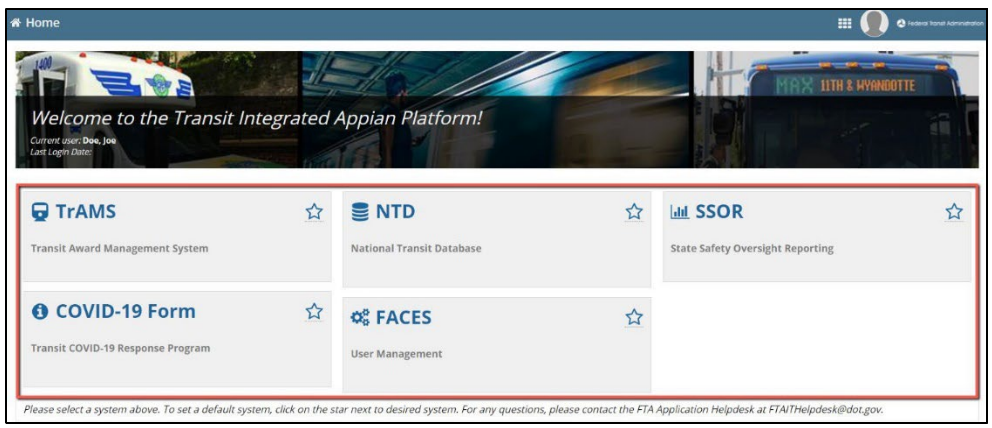
5) **Backup codes** - are an accessible option for users who do not have access to a phone. However, backup codes are the least secure option for two-factor authentication. Login.gov will generate a set of ten codes. Backup codes must be printed or written down which makes them more vulnerable to theft and phishing. After you sign in with your username and password, you will be prompted for a code. Each code may be used only once. When the tenth code has been used you will be prompted to download a new list.



6) Once the authentication method has been set up, the user will be redirected to sign in to Login.gov using the credentials just created.



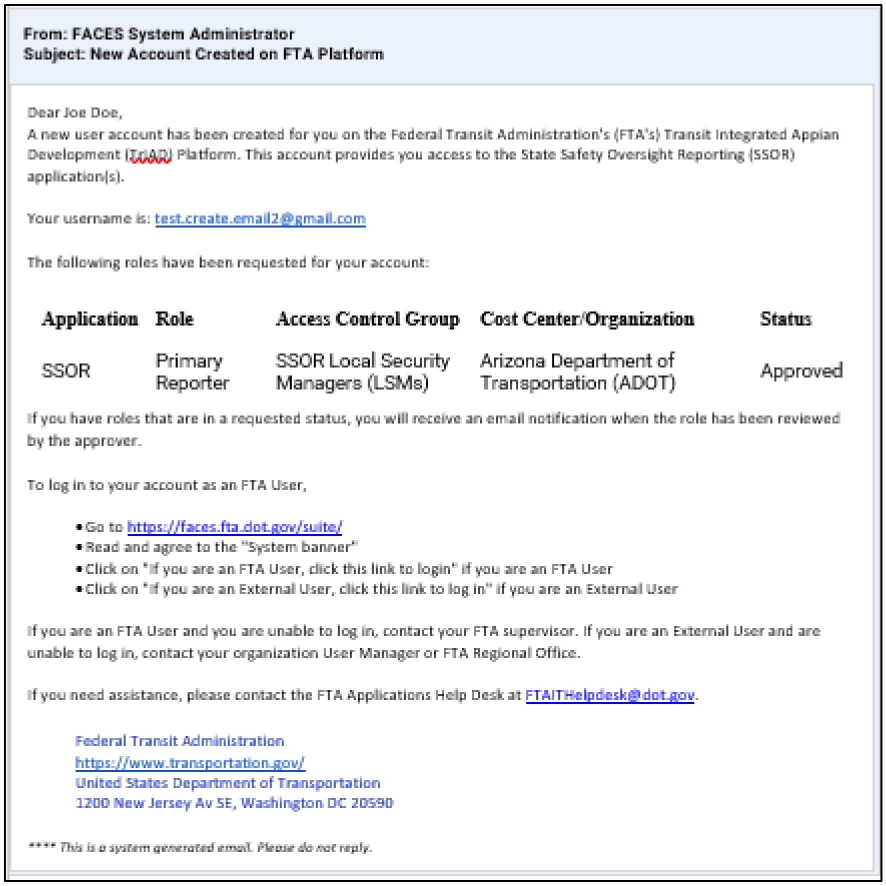
7) The user will be directed to the **FTA Homepage**.



2.1.2 FTA User Setup

New users will receive an automatic email notification from FACES once their account is created. If you need an account on the TrIAD platform, then reach out to your User Manager or Local Security Manager.

1) The email will be formatted much like the one below:



From: FACES System Administrator
Subject: New Account Created on FTA Platform

Dear Joe Doe,
A new user account has been created for you on the Federal Transit Administration's (FTA's) Transit Integrated Appian Development (TriAD) Platform. This account provides you access to the State Safety Oversight Reporting (SSOR) application(s).

Your username is: test.create.email2@gmail.com

The following roles have been requested for your account:

Application	Role	Access Control Group	Cost Center/Organization	Status
SSOR	Primary Reporter	SSOR Local Security Managers (LSMs)	Arizona Department of Transportation (ADOT)	Approved

If you have roles that are in a requested status, you will receive an email notification when the role has been reviewed by the approver.

To log in to your account as an FTA User,

- Go to https://faces.fta.dot.gov/suite/
- Read and agree to the "System banner"
- Click on "If you are an FTA User, click this link to login" if you are an FTA User
- Click on "If you are an External User, click this link to log in" if you are an External User

If you are an FTA User and you are unable to log in, contact your FTA supervisor. If you are an External User and are unable to log in, contact your organization User Manager or FTA Regional Office.

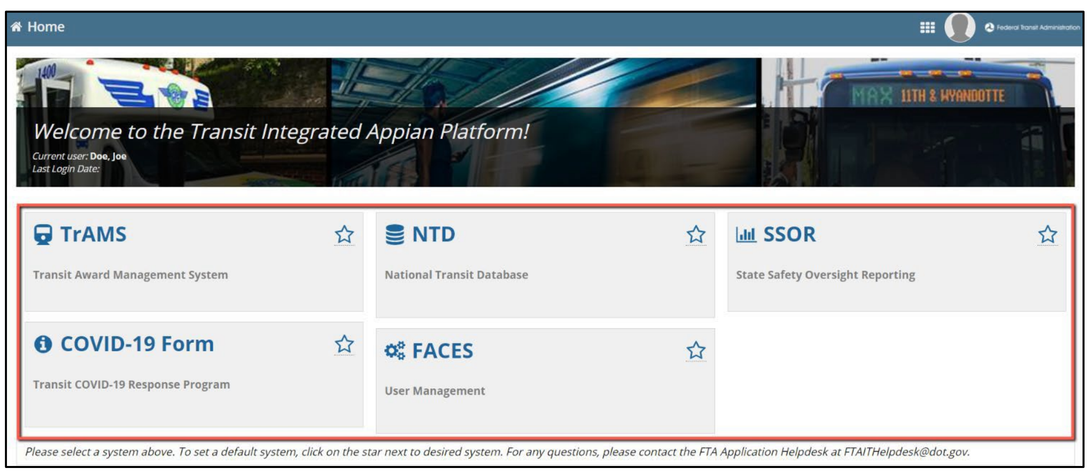
If you need assistance, please contact the FTA Applications Help Desk at FTAITHelpdesk@dot.gov.

Federal Transit Administration
https://www.transportation.gov/
United States Department of Transportation
1200 New Jersey Av SE, Washington DC 20590

***** This is a system generated email. Please do not reply.*

2) Using the email, select the URL (internet link) to access the site, https://faces.fta.dot.gov/.

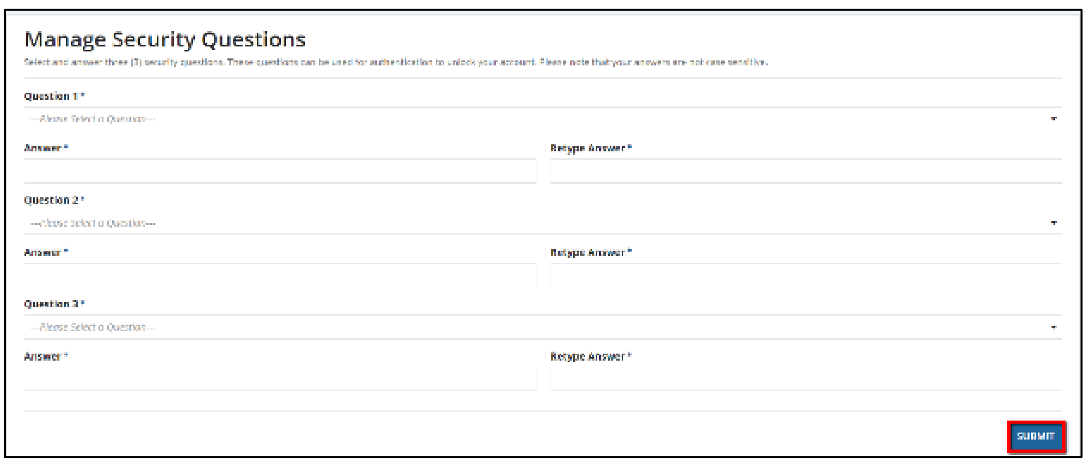
3) The user will be automatically logged while inside the network or using VPN.



All new users will have to set up **Security Questions and Answers (Q&As)** to ensure the security of the account and to provide a mechanism to re-establish access when lost due to a lockout, etc. **It is**

strongly recommended that all users set up account security questions. Click on, "Click here to finish setting up your Security Questions and Answers" to continue.

4) On the **Manage Security Questions** page, select three questions and provide appropriate answers that can be easily recalled when needed. A few rules apply to the setting of Security Q&As:
    a. All users can set up and manage three (3) security questions through the **Manage Security Questions** page.
    b. Questions must be selected from an FTA approved list and 3 distinct questions must be selected.
    c. Answers must contain at least three (3) characters and the same answer cannot be used for more than one question.
    d. Answers are case insensitive (e.g., "dog" is the same as "DOG").
    e. Once questions are established, users must correctly answer their existing questions to change them. Section 5.2.3 address how to change existing security questions.
5) Click ***Submit***.



6) Users will receive an automated email notification that their questions have been updated.

2.2. Logging In

FACES manages user access to the FTA platforms via the FACES login page, accessed via a web browser. Two login methods are available, but one is only accessible to FTA employees using FTA's internal network. User access to software systems like TrAMS and NTD is based on the user's assigned **Roles**.

2.2.1 Standard Login (Non-FTA Employee)

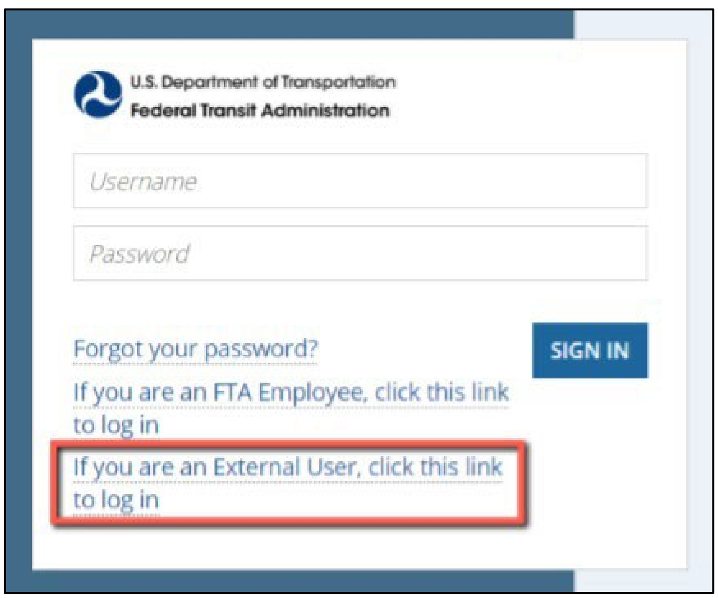
Non-FTA Employees will be redirected to Login.gov for authentication.

To login:

1) Open a web browser and enter the FACES URL, https://faces.fta.dot.gov/.

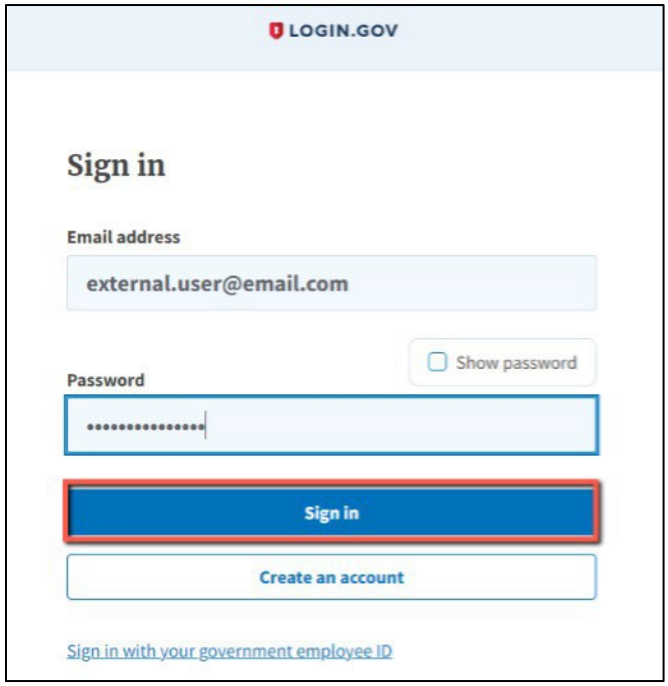
2) Read the security policy and click ***I AGREE***.

3) On the login page, select the ***If you are an External user, click this link to log in*** link next to ***Sign In***.

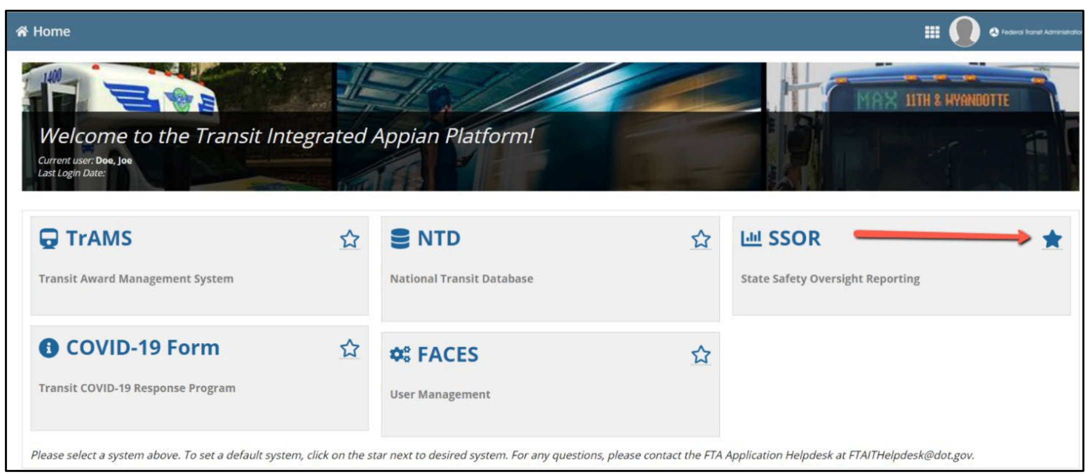


4) Users will be redirected to Login.gov where all external users will need to sign in with the account that was created in section 2.1.1 and

will need to be authenticated with the authentication method that was set up.



5) The user will be taken to the **Homepage**, where the user has the option to click the system they wish to use. If the user has access to more than one FTA platform (TrAMS, NTD, DGS, SSOR or FACES) all those options will be available to click.

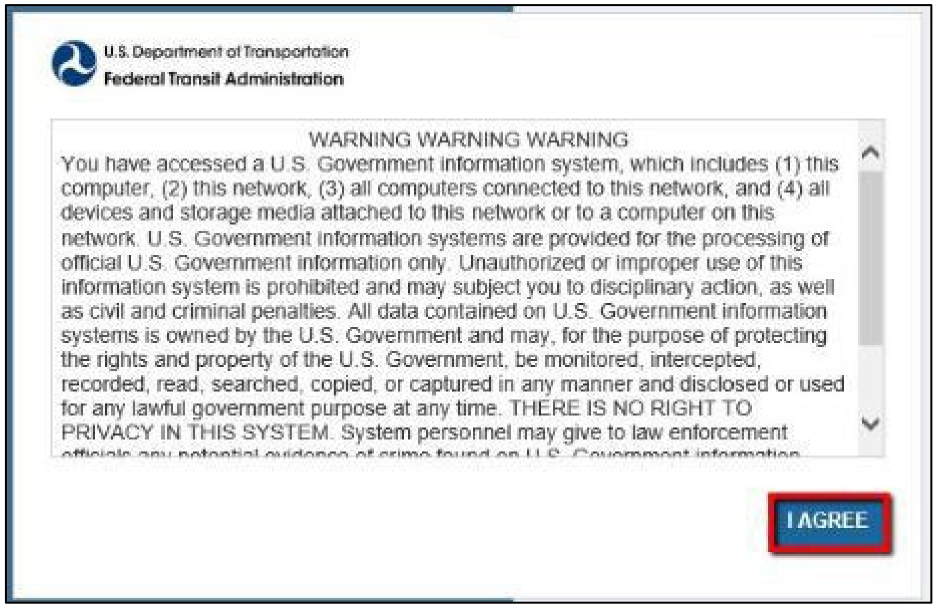


2.2.2 FTA Employee Login

FTA employees should access FACES via the FTA network.

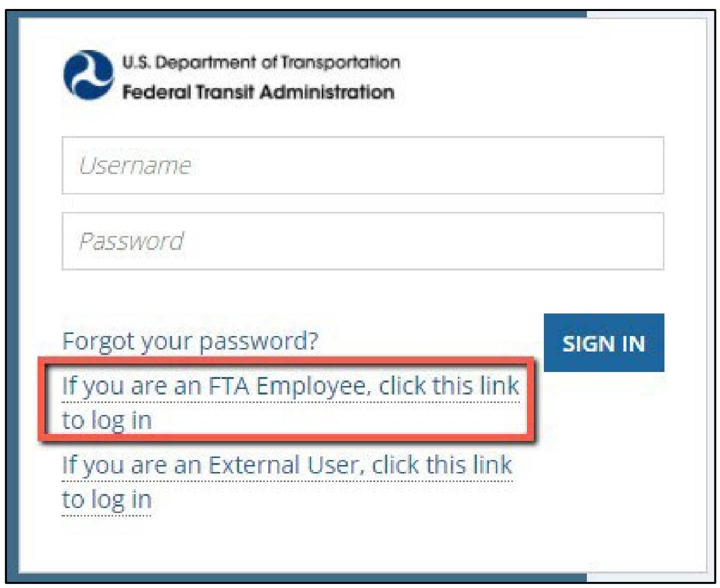
To log in:

1) Open a web browser and enter the FACES URL, https://faces.fta.dot.gov/.



2) Read the security policy and select ***I AGREE***.

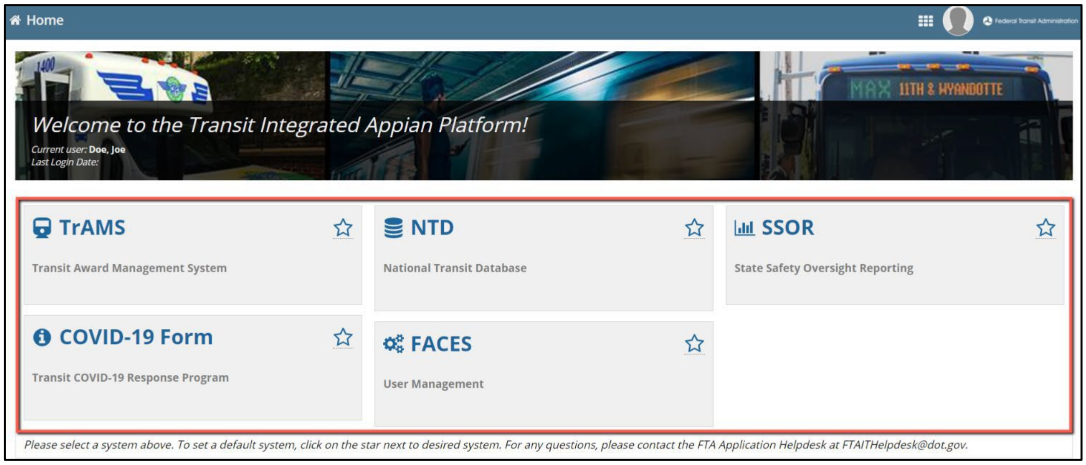
3) On the login page, select the ***If you are an FTA Employee, click this link to login*** link.



4) FTA Users will be automatically taken into the TrIAD Platform home page if they are in FTA network or logged into VPN.

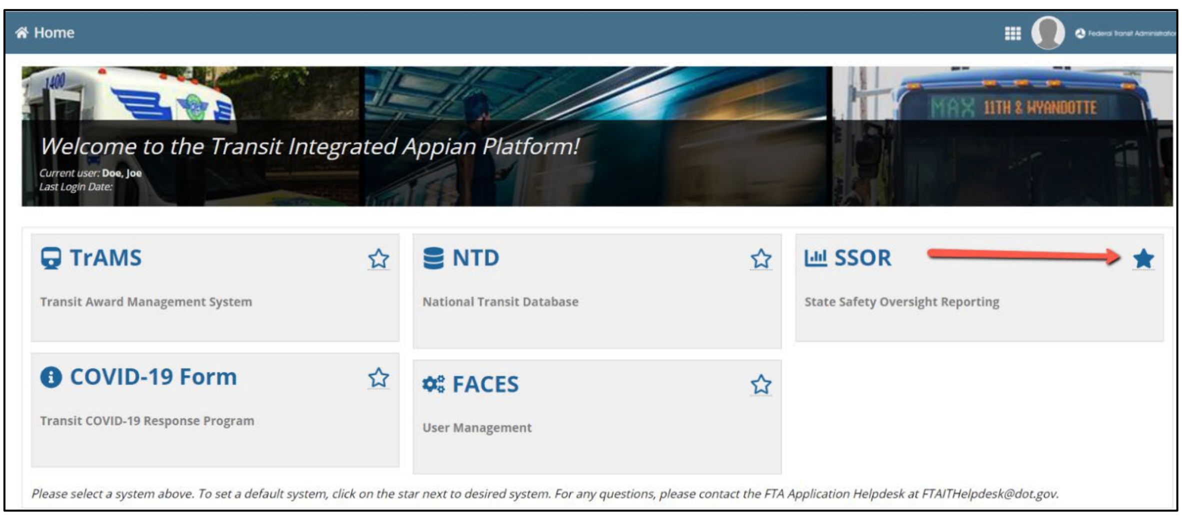
5) On the Homepage, the user has the option to click the system they wish to use. If the user has access to more than one FTA platform (TrAMS,

NTD, DGS, SSOR or FACES) all those options will be available as an option on the Homepage.



2.2.3 Setting A Default System

The Homepage has the option for a user to select an FTA System to become the default system they log into the next time the user logs in. This is done by clicking on one of the stars next to the system you wish to make your default.

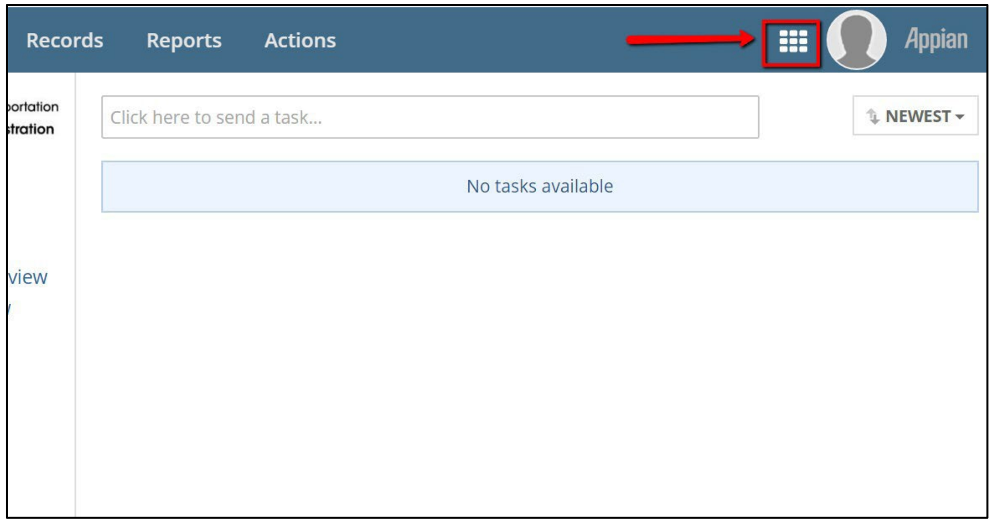


When a default system is selected, the next time a user logs in, they are taken to the default system and bypass the Sites Splash page.

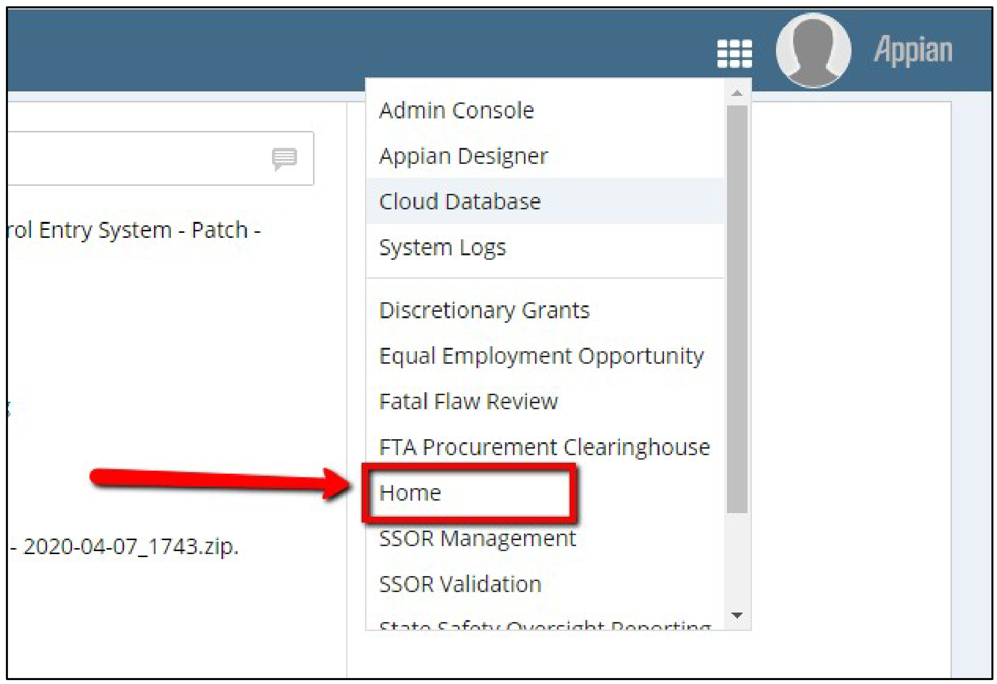
2.2.3.1 Changing User Default System or Return to Homepage

If a user wishes to change their default system to another system, they can do so by returning to the Homepage. To return to the home page,

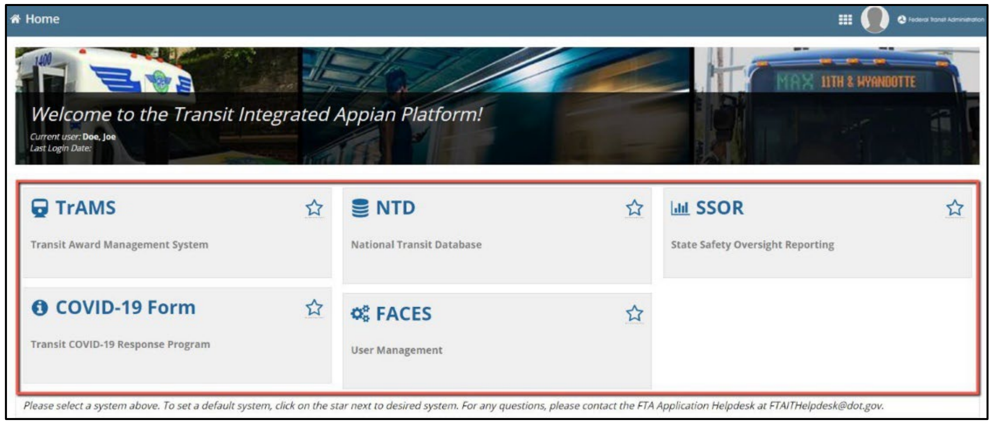
1) Click on the **NAVIGATION** button at the top right corner, next to the avatar.



2) In the drop-down menu, find Home and click on it.



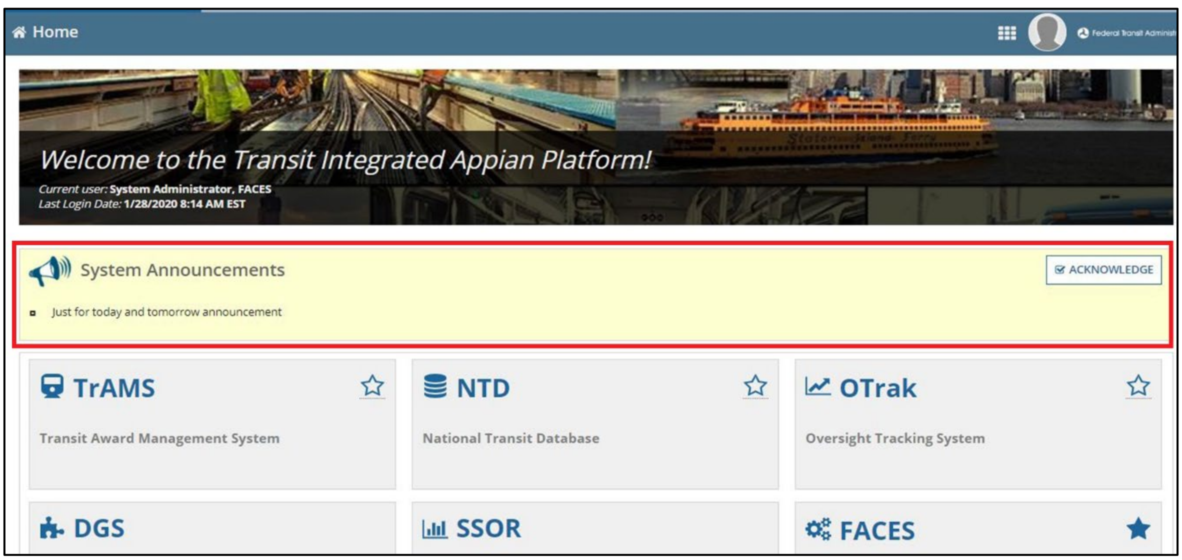
3) The user is taken back to the Homepage and can select another system to make a default system.



4) The next time the user logs in, they will then be taken to the new default system.

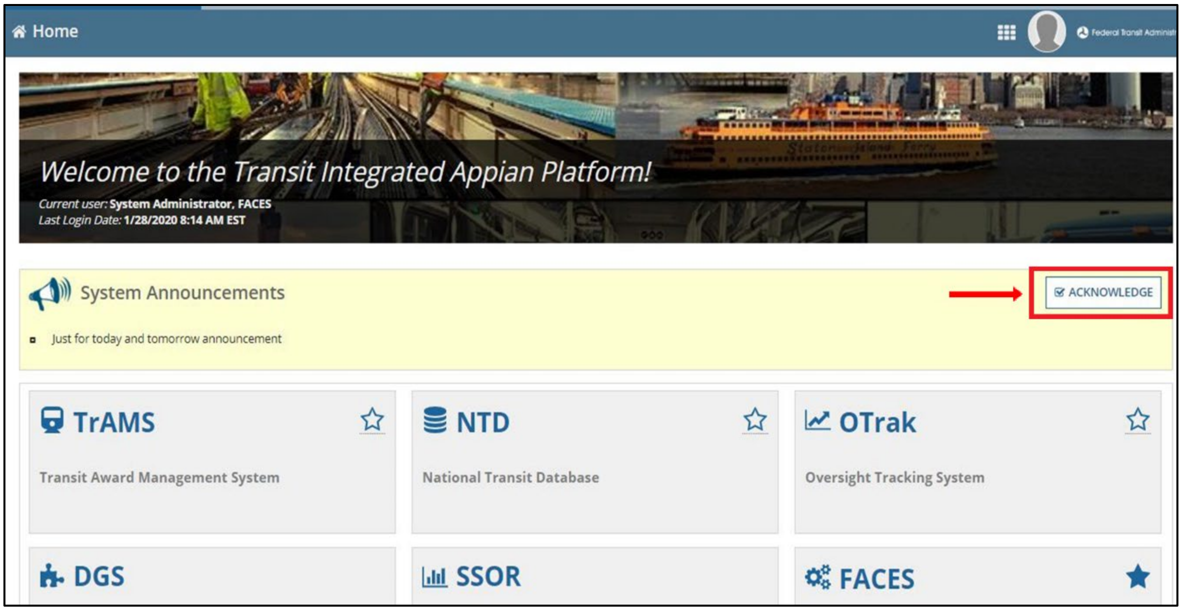
2.2.4 System Announcements

System Announcements are often needed to communicate to users about important information. When an announcement is created, it is posted in a yellow banner in the Homepage as shown below.



All users regardless of having set a default system (4.2.3 Setting A Default System) or not, will be redirected to the FTA Homepage when they log in. System Announcements will remain visible on the Homepage until they expire. The user can bypass being automatically directed to the Sites Splash page when they log in by acknowledging the System Announcement.

To acknowledge the System Announcement(s), click on **ACKNOWLEDGE** to the right of the banner.



The next time the user logs in, they are directed to their default system if they elected one. However, anytime there is a new System Announcement, the user will always be directed to the FTA Home page when they login until they have acknowledged the announcement.

2.2.5 Accessing User Record

A user can access their own profile in two different ways: from either the ***Account*** information area or through the ***Records*** tab.

To view your own **Profile** from the ***Account*** information area:

1) Select the down arrow next to the user's name to reveal the dropdown menu and click ***Profile***.

2) The user records **Summary Page** displays.

2.3. Account Information

2.3.1 Non-FTA User Setup

FACES stores user profile information such as name, username, address, contact information, security questions, and PINs. User information displays on the user's record as discussed in Section 6.4. Users can self-manage security questions and PINs (no other user can set up security questions or PINs for another user). Administrators and appropriate chain of command (e.g., User Managers) can modify specific user profile information and role assignment.

There are explicit rules controlling access to user information within the system:

1) FTA users cannot edit their **Profile** information (this is automatically handled via a nightly data sync with FTA systems).
2) Non-FTA users can edit all **Profile** information other than their username AND email address.
3) **User Managers** can edit **Profile** information for users in their organizations.
4) **Local Security Managers (LSMs)** can edit the user **Profile** of users in their FTA Regions/Cost Centers.
5) **Global Security Managers (GSMs)** can edit the user **Profile** of any non-FTA user in their system (e.g., a TrAMS GSM can manage the profile of any non-FTA user in TrAMS).
6) All users can self-manage their security questions and, if applicable, their PINs.

2.3.2 Account Settings

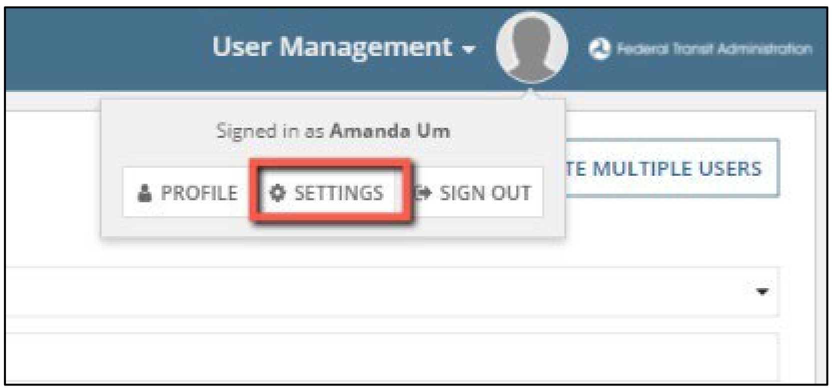
The account settings page provides a way for the user to manage their own preferred localized settings for date/time formats, language, and time zone.

Non-FTA users can also change their password via the settings page. The following settings can be adjusted:

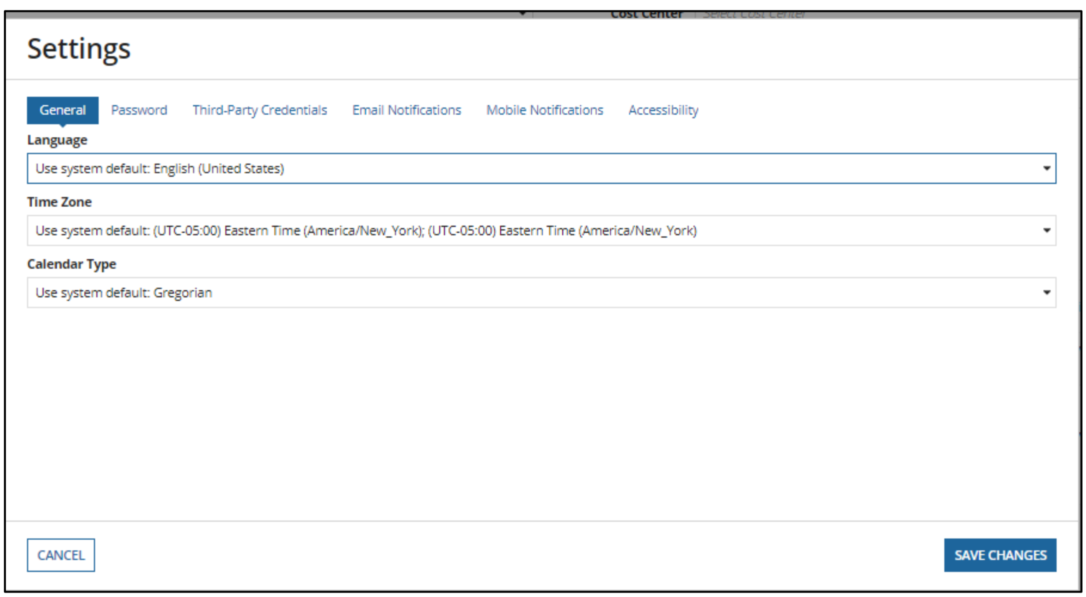
- Language
- Time Zone
- Calendar Type
- To access user account

Settings:

1) Select the icon (circular image) in the top right-corner of the screen to reveal a dropdown menu and click **Settings**.



2) The **General** tab displays.



3) Using the dropdown lists for Language, Time Zone, and Calendar Year, make whatever adjustments are necessary.

Note:	*At present, English is the only language available for selection.*

4) Click ***Save Changes*** to update the settings.

2.4. Passwords

Login Passwords are handled differently for FTA Employees and Non-FTA Employees. Please make sure to review the appropriate password related sections for FTA or Non-FTA Employees.

2.4.1 Forgotten Passwords (FTA Employees Only)

If the user has forgotten their password, they will need to contact 5-Help to rest their password.

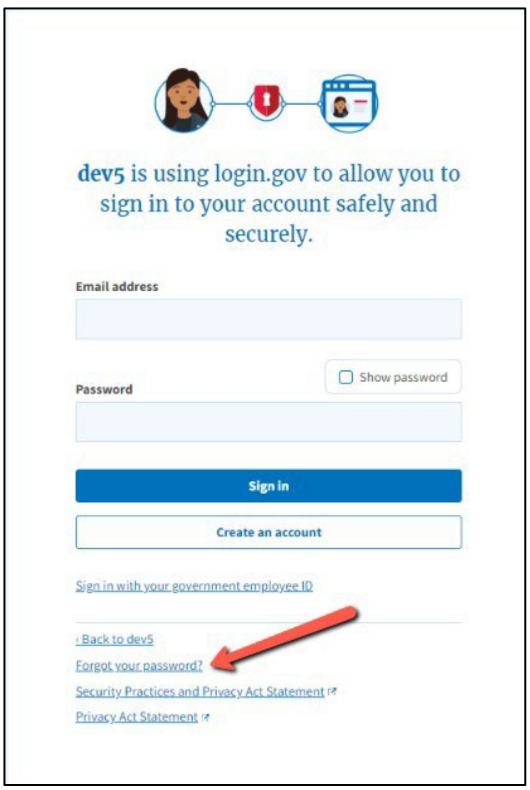
- **Internal:** 5-HELP (x5-4357)
- **External:** (202) 385-4357
- **Toll-free:** (866) 466-5221

2.4.2 Forgot Login.gov Password (Non-FTA Employees Only)

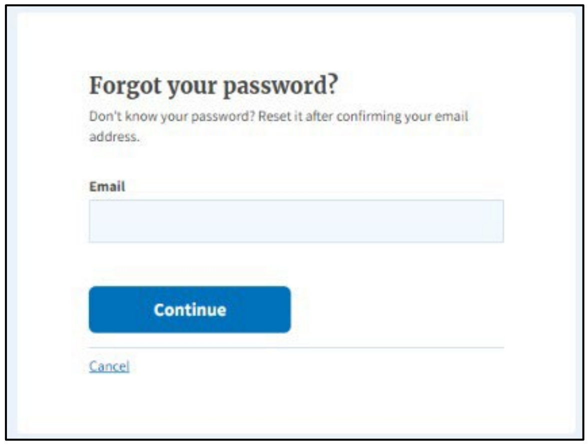
If a non-FTA Employee has forgotten their password, they can reset it by using a link on the Login.gov screen.

To reset a forgotten password:

1) On the Login.gov sign in screen, click on Forgot your password?



2) Enter the users email address and click Continue.



3) Look for an email "Reset your password" from Login.gov and click on Reset your password link in the body of the email.

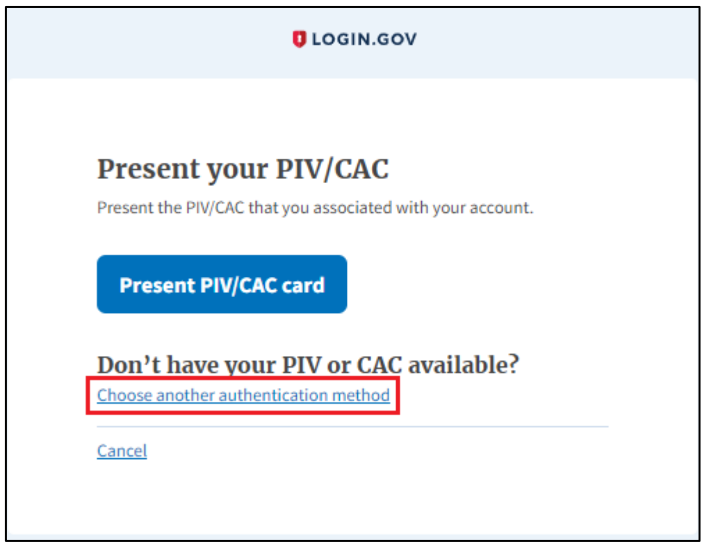
4) User is taken to Login.gov page to change the password, enter new password and click on Change password.

5) The user can sign in using their email and newly created password.

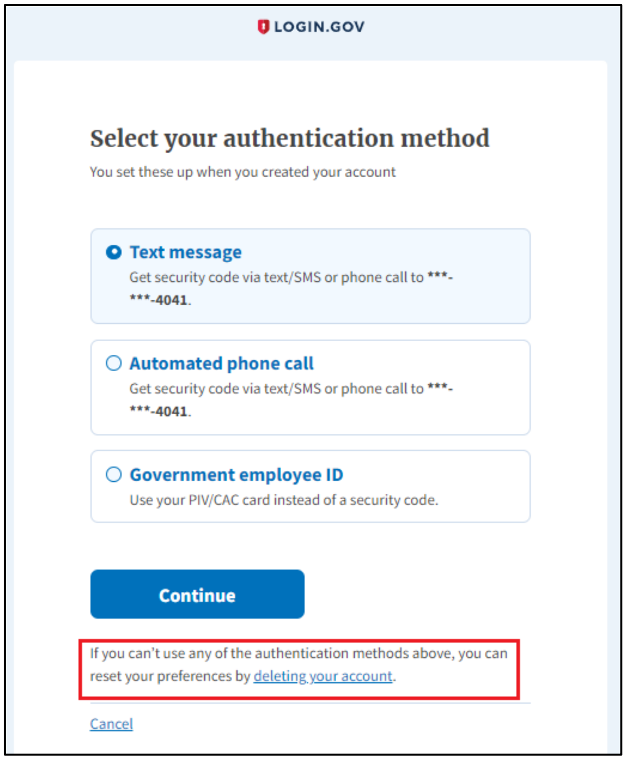
2.4.3 Reset Login.gov Account (Non-FTA Employees Only)

If a user is unable to login to Login.gov using their password and authentication method(s), they will need to delete their account. As a security measure, Login.gov requires a two-step process and 24-hour waiting period if you have lost access to your authentication methods and need to delete your account.

1) Sign in with your email and password.
2) On the authentication page (enter your security, app, or backup code; PIV/CAC card; or security key), click on "Choose another security option".



3) Scroll to the bottom and click on the "deleting your account" link.



4) Read through all the information carefully to make sure deleting your account is your only option.
5) Click on "Yes, continue deletion".
6) You will receive two emails.
   - The first email confirms Login.gov received your request. Your account is not yet deleted. Additional action is required.
   - The second email is sent to you 24 hours later. Follow the directions in that email to complete the deletion process.

3. System Layout

The software systems residing on the FTA Platform, https://faces.fta.dot.gov, all share a common layout. This section provides a high-level view of the system and how to navigate, find, and work with data.

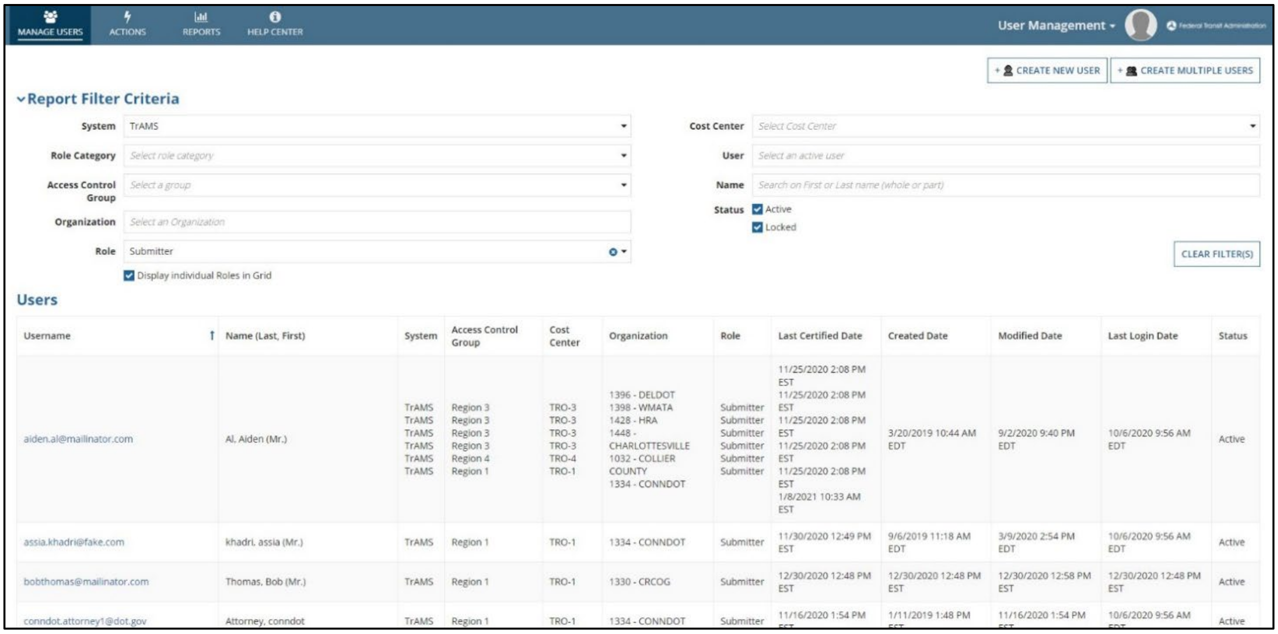
3.1. Account Information

Account Information provides access to information specific to the user. It lists the user's first and last name. By selecting the username, the user will be presented with the following three options:

1) **Profile** – Provides a means for the user to view and update their individual profile information, and to set their Personnel Identification Number (PIN). Refer to Section 4, for more details.
2) **Settings** – Opens the Settings Page where the user can select language and time zone and subscribe to news feeds. Non-FTA users can also change their password here.
3) **Sign Out** – Select ***Sign Out*** to log out and exit FACES.

3.2. Manage Users

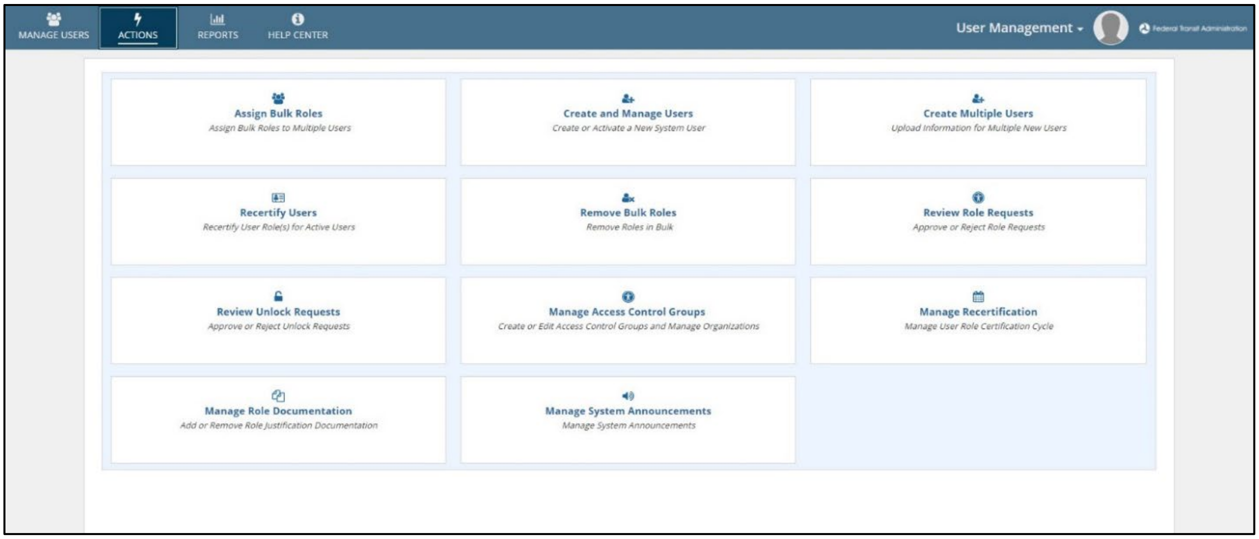
The **Manage users** tab provides access to view all users that the logged-in user is approved to see (generally, users within their same organization). More information on the content of user records is in Section 3.4 of this user guide.



Selecting a specific record displays a **User Summary Page**, containing detailed information associated with that selected user. The specific pages of the user record are discussed in Section 3.4.

3.3. Actions

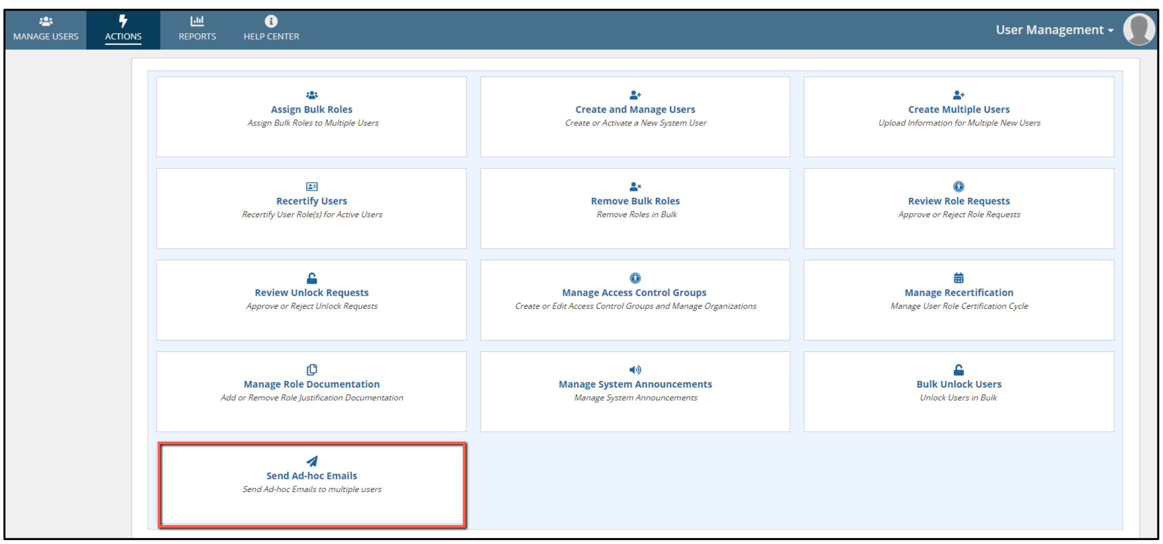
The **Actions** tab provides a list of actions that the logged-in user is approved to take within the system. In general, FACES actions are only visible to users with user management roles (e.g., User Managers, Local Security Managers, and Global Security Managers). In the case below, the User Manager is presented with a list allowing them to create and manage users (even multiple users), manage role documentation, review unlock requests, and perform searches for specific records. Users will see other actions specific to their roles in the other FTA software systems. The **Actions** available to any user are limited to their **role(s)**.



Selecting a specific Actions displays detailed information related to the Actions. The specific pages of the Actions are discussed in Section 6.5.

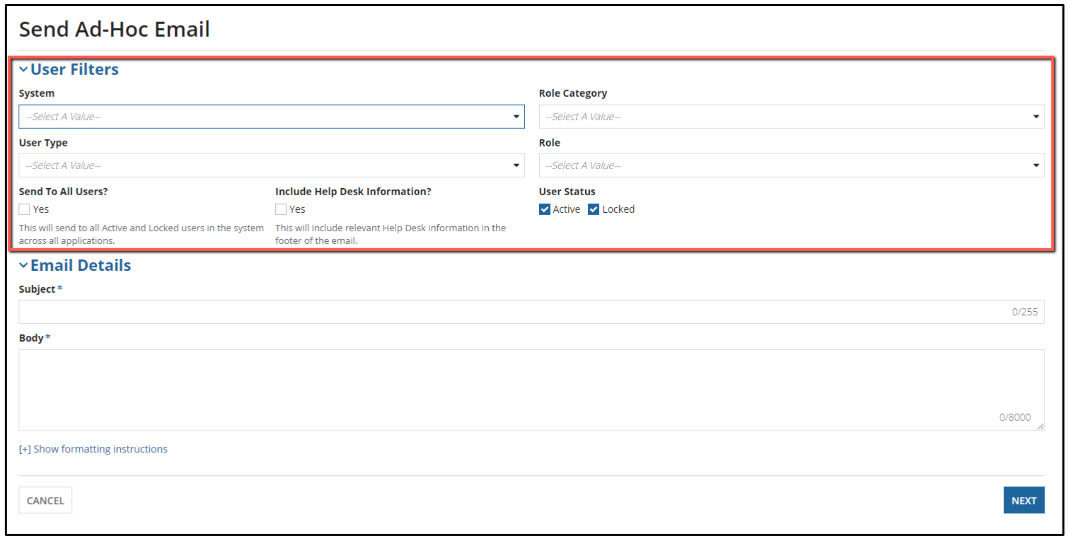
3.3.1 Action: Send Ad-hoc Emails (GSMs Only)

The Send Ad-hoc Emails action is available for all GSMs. This action can be used to send system-specific and user-specific emails for general information purposes.

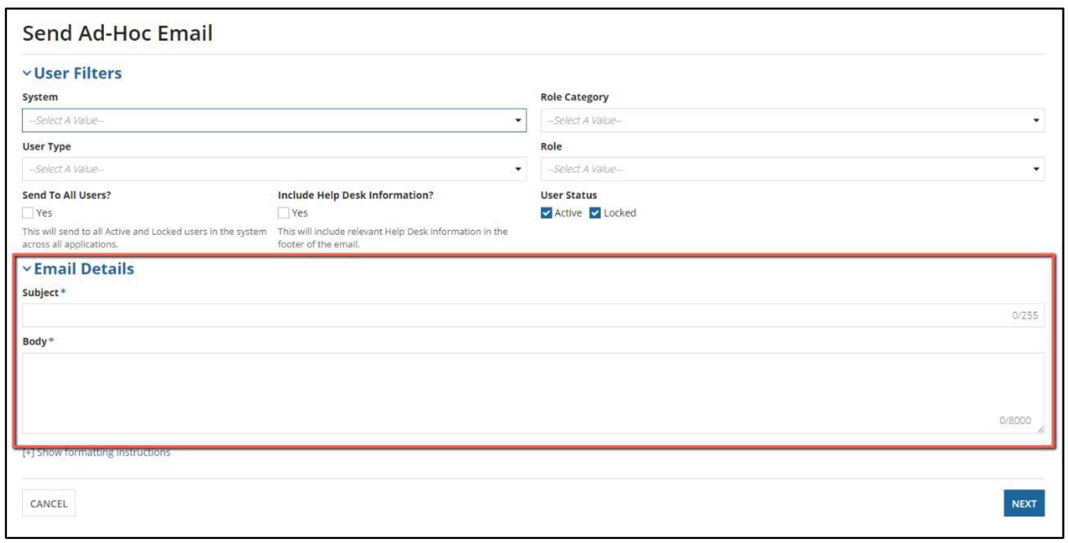


To create and send an Ad-hoc email:

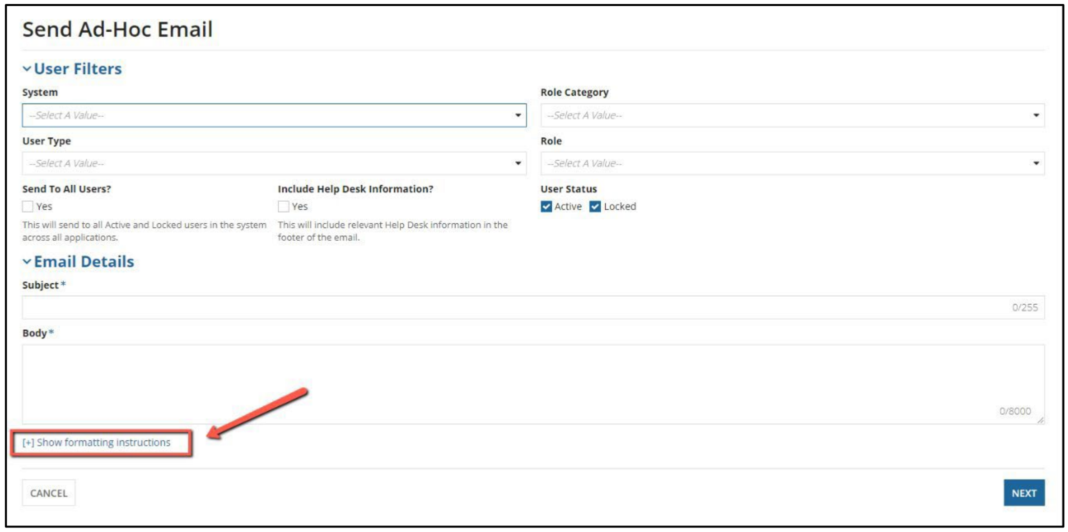
1) Under the Actions Tab click on Send Ad-hoc Emails.
2) On the next page the GSM can use the User Filters section to narrow down the audience for which the Ad-hoc email is intended for.



3) In the Emails Details section, the GSM enters the Ad-hoc email message.



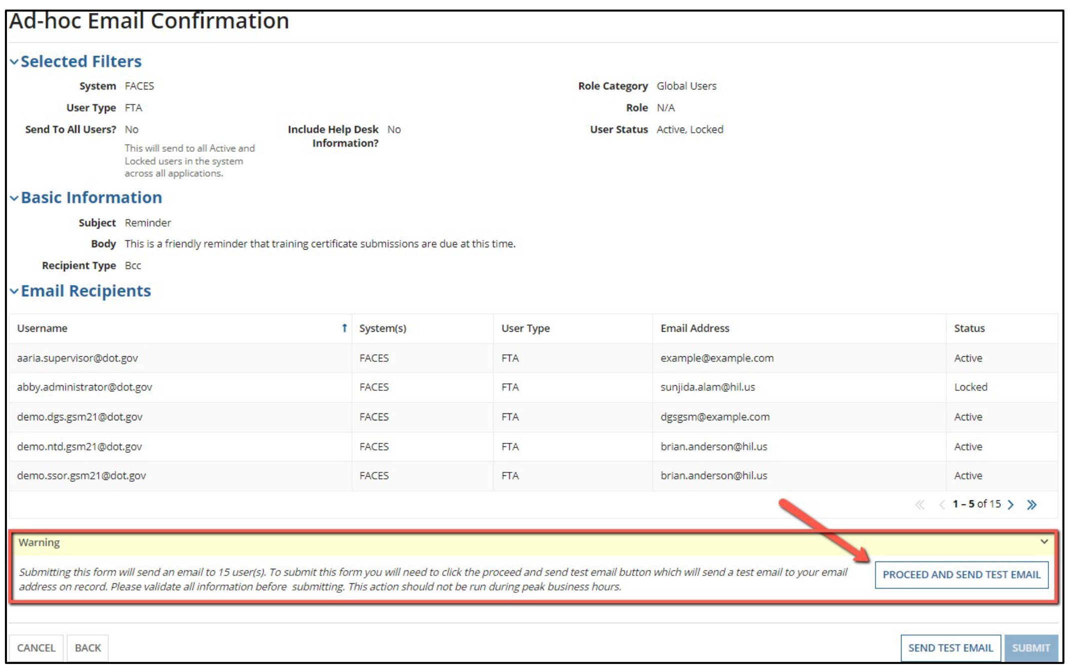
4) Additional formatting instructions are available by clicking on **[+] Show Formatting Instructions**.



5) After completing the email, click "Next" to go to the next screen.

6) On the confirmation screen, the GSM can review all the details pertaining to the ad hoc email.

7) Towards the bottom of the page there is a warning banner which will show the number of users to whom the ad-hoc email will be sent. The GSM may click on **Proceed and Send Test Email**. This will send the GSM a test email.



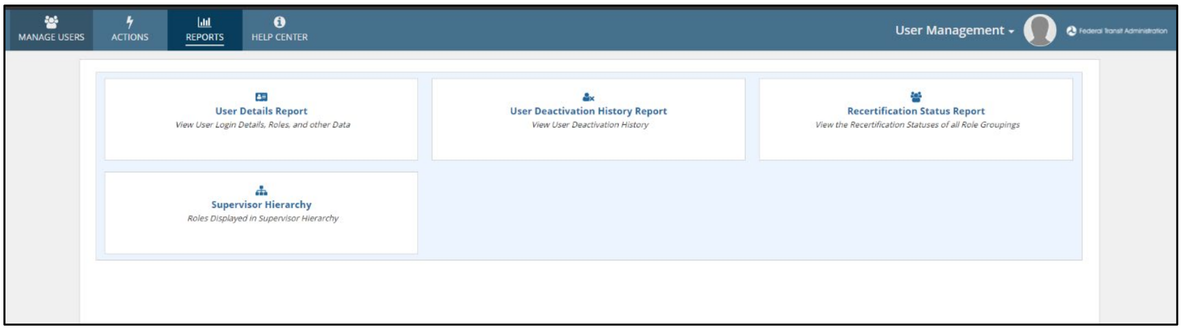
8) Any changes can be made to the email by clicking on Back.

9) When ready to send the final email, click on Submit.

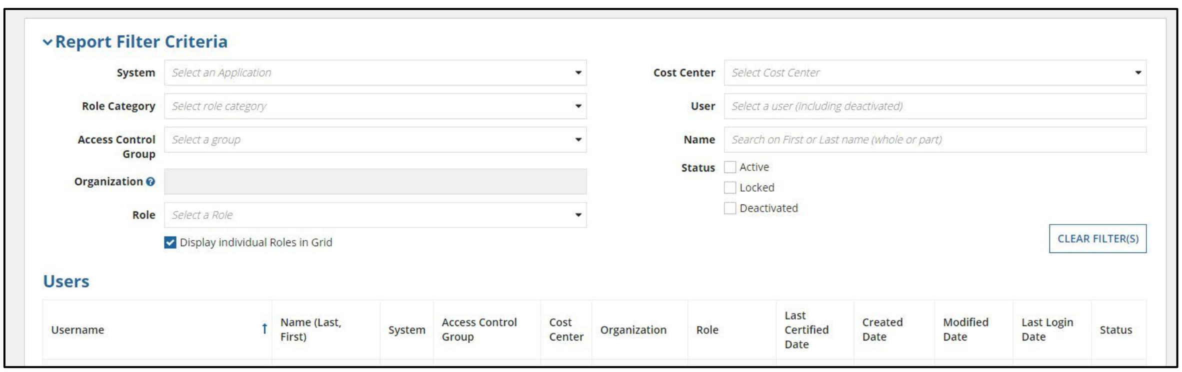
3.4. Reports

3.4.1 User Details Report

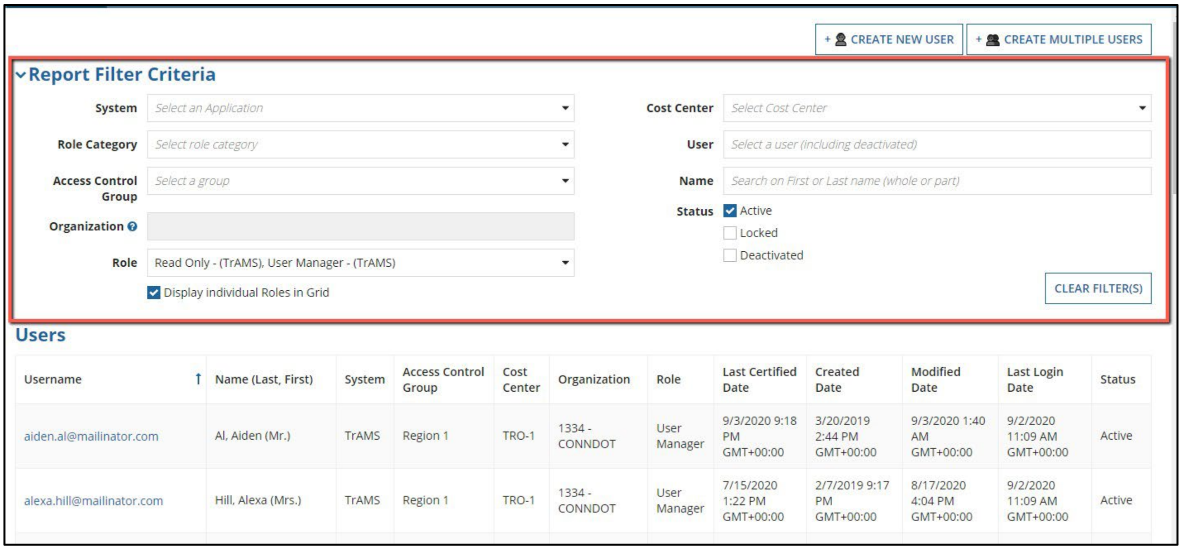
The **Reports** tab contains all reports that the user has access to. The purpose of this report is to provide a way to search for users by different characteristics. The logged-in user can only search for other users that he or she is approved to see (the same set of users that displays on the User records list in Section 3).



Selecting an individual report from the list will launch the report process that presents the finished report details to the page. Selecting ***User Details Report*** from above presents:

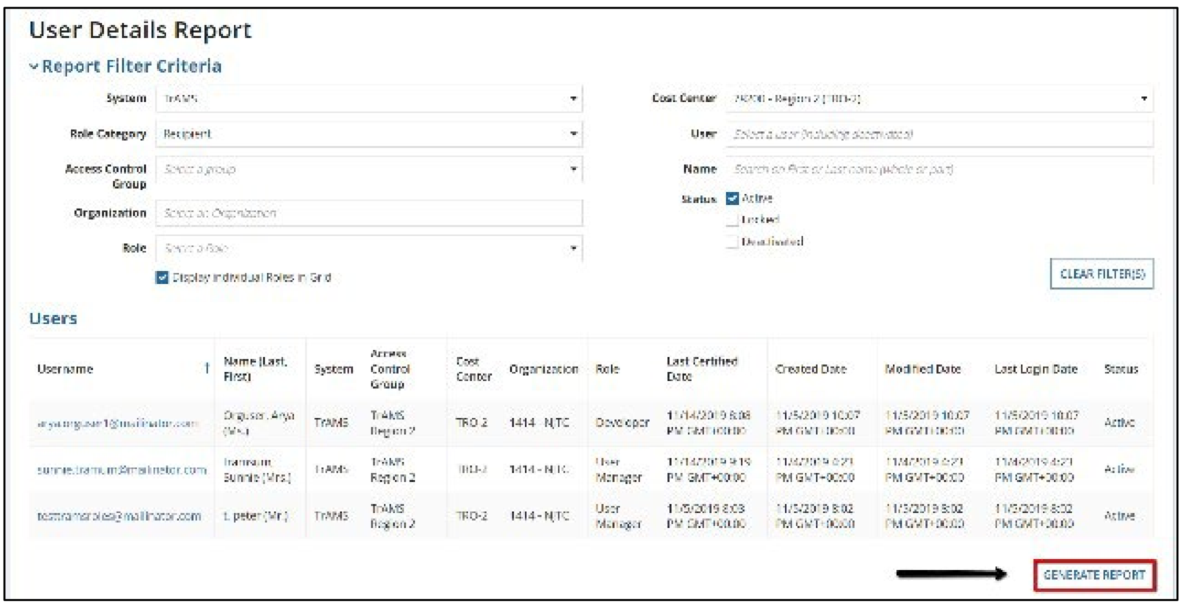


The report page provides several ways to filter the data presented. In most cases, the report filter is pre- determined by the logged-in user's characteristics (**Role Category**, **Access Control Group, Cost Center** and/or **Organization)**. The filter can be further limited by Username, or by partial name (first or last). The list can also be filtered by users who are **Active**, **Locked**, or **Deactivated**.

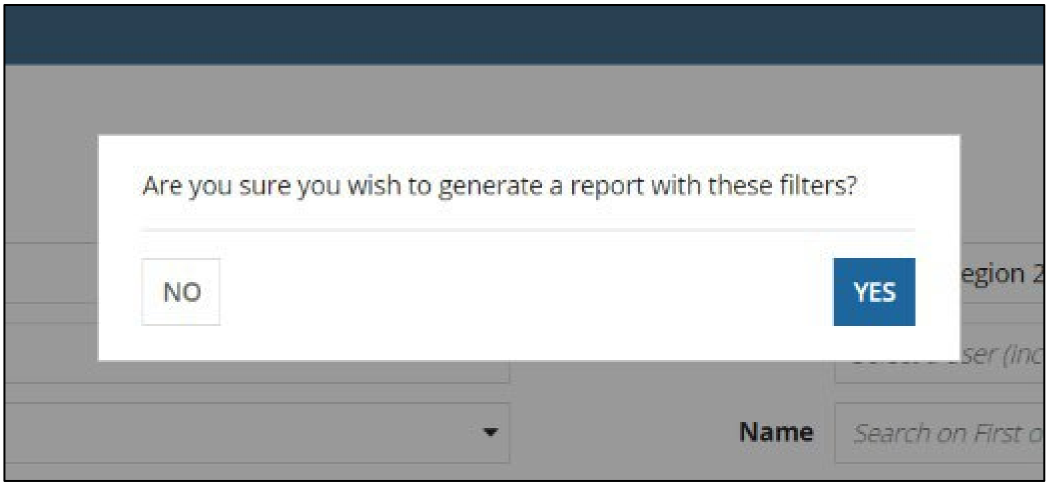


To return to the full list, select ***CLEAR FILTER(S).***

Clicking ***GENERATE REPORT*** will execute a process to create an Excel spreadsheet of details.



A prompt will pop up asking to verify to generate a report with the current filters.



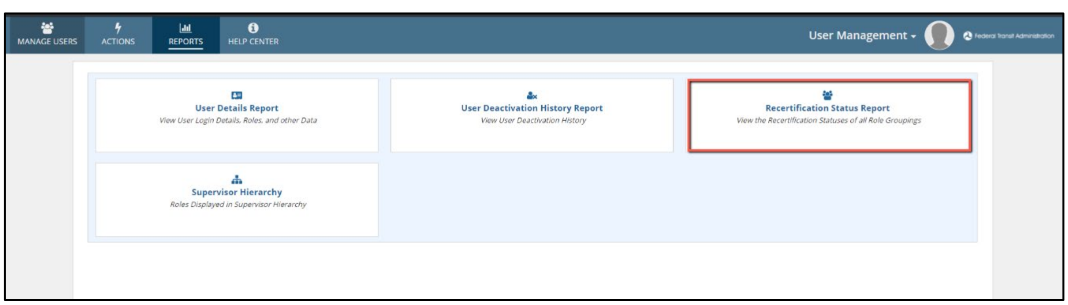
Clicking the link to the report (***User Details Report***) will create a task with a download link. Once opened, the Excel spreadsheet presents separate data pages based on the details selected.

3.4.2 Recertification Status Report

After the end of each recertification window, FACES will generate a recertification status report, accessible by Global Security Managers and Local Security Managers only (*see Section 8.1 for* Recertification Process*)*.

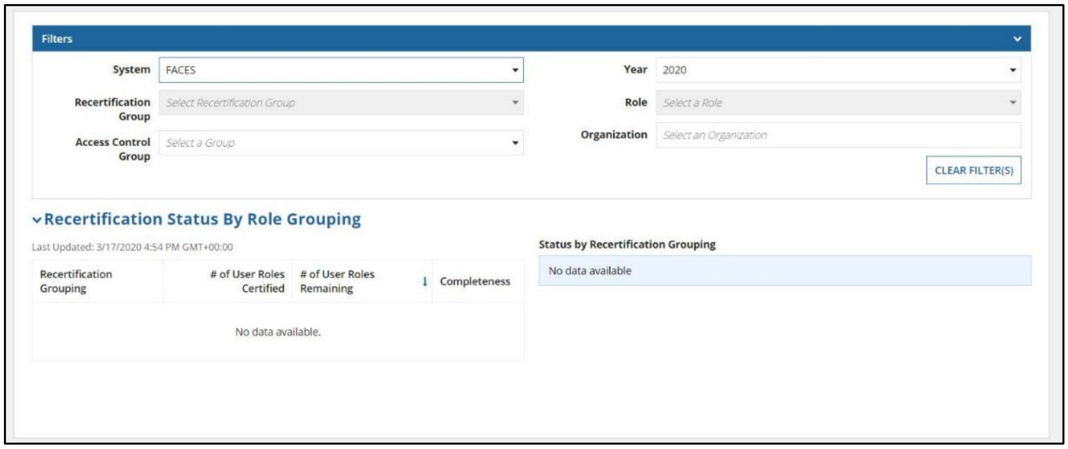
How a **Certifier** can view recertification status report:

1) **Certifier** log into System and clicks Reports.
2) User clicks ***Recertification Status Report***.

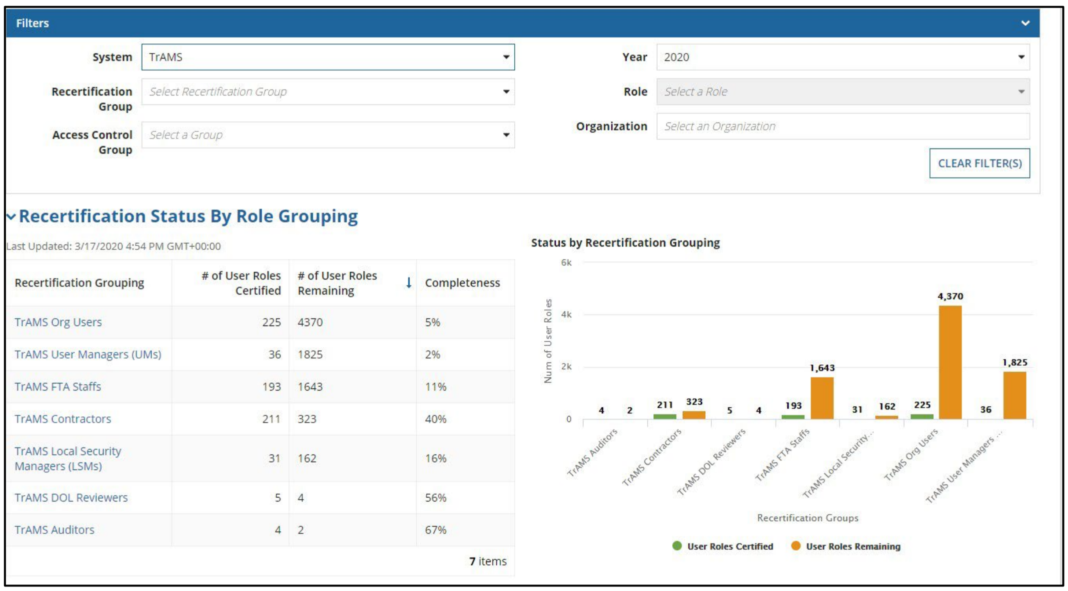


3) The **System** displays Recertification Status Report.

4) The **Certifier** has the filtering options by systems, year, role, recertification group, organization, and access control group.

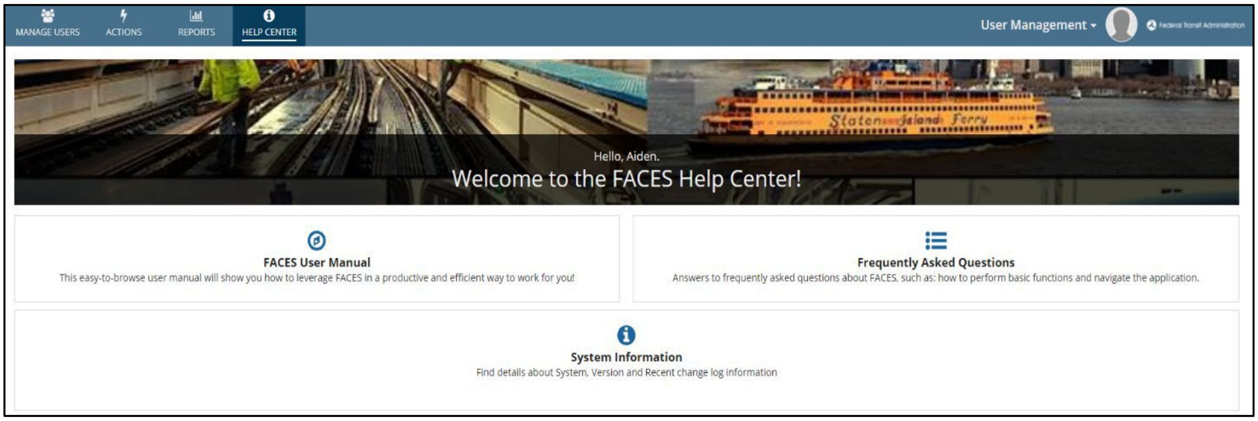


5) The **Certifier** can see recertification status by role grouping.



3.5. Help Center

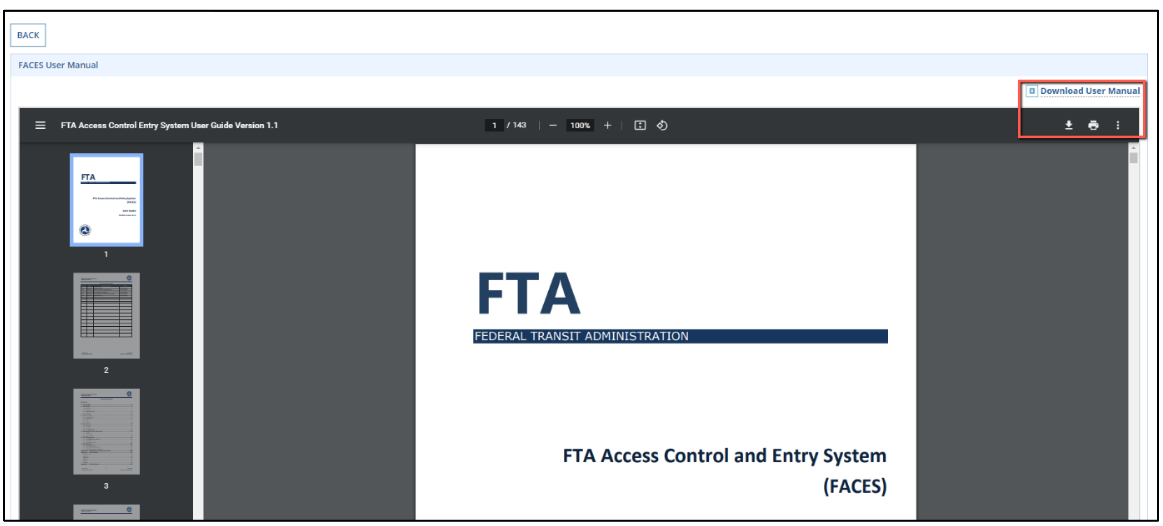
The **Help Center** tab contains the FACES User Manual, Frequently Asked Questions (FAQs), and System Information.



3.5.1 FACES User Manual

To access the User Manual/User Guide, click on FACES User Manual.

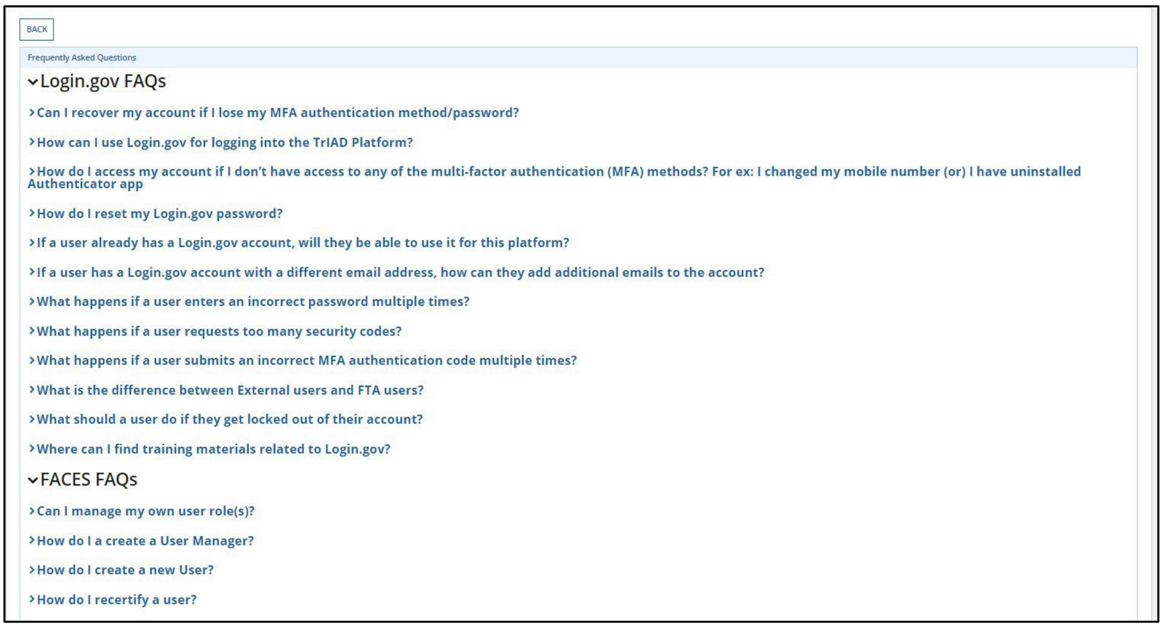
On this page the user can view it directly, download, or print it out.



3.5.2 Frequently Asked Questions

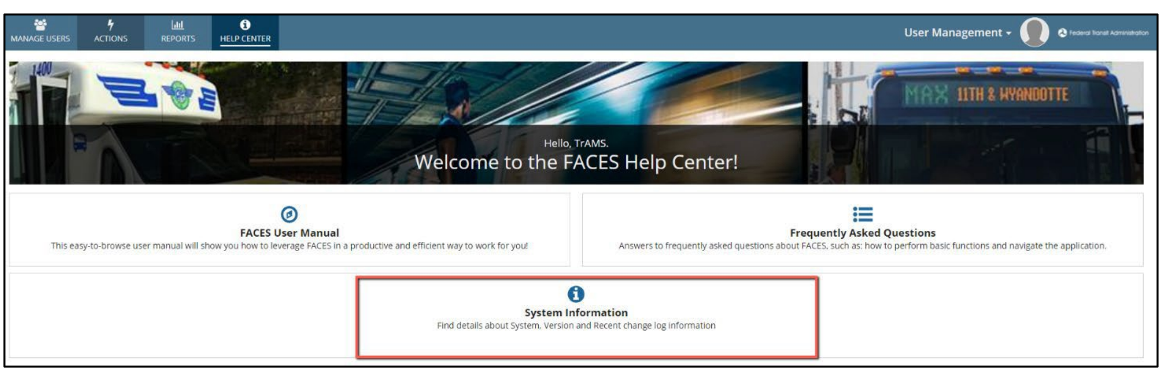
Users can click on Frequently Asked Questions to review helpful answers for questions that are frequently asked.

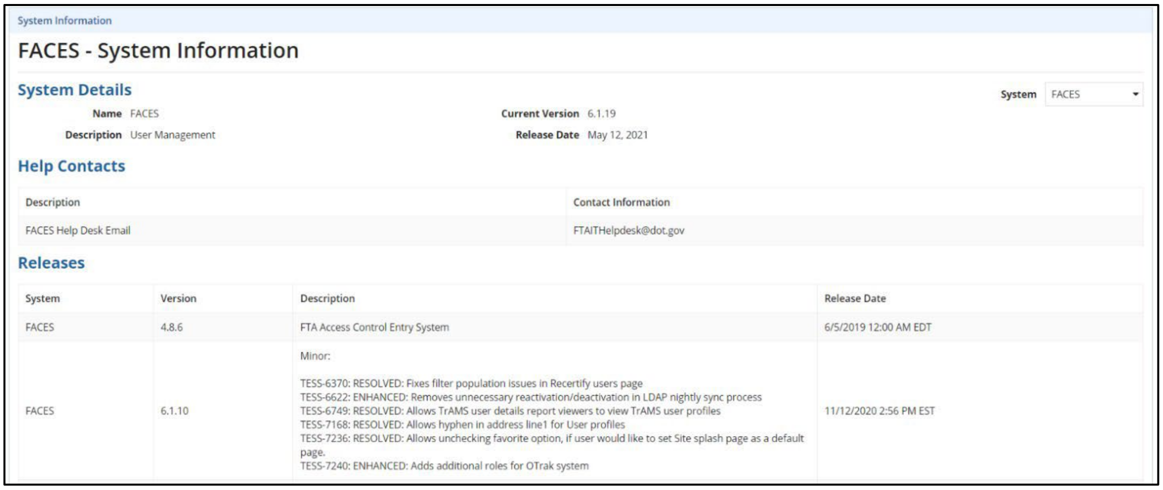
Responses for each question can be expanded by clicking on a question.



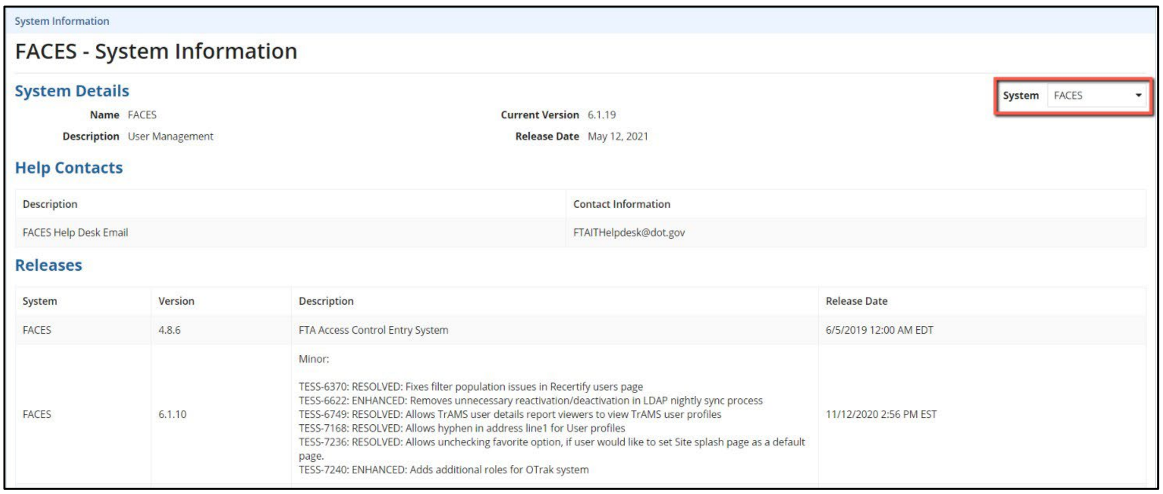
3.5.3 System Information

System Information allows a user to view information on the latest version of the system and provides Help Desk information to the user should they encounter any issues with FACES.





Users with access to multiple systems can use the drop-down feature to view system information for other systems they have access to.



4. System Users

A User Record includes all information directly related to the user's **Profile** (e.g., name, address, title, and role(s), audit history). It also includes all news items specific to the user and any Kudos received. Users may see other staff members' **User Summary** page and **User Details** within their organization.

Each user may manage their own **Profile** information. Some user information may be edited by the individual user. User roles are granted and managed by **User Managers, Local Security Managers (LSMs), and Global Security Managers (GSMs)**.

4.1. User Types

There are three account types used to classify each user on the FTA platform: FTA users, Organization users (e.g., TrAMS Recipient, DGS Recipient and NTD Reporter), and External users.

1) **FTA Users:** This user type includes FTA employees and federal contractors who directly support FTA. All FTA users have FTA email accounts ending in @dot.gov.
2) **Organization Users:** This user type includes individuals who are employed by or support an organization that uses an FTA platform software system. The users are grouped by their organization(s). This user type includes TrAMS Recipients, DGS Recipients, and NTD Reporters.
3) **External Users:** This user type includes individuals external to FTA but provide support or oversight to one of the FTA platform software systems. External users have three sub-types: Auditors, Contractors, DGS DOT users and Department of Labor (DOL) users.

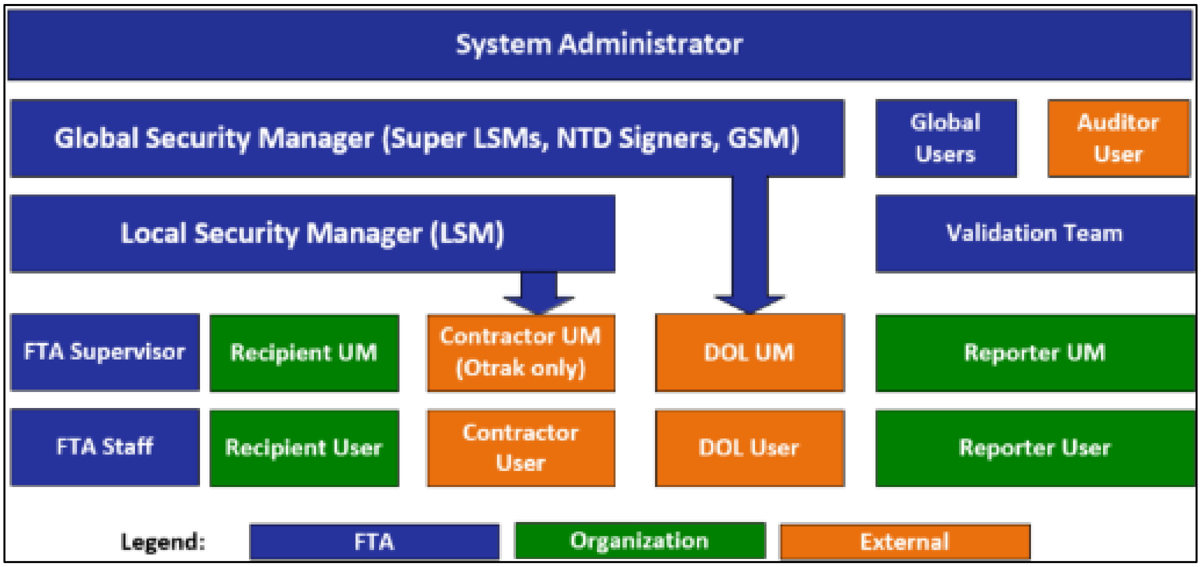
The types of roles that a user can be granted are specific to the user's account type. FACES defines standardized role types, role hierarchy, and security for the various software systems on the FTA platform. New roles and user categories may be incorporated as needed in the future to allow FACES to support additional software systems and to meet changing requirements.

4.2. User Roles

User roles on the FTA platform are grouped by role category (e.g., FTA Staff, TrAMS Recipient Users, TrAMS Reporters and DGS Recipient Users).

Each organization user has an assigned ***User Manager***. The **User Manager** assigns roles to each user in their organization in accordance with the rules specific to their FTA software system (e.g., TrAMS, NTD, SSOR, etc..). Users may be assigned one or multiple roles within their organization. Roles assigned to each user control the **Actions** available to a user and the **Tasks** assigned to the user.

The image below provides an outline of all user roles within the FACES landscape. Each will be further defined in subsequent paragraphs.



The following tables lists the available user roles that may be assigned. For definitions of each role and associated privileges, please see the corresponding system user guide.

	Organization User Roles	**FTA User Roles**	**External User Roles**
NTD Reporters	1) CEO 2) CEO Delegate 3) Editor 4) NTD Contact 5) Safety Contact 6) Safety Editor 7) Safety Viewer 8) User Manager 9) Viewer	System Administrator 1) System Administrator Global Roles 1) FTA Signer 2) FTA Viewer 3) Global Security Manager (GSM) 4) Global Viewer 5) User Details Report Global Viewer FTA Staff 1) Local Security Manager (LSM) Validation Team 1) Validation Analyst 2) Validation Ops 3) Validation PM 4) Validation QA	1) Auditor
TrAMS Recipients	1) Attorney 2) Civil Rights 3) Developer 4) FFR Reporter 5) JPC Procurement Officer 6) MPR Reporter 7) Official 8) Read Only	System Administrator 1) System Administrator Global Roles 1) Global Security Manager (GSM) 2) Global Viewer 3) TrAMS Help Desk 4) User Details Report Global Viewer FTA Staff	Auditor 1) Auditor DOL User 1) DOL Reviewer 2) DOL User Manager Contractors 1) Contractor

	9) Submitter 10) User Manager	1) Administrator 2) Apportionment Manager 3) Budget Analyst 4) Budget Director 5) Civil Right Officer 6) Dataset Administrator 7) DBE Approver 8) Director 9) Director of Operations 10) Discretionary Admin 11) Discretionary Manager 12) Environmental Reviewer 13) Initial Reviewer 14) Intake Manager 15) Legal Counsel 16) Local Security Manager (LSM) 17) Post-Award Manager 18) Pre-Award Manager 19) Read-Only 20) Reservationist 21) Supervisor 22) TCA Recorder 23) Technical Reviewer 24) Transit Director 25) Vendor Setup	
DGS		System Administrator 1) Administrator Global User 1) Global Security Manager (GSM) 2) Global Viewer FTA Staff 1) DGS FTA – Fatal Flaw Reviewer 2) FTA Staff Read Only 3) Local Security Manager (LSM) 4) Management 5) Program Admin/Manager 6) Reviewer 7) Team Lead	Auditor 1) Auditor DOT User 1) DGS External – Fatal Flaw Reviewer 2) External Read Only 3) Reviewer Non-DOT User 1) External Reviewer

SSOR	1) Alternate Reporter 2) Primary Reporter 3) User Manager 4) Viewer	System Administrator 1) System Administrator Global Roles 1) Global Security Manager (GSM) 2) Global Viewer 3) Program Management Lead FTA Staff 1) Director 2) Local Security Manager (LSM) 3) Program Management Team Member 4) Regional Safety Officer 5) Validation Lead 6) Validation Team Member	Auditor 1) Auditor DOT User 1) External Validation Team Member
CRM		System Administrator 1) System Administrator Global Roles 1) Global Security Manager (GSM) 2) FTA Users 3) Global Viewer	

OTRAK	1) Recipient User 2) User Manager	Administrator 1) System Administrator Program Admin 1) Program Administrator Global Users 1) Global Security Manager (GSM) 2) Global Viewer FTA Staff 1) Local Security Manager (LSM) HQ Staff 1) Civil Rights Officer 2) FMO Program Manager 3) HQ User 4) OAT Program Manager 5) PSR Program Manager 6) Single Audit HQ Program Manager 7) SMR Program Manager 8) SSO Audit Program Manager 9) TCR Program Manager 10) TR Program Manager 11) Tribal Transit Program Manager Region 1) Region Read-only 2) Region User 3) Regional Oversight Director 4) Regional Tribal Liaison 5) Single Audit Regional/Program Office Point of Contact	External Auditor 1) DOT User External Read Only 2) OIG Auditor (Read-only) Contractor 3) CTR Program Manager 4) CTR Recipient Delegate 5) CTR Regional Delegate 6) CTR Reviewer 7) CTR User Manager HQ Staff CTR Delegate 8) CTR Review Requirement Editor
COVID-19	1) CEO 2) NTD Contact 3) Editor 4) Viewer 5) Safety Contact 6) Safety Editor 7) Safety Viewer 8) CEO Delegate		

ECHO-Web	1) Grantee 2) Read Only 3) Approving Official	Global Users: 1) Global Security Manager (GSM) 2) Global Viewer FTA Staff: 1) Local Security Manager (LSM)	

Table 1 – Organization User Roles

4.2.1 User Visibility

There are explicit rules controlling access to user records and user information within the system. The following rules independently to each FTA system (e.g., TrAMS, NTD):

1) Organization users can see all other users within their organization(s). For example, a user who belongs to 'Transit Organization Blue' will see all other users with roles in 'Transit Organization Blue'.
2) Organization users cannot see FTA user records, external user records, or users outside their organizations.
3) FTA users can see all other FTA users within their system (e.g., TRAMS, NTD, DGS).
4) FTA users can see all organization users who belong to organizations within their FTA region or cost center. Global FTA users can see all organization users within their system (e.g., TrAMS, NTD, DGS).
5) FTA users with specific roles (e.g., GSM, validation analyst, LSM) can view external user records.
6) External users can only see user records for other external users of the same subtype. For example, TrAMS DOL users will only see other DOL users in TrAMS.

The following table summarizes these rules from the perspective of the logged-in users type:

	User Records I Can View		
My User Type	Organization	FTA	External
Organization	All organization users within my own organization(s).	No FTA user records.	No external user records.
FTA	All users belonging to organizations within their FTA cost centers. A global user sees all organization users within his/her system (e.g., TrAMS).	All FTA users within the user's system (e.g., NTD, DGS).	See some external user records depending on roles assigned.

External	No organization user records.	No FTA user records.	All users of same external subtype (e.g., Auditor) in my approved systems (e.g., TrAMS, NTD, DGS).

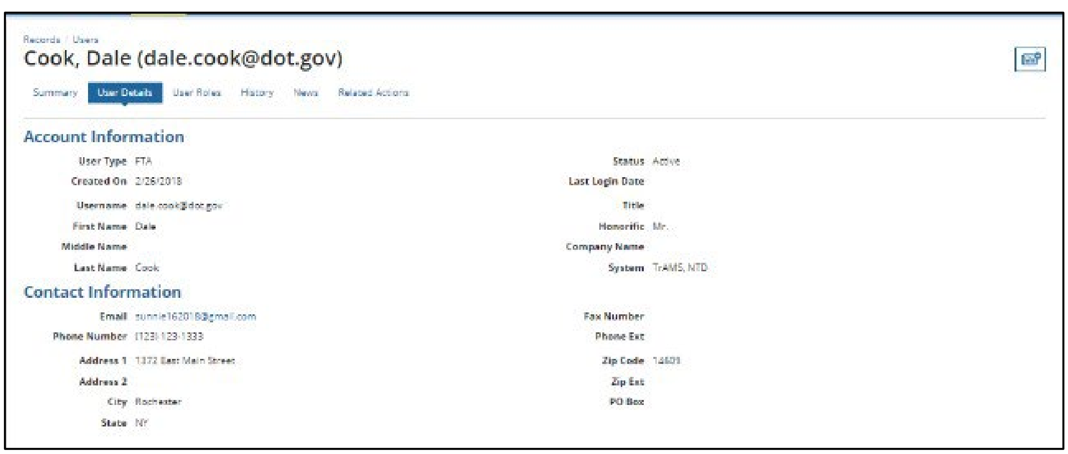
Table 2 – User Record Viewing Privileges

4.2.2 User Record Content

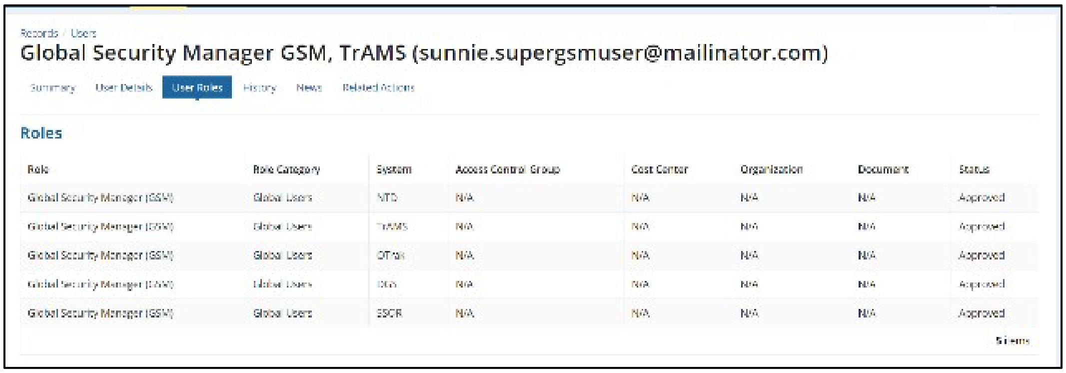
Each user's record opens to a user ***Summary*** page.

User record content is split between multiple pages. Each user's record contains:

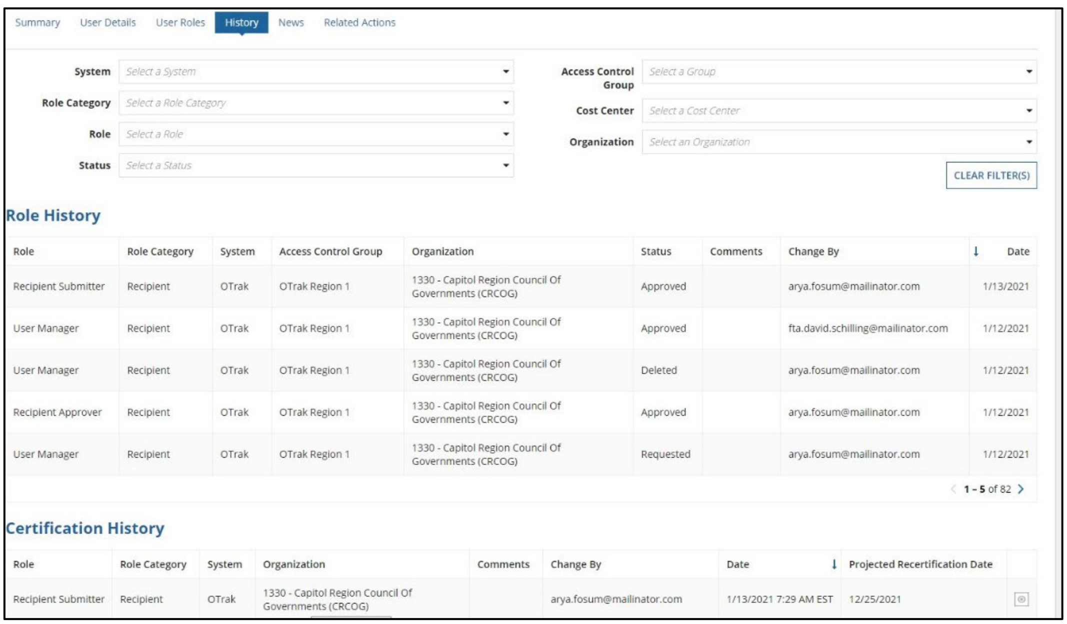
1) A ***User Details*** page visible to all users who have access to that user's record. The ***User Details*** page contains the user's account and contact information (e.g., first and last name, email, user type, and account status).



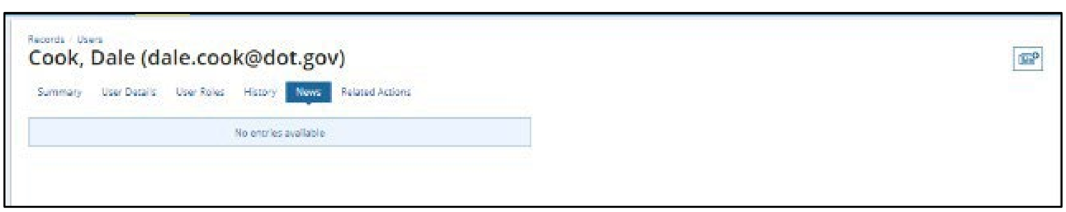
2) A ***User Roles*** page visible to all users who have access to that user's record. The ***User Roles*** page contains a grid of the user's active **Roles** and current **User Managers**.



3) A ***History*** page visible to each user and their management chain (User Managers, Validation Analysts, LSMs, GSMs). This ***History*** page contains an audit trail of changes to the user's **Profile** and **Roles**. Users can filter role history using the following filters: System, Role Category, Status, Cost Center, Organization and Role.



4) The ***News*** tab shows a listing of user activity with the most recent news displayed first.



5) The ***Related Action*** page contains any actions the viewing user is allowed to perform on the record. On this page, the user can manage their **Profile**, **Security Questions**, and **PIN**.

For detailed information about these user record pages, please reference Section 6.4.

5. Managing the User's Own Record

5.1. Related Actions

By selecting ***Related Actions*** users will be provided with additional options that can be performed on their **Summary** page.

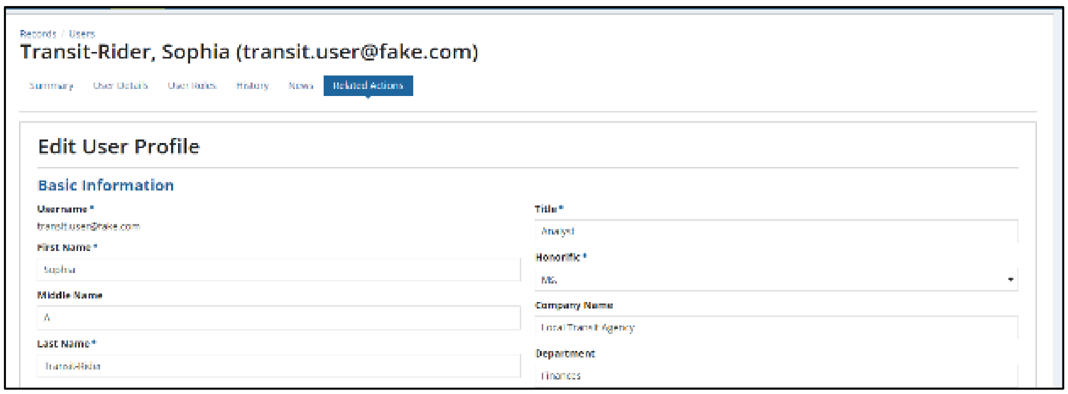
5.1.1 Related Action: Edit Profile

All non-FTA users can edit their own user profile (name, contact information, and business address) using a profile related action. The only profile information users cannot self-update is their username and email address. FTA users cannot edit their profile information because their information is provided to FACES by a nightly information transfer from FTA's internal systems. If an FTA user's information is incorrect, the information must be updated in FTA's internal systems.

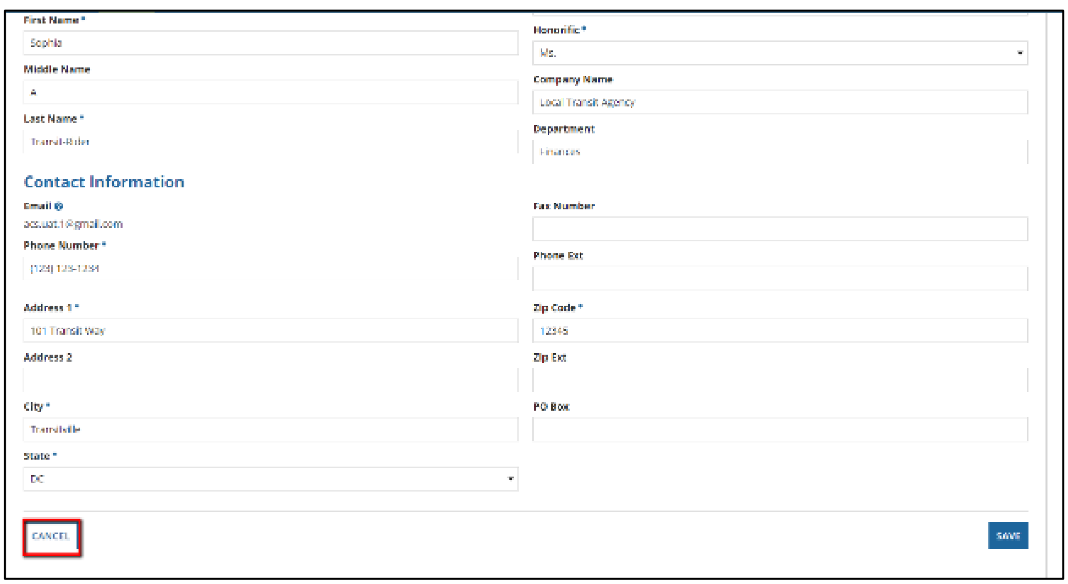
To edit the user's profile:

1) Locate the **User Profile** through either the **User Settings** page or the **Records** page.
2) Select ***Related Actions***.
3) Click ***Edit Profile***.

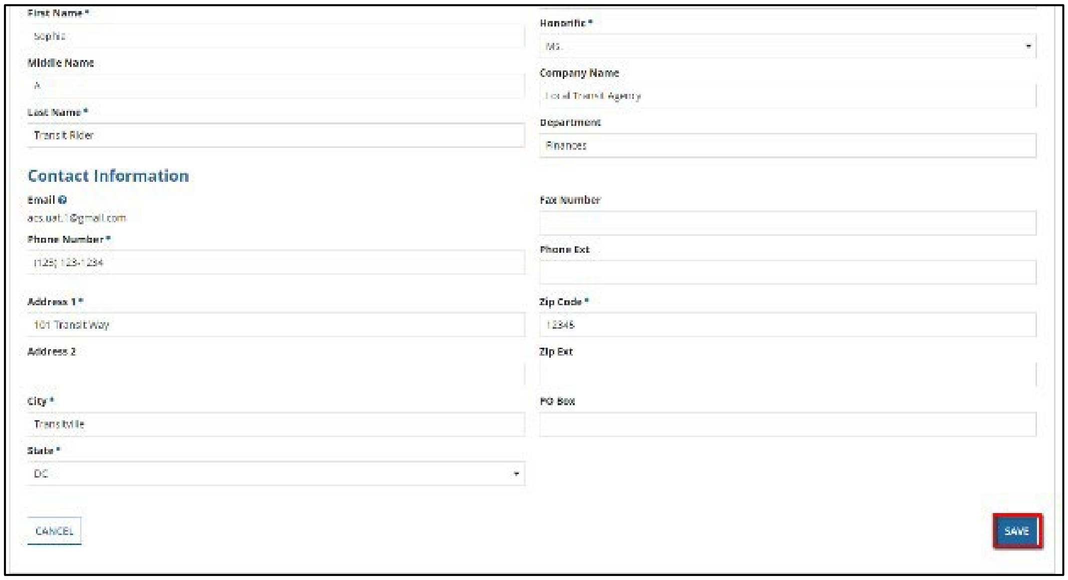
4) The **Edit User Profile** page will display all previously saved user-associated details in editable fields.



5) Click ***Cancel*** to return to the **Related Actions** page without saving any changes.



6) Update any of the data fields as needed and then click ***Save*** to save all details. Required fields are marked with an asterisk * on the form. If required fields were missing from the previous FACES version, you will be required to add this information to save any other updates.



7) Selecting ***Save*** will execute a validation script to ensure that all data entered matches pre-determined rules (e.g., the PO Box field cannot contain any letters). Once the data is validated, the information is saved and the **Related Actions** page displays. The system will briefly display (within the header area of the Related Actions page) a message that the *Action Completed Successfully*, indicating that all of changes were accepted.

5.1.2 Related Action: Set Security Questions/Answers

New user accounts are automatically assigned a **Task** to set up an initial set of **Security Questions and Answers (Q&As)** to ensure the security of the account and to provide a mechanism to re-establish access when lost due to a lockout, etc. To begin that process, the user must be assigned a **Task** to ***Set Security Q&As***.

A few rules apply to the setting of **Security Q&As**:

a) All users can set up and manage three (3) security questions through the **Manage Security Questions** page.

b) Questions must be selected from an FTA approved list and 3 distinct questions must be selected.

c) Answers must contain at least three (3) characters and cannot be used for more than one question.

d) Users must correctly answer their existing questions to change them.

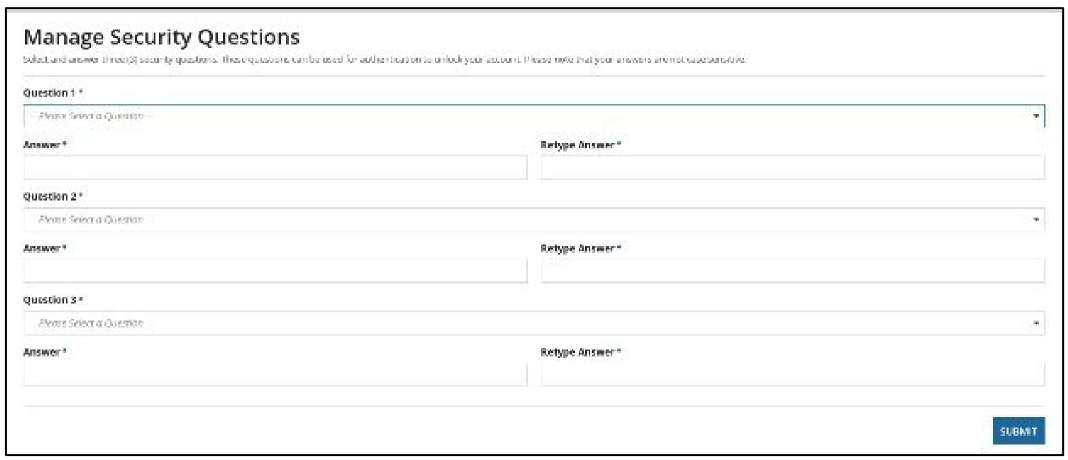
e) Users have three (3) attempts within a calendar day to answer their security questions correctly before they are locked out of the action.

f) Users cannot see the **Manage Security Questions** page on any other user's account.

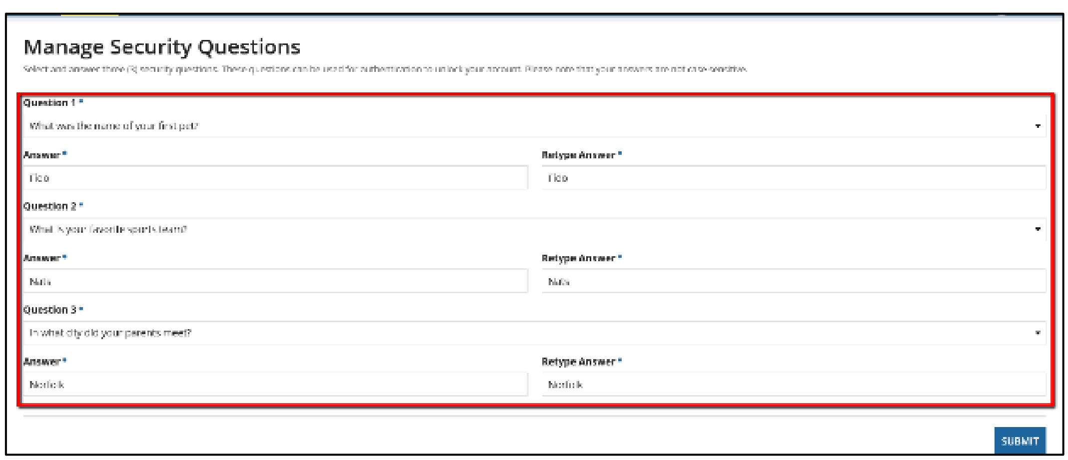
g) Users will receive an automated email notification any time their questions have been updated.

To being the process of setting one's own security questions:

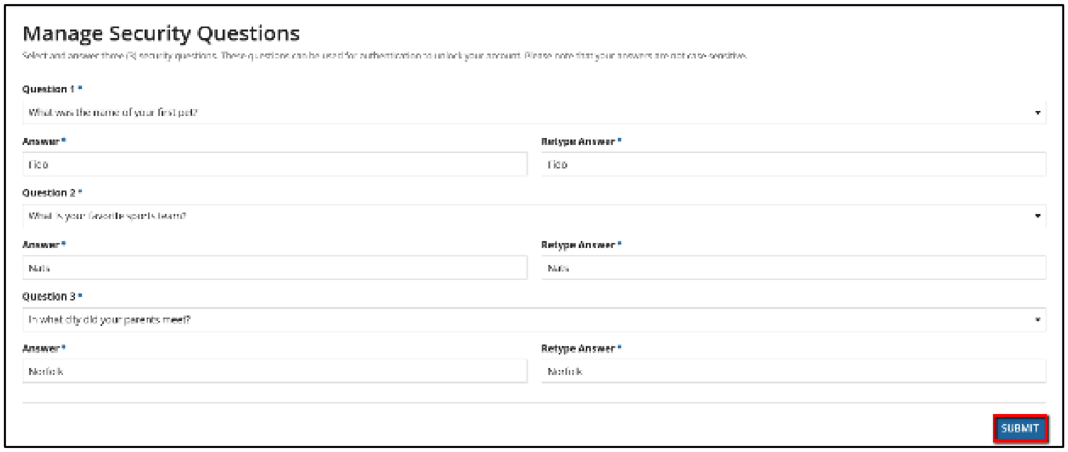
1. Locate the **User Profile** through either the **User Settings** page or the **Manage Users** page.
2. Select ***Related Actions***.
3. Click ***Manage Security Questions***.
4. The **Manage Security Questions** page displays, providing three areas for the user to select from a dropdown of questions and to enter their own answers to those questions.



5. Select the question for each of the three security questions and enter the appropriate answer.



6. When all three questions have been selected and answers provided, click ***Submit***.



7. The **Tasks** tab will display with the just completed ***Set Security Q&As*** task being cleared from the page.

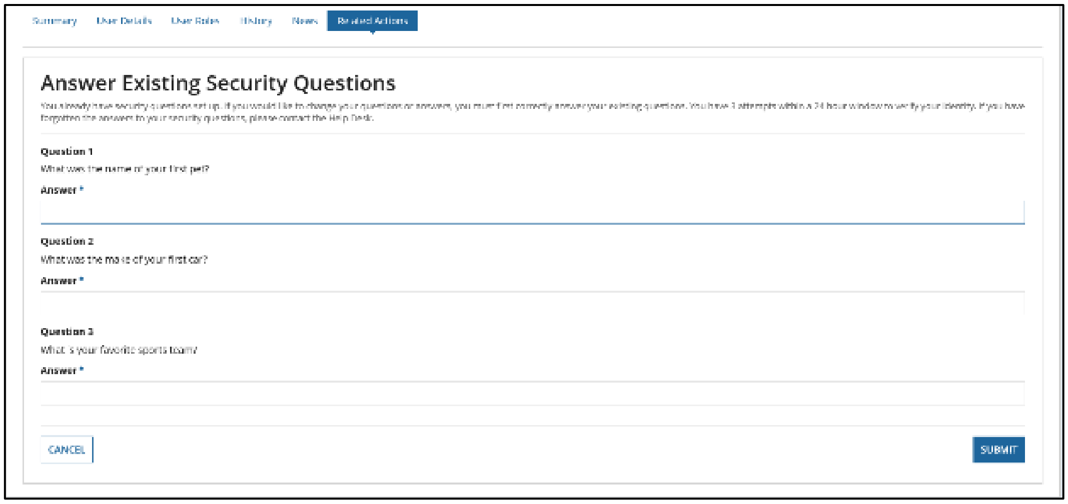
5.1.3 Related Action: Manage Security Questions/Answers

FACES provides a set of questions to add security to some of its functions. Three security questions, as set by the users themselves, are required to complete specialized actions.

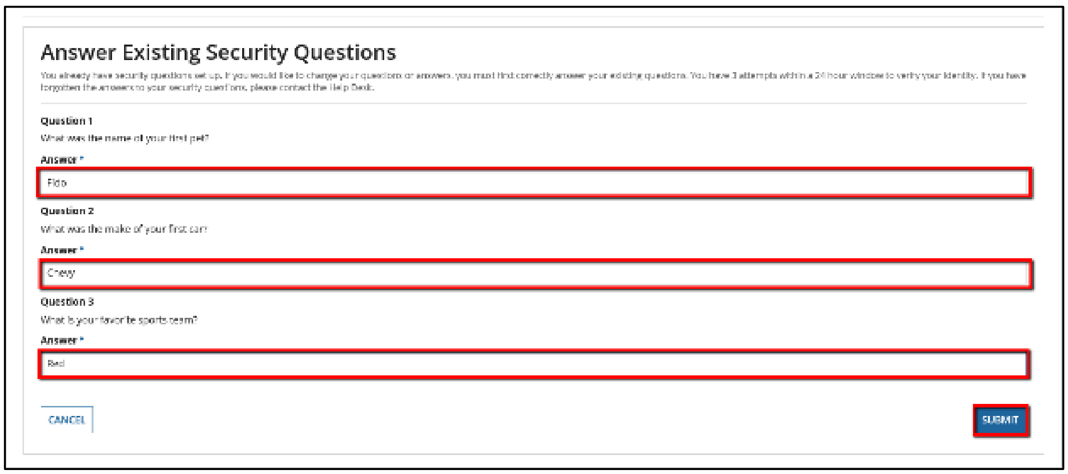
To begin the process of managing one's security questions:

1) Locate the **User Profile** through either the **User Settings** page or the **Records** page.
2) Select ***Related Actions***.
3) Click ***Manage Security Questions*** from the **Related Actions** page.

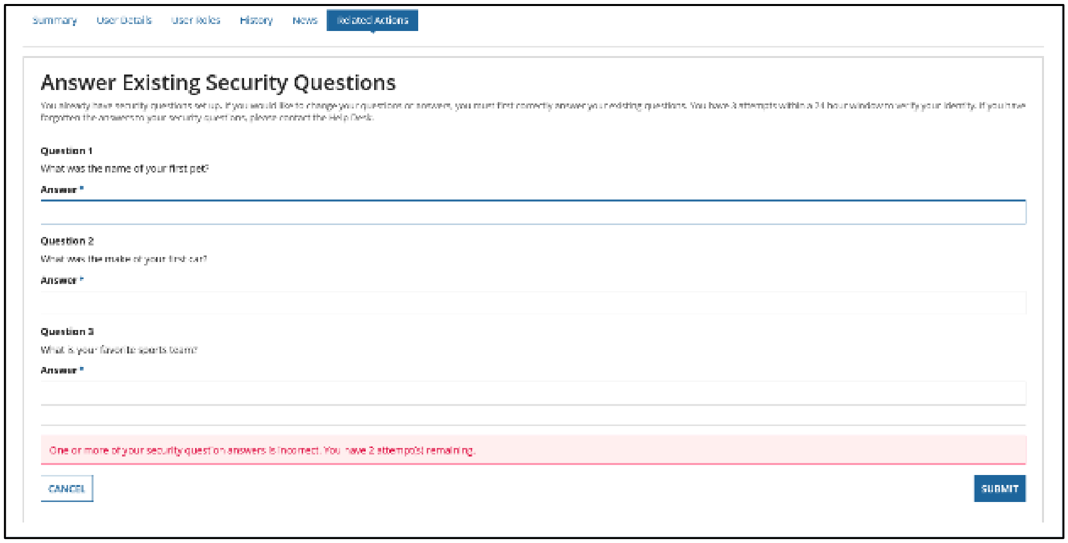
4) If there are existing security questions associated with the user profile, the **Answer Existing Security Questions** page displays. This page presents three questions and gives the user three attempts (within a 24-hour period) to answer them correctly.



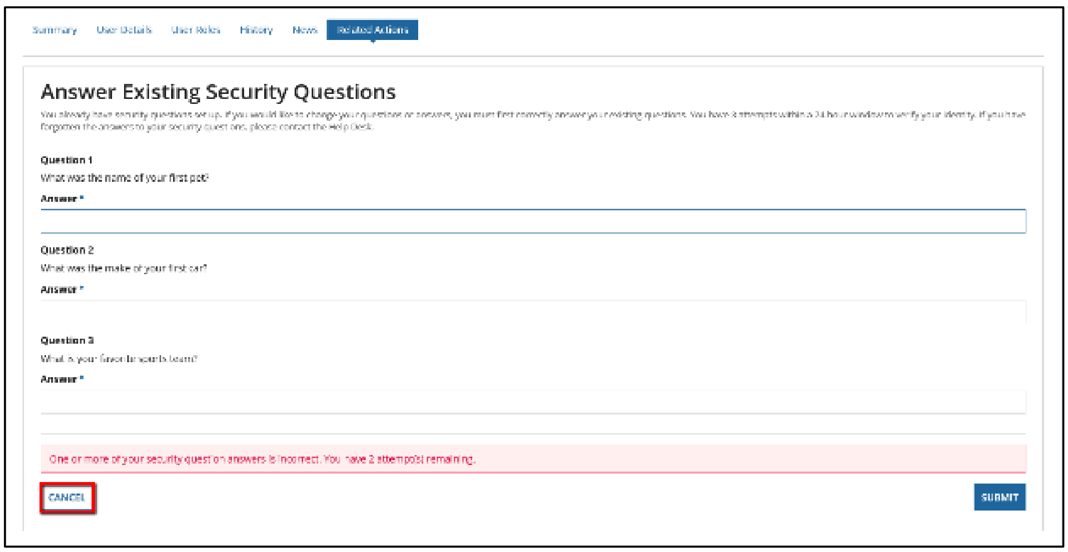
5) Enter the appropriate information and click ***Submit***.



6) If the information entered for each question is incorrect, the answer to all questions is removed and a prompt is displayed to alert the user that they have not entered correct answers.

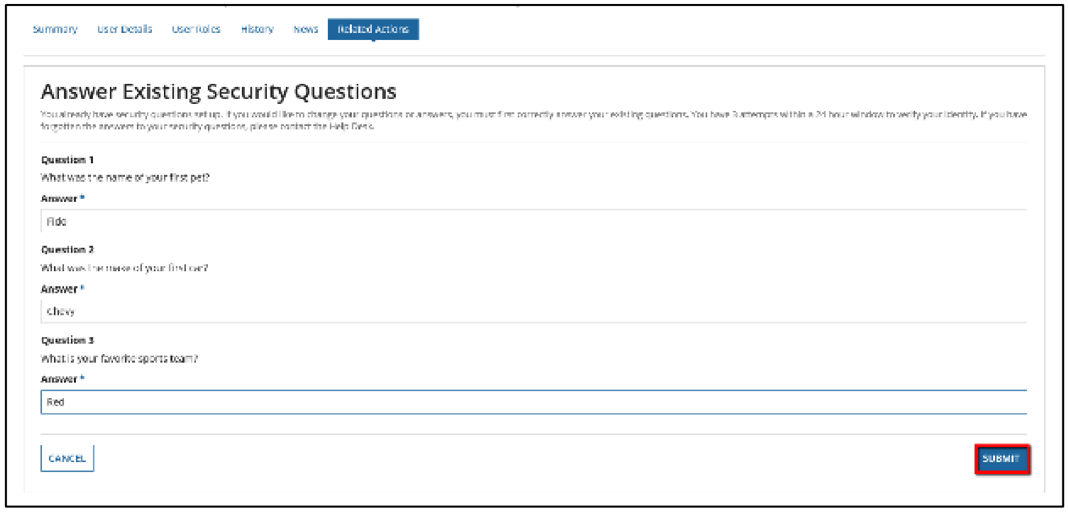


7) Click ***Cancel*** to abort the security questions page.

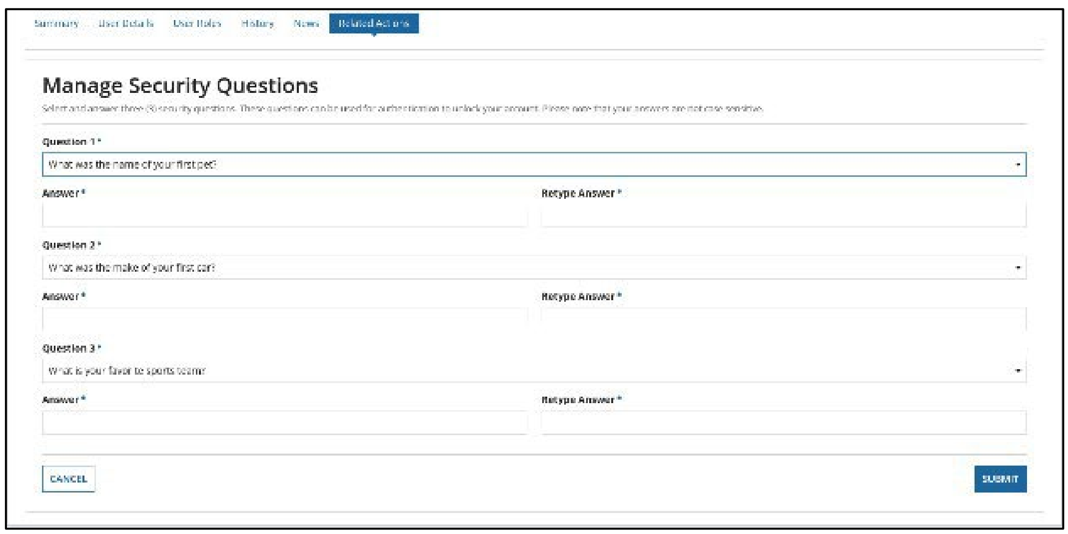


8) The **Related Actions** page is again displayed.

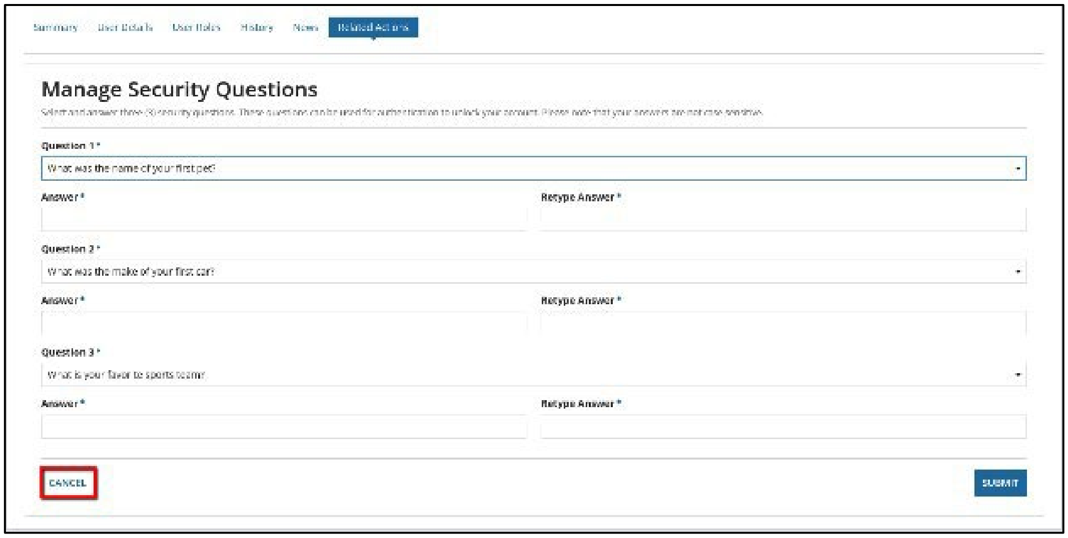
9) If the information entered has been corrected for each question, click ***Submit*** once more.



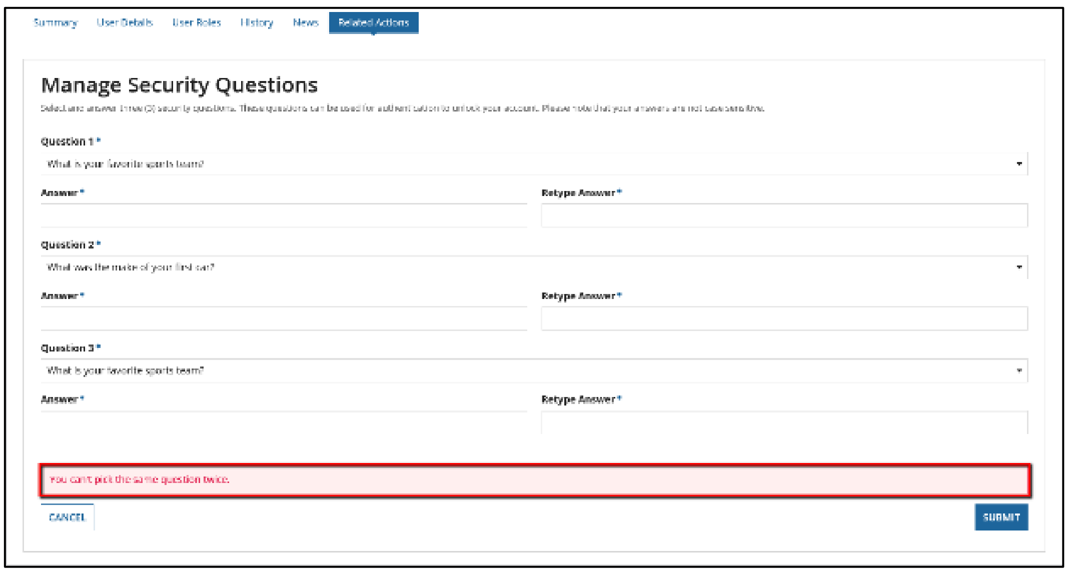
10) Once the three answers have been verified, the user is presented with a fresh page within which to enter either a fresh set of questions/answers or using one or more of the previous questions/answers and adding more.



11) Click ***Cancel*** to abort the security questions page and return to the **Related Actions** page.

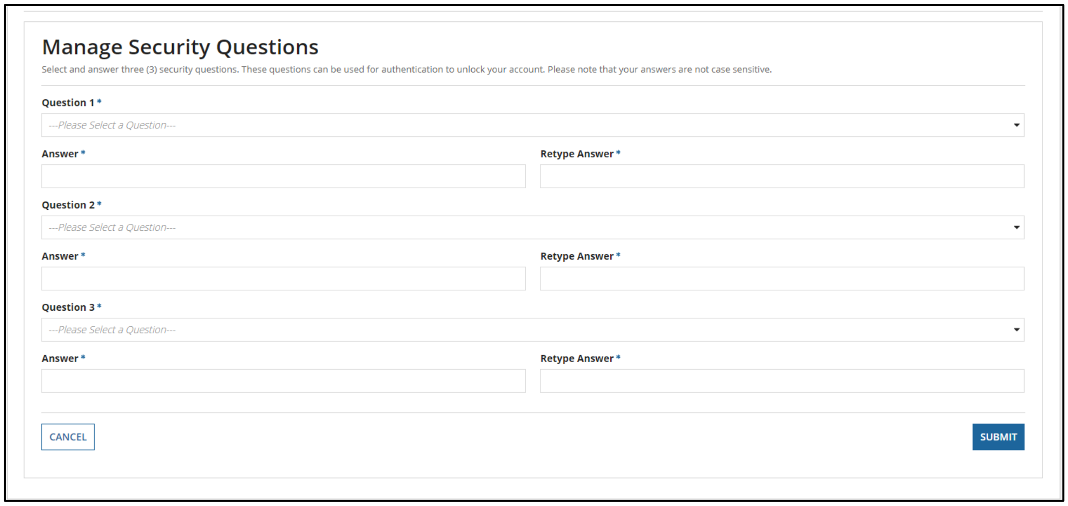


12) If a previously used question is selected from the dropdown provided, an error message is raised that warns the user that *You can't pick the same question twice*.



13) Click ***Submit*** to save any changes made to any of the questions/answers.

Note:	*Only the first question was changed.*



14) The **Related Actions** page is again displayed.

5.1.4 Related Action: Reset Security Questions

If a user is unable to answer security questions to re-establish access due to a lockout, etc., security questions can be reset by a System Administrator or through contacting the TrAMS Help Desk.

5.1.5 Related Action: Creating a PIN

Some user roles require a personal identification number (PIN) to complete actions or tasks within the system. These roles include the TrAMS Submitter, Attorney, Official, and Regional Administrator. Users that have one or more of the PIN-based roles gain access to a new user profile **Related Action** to set their personal four-digit PIN code. This **Related Action** will be shown as ***Manage PIN***. Adding any of the PIN-based roles to a user record will require that user to make use of a PIN code for certain actions that can only be performed by those roles.

There are a few basic rules surrounding the use of PINs:

a) Users with PIN roles (**TrAMS Submitter**, **Official**, **Attorney**, **Administrator**) will have access to a ***Manage PIN*** profile **Related Action** to create or change a PIN.

b) No user can see the ***Manage PIN*** profile **Related Action** on any other user's account.

c) PINs must be 4-digit numeric codes (e.g., "1234").

d) To reset a PIN, a user must correctly enter their current PIN or correctly answer their Security Questions.

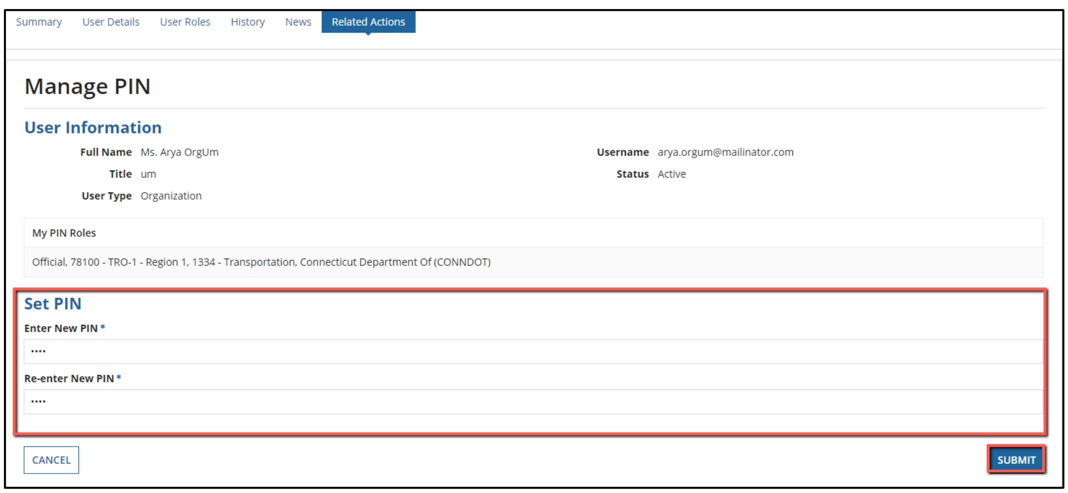
e) Users have 3 attempts per calendar day to reset their PIN before they are locked out of the action.

f) Users will receive an automated email notification any time their PIN has been updated.

To create the **PIN** code:

1) Locate the **User Profile** through either the **User Settings** page or the **Records** page.
2) Select ***Related Actions***.
3) Click ***Manage PIN***.

4) First time users will see the **New PIN** field. Enter a four-digit PIN code. **This is a required field**.



5) Select ***SUBMIT*** so save the PIN.
6) Select ***Cancel*** to return to the **Related Actions** page without saving any changes.

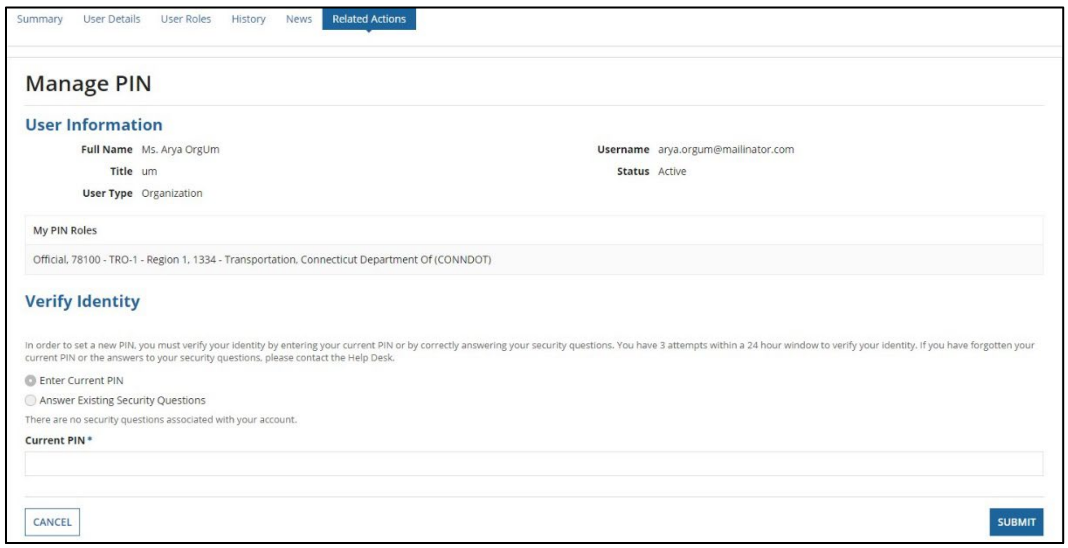
5.1.6 Related Action: Changing the PIN

Once the PIN has been created, a user may again select the ***Manage PIN*** function from the **Related Action** page to change or re-set their personal four-digit PIN code.

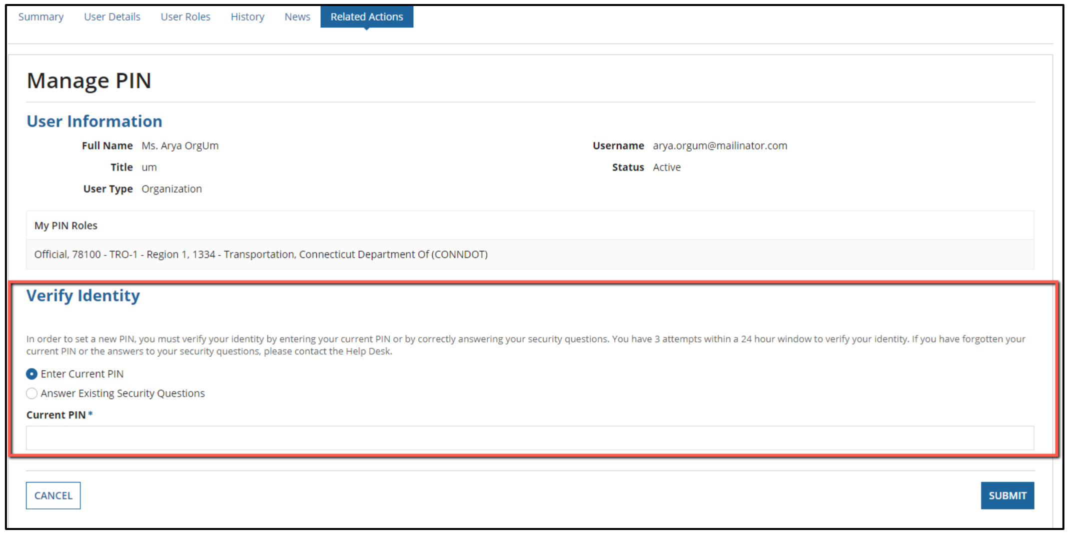
To change the PIN code:

1) Locate the **User Profile** through either the **User Settings** page or the **Manage Users** page. Select ***Related Actions*** and then click ***Manage PIN***.

2) The **Manage PIN** page will display **User Information** as well as the roles to which the PIN has been applied.



3) The user is provided with two separate mechanisms by which they can verify their identity. One includes simply entering the PIN (if known). The other allows the user to verify their identity by answering their security questions.

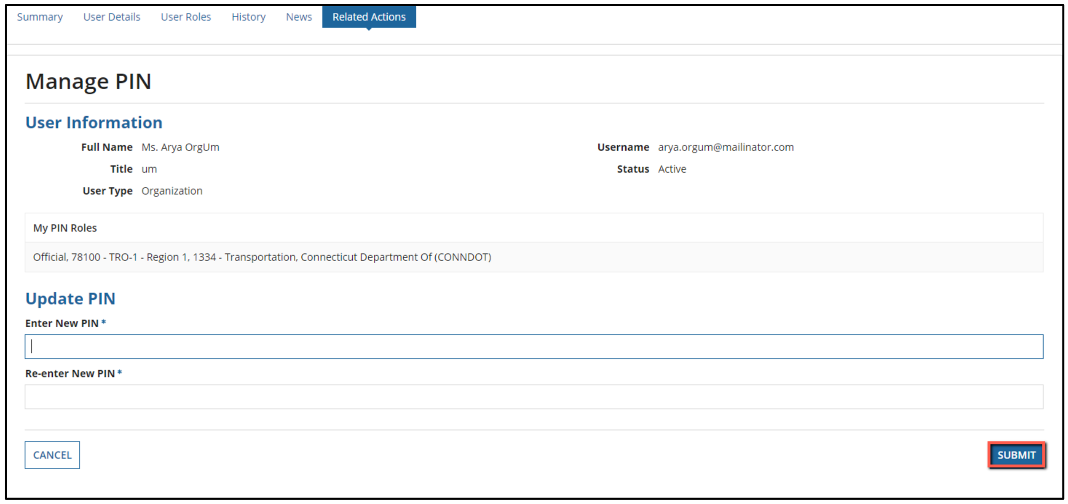


4) Select ***Answer Existing Security Questions*** by selecting the radio button next to that item. This will cause the three questions to be presented for the user to enter the verified information.

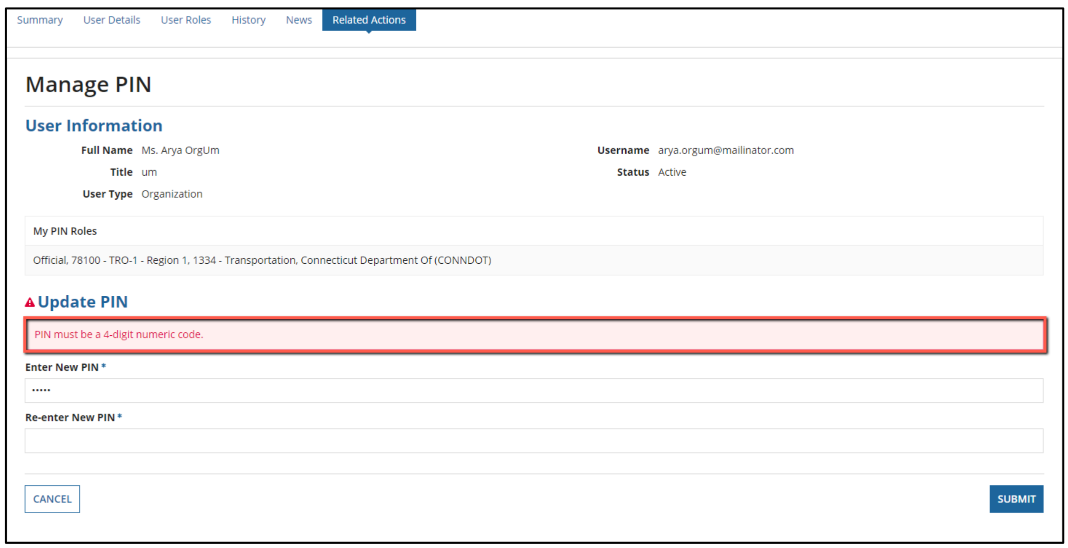
5) Click ***Cancel*** to abort the security questions page and return to the **Related Actions** page.

6) Complete the information and click ***Submit***.

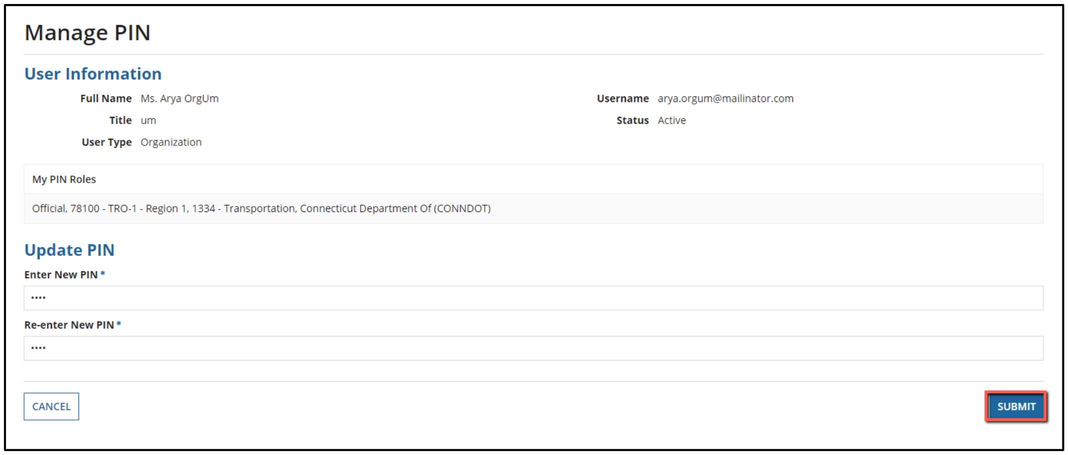
7) After entering all the information for the security questions and clicking ***Submit***, the user is presented with the **Update PIN** page, allowing them to enter a new PIN to be associated with their role(s).



8) The user enters a new PIN and re-enters the same PIN for confirmation. If, however, the PIN is not exactly four characters (not less, not more), an error message is raised that *PIN must be a four-digit numeric code*.



9) Correct the PIN and click ***Submit***.



10) The **Related Actions** page displays.

Note:	*If the user cannot remember either their existing PIN or security question answers, the user must contact the Help Desk for assistance.*

5.1.7 A Locked Account

FTA complies with U.S. DOT Information Technology (IT) Security guidelines. FACES uses several security features to ensure that only valid and active users have access to the FTA platform. One of those features is the User Lockout function. An automatic account lockout occurs after 60 days of user inactivity (i.e., after 60 days of the user failing to log in to the FTA platform). The lockout also occurs when the user is required to comply with an annual user recertification. Annual user recertification verifies that each user has valid system access and the correct user roles. A user will be locked if the user is not recertified during the recertification window. These security features apply to all software systems that rely on FACES for access.

Users with locked accounts can still log onto the FTA platform but they will be unable to complete any actions on their account or specific to their roles. The standard tabs (***Manage Users***, ***Reports***, and ***Actions***) will contain a limited amount of data and security-related actions. For example, no tasks will be available.

Locked users can unlock their accounts using one of two methods: (1) correctly answering their existing security questions; or (2) submitting an unlock request. Both methods are available via a single action on the **Actions** tab. It is preferred that all users attempt to self-unlock their accounts by answering their previously setup security questions before submitting an unlock request; this is the quickest and most efficient route to unlock an account. However, if a user is locked due to recertification, the user will not be able to use self-unlock to unlock his or her account. Once an account is unlocked, the user's access privileges will be fully restored.

5.1.8 Answer Security Questions

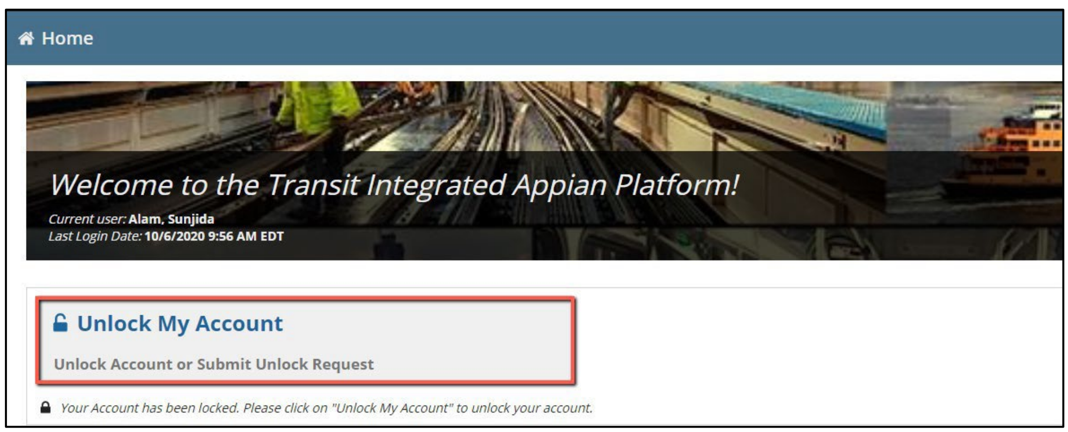
If the account is locked and security questions were previously set up, the user can attempt to unlock the account by answering their security questions through the ***Unlock Account*** link on the **Actions** tab.

Note:	*See Related Action: Set Security Questions/Answers or Related Action: Manage Security Questions/Answers for instructions on setting up Security Questions. User Security Questions cannot be modified while the account is locked.*

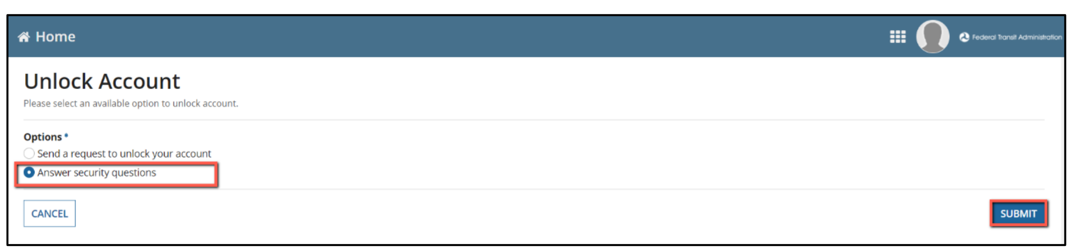
The user is allowed three (3) attempts per calendar day to correctly answer the security questions. Users who have not set up security questions or who cannot remember the correct answers to their questions must instead submit an unlock request.

To unlock the account via security questions:

1) Login to your account.
2) Click ***Unlock my Account***.

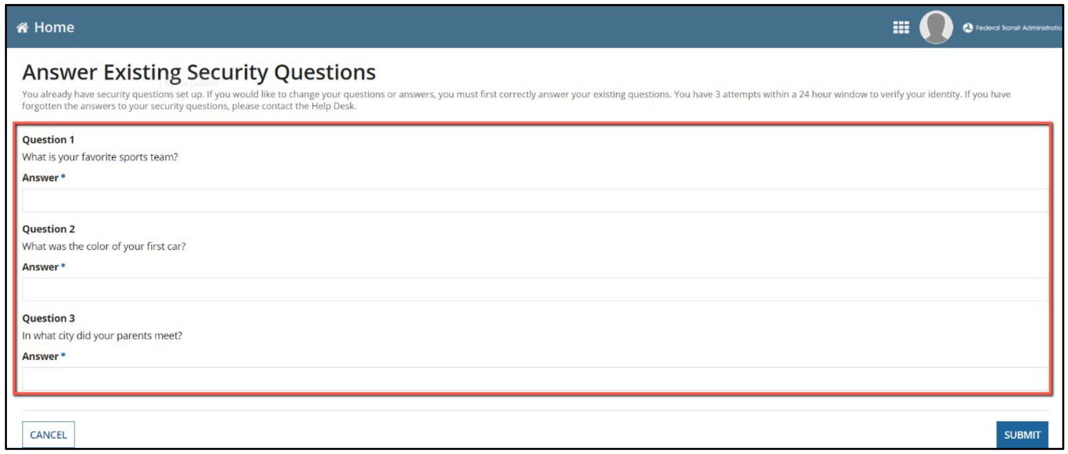


3) If **Security Questions** have already been established, then click ***Answer Security Questions*** from the **Unlock Account** page and then click ***Submit***.

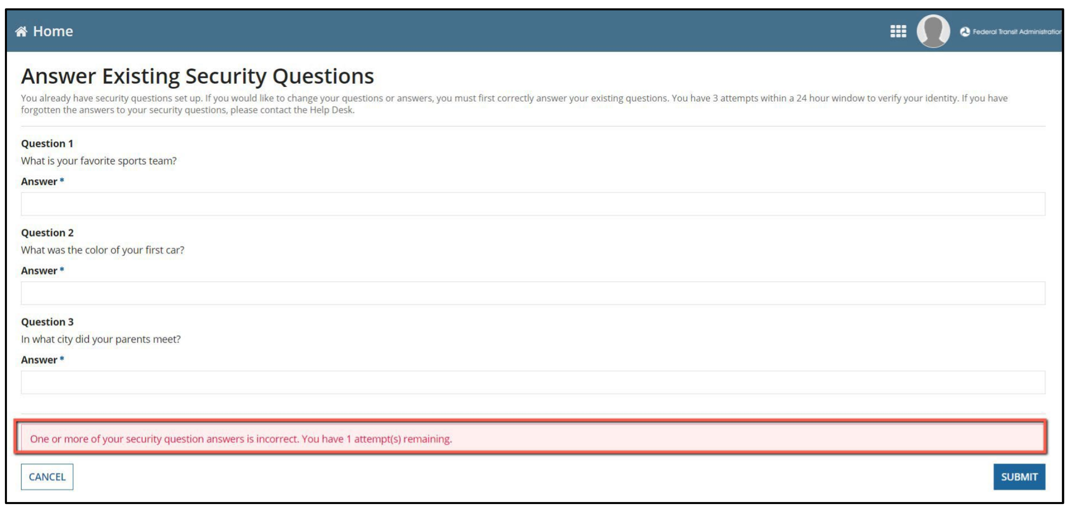


4) Provide the correct answers to the three previously established questions and click ***Submit***.

Note:	*Answers are case insensitive.*



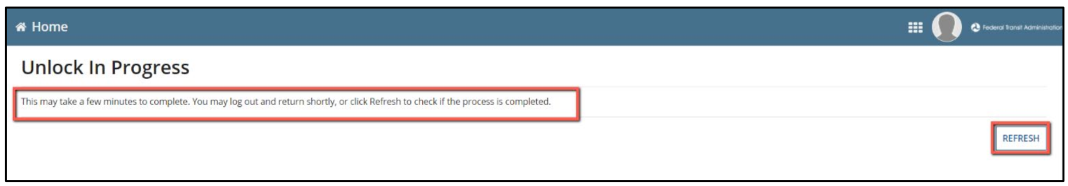
5) If incorrect information was entered, a validation error message will display that indicates the number of attempts remaining for <u>the current calendar day</u>. After three incorrect attempts, the user will need to submit an unlock request. See section **5.2.2** to learn how to submit an unlock request.



6) If incorrect information was entered, <u>all three answers</u> will be erased regardless of which one of the three answers was correct.

7) Enter the correct information and click ***Submit***.

8) A message indicating **User Unlock Processing** will display.
9) Click ***Refresh***.



10) A message indicating **Your Account has been unlocked** will display.

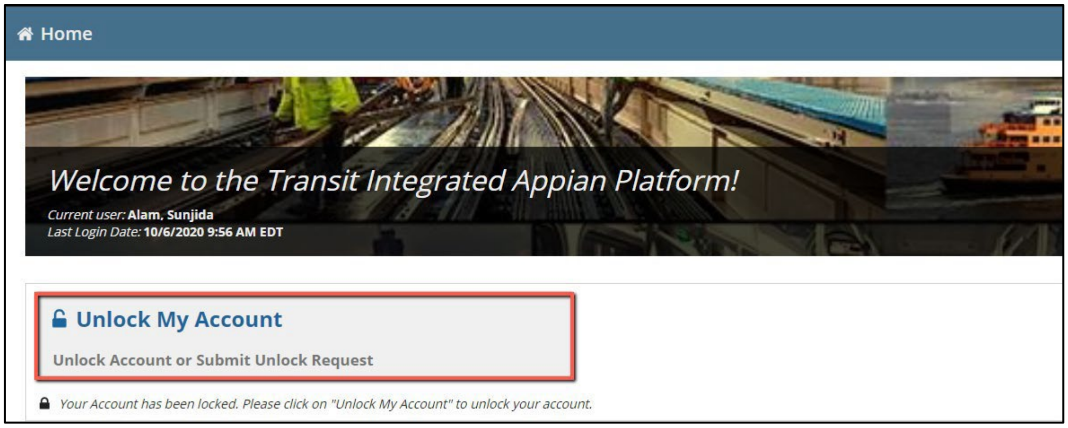
11) The user can Click the link to return to the Homepage.
12) An email will be auto generated and sent to the user.

5.1.9 Submit Unlock Request

If a user has not set up security questions or cannot remember their answers, they can submit an unlock request by selecting ***Unlock Account*** on the **Actions** tab. The unlock request is automatically routed to the appropriate approvers (User Managers, Validation Analysts, LSMs, or GSMs). If an organization does not have a User Manager or the locked user is the User Manager, the request will go to the next level approver. If the user belongs to multiple organizations, the request will go to each of the organization's user management chain.

To submit an unlock request:

1) Log into FACES and Click ***Unlock My Account***.



2) Select the ***Send a Request to Unlock Your Account*** option, enter any comments pertinent to regaining access, and then click ***Submit*** to finalize the action.

3) A message indicating **Unlock Request Successfully Submitted** will display.

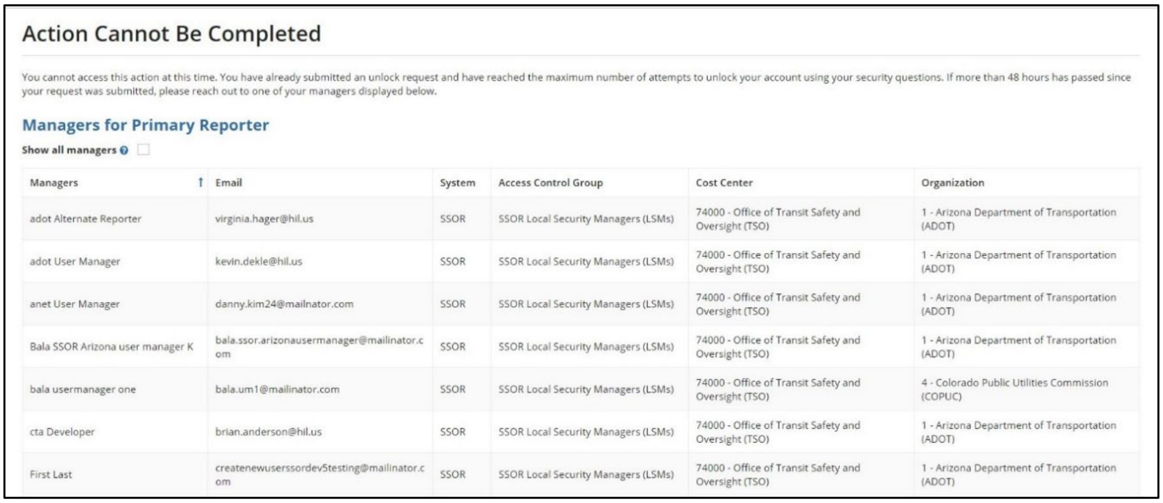
4) Click ***Close***.

5) The request for the unlock will automatically be routed to the appropriate approver(s).

Users are only allowed to submit one unlock request at a time. Once an unlock request has been submitted, the user cannot self-unlock their account via security questions or submit a new unlock request After submitting the unlock request, the **User Manager, LSM, Validation Analyst, User Manager Supervisor, FTA Signer, or GSM** (as appropriate) will receive an email notification to review the submitted request. They can either approve or deny the request. The user will be notified via email of either decision.

If the request is approved, the account will unlock, and all previous permissions will be restored. If the request is denied, the account will remain locked. The user will see the message below if they attempt to submit another unlock request. If the account remains locked after 48 hours since the request was submitted, the user should contact any of their assigned **User Manager, Validation Analyst, LSM, or GSM** by clicking on the link.

A list of the managers for the user will appear with information for all the user's managers.



Managers	Email	System	Access Control Group	Cost Center	Organization
adot Alternate Reporter	virginia.hager@hil.us	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	1 - Arizona Department of Transportation (ADOT)
adot User Manager	kevin.dekle@hil.us	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	1 - Arizona Department of Transportation (ADOT)
anet User Manager	danny.kim24@mailnator.com	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	1 - Arizona Department of Transportation (ADOT)
Bala SSOR Arizona user manager K	bala.ssor.arizonausermanager@mailinator.com	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	1 - Arizona Department of Transportation (ADOT)
bala usermanager one	bala.um1@mailinator.com	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	4 - Colorado Public Utilities Commission (COPUC)
cta Developer	brian.anderson@hil.us	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	1 - Arizona Department of Transportation (ADOT)
First Last	createnewuserssordev5testing@mailinator.com	SSOR	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight (TSO)	1 - Arizona Department of Transportation (ADOT)

6. User Management

6.1. User Management Responsibilities

User management responsibilities include user creation, role assignments, deactivation, reactivation, and unlocking. Responsibilities vary somewhat by management level. At the lowest level, each organization will have one or more users assigned to the **User Manager** role. FTA approval is required to obtain or assign the **User Manager** role to any individual. The **User Manager** for an organization can perform the following actions for users within their organization:

- Create and Manage Users.
- Edit user profile information.
- Manage role documentation.
- Deactivate and Reactivate users.
- Unlock users.

- Recertify users.

FTA Global Security Managers (**GSMs**) can create and manage all other users within their system (e.g., TrAMS, NTD, SSOR, DGS and CRM).

FTA Local Security Managers (**LSMs**) can manage all FTA users within their cost center, organization users within any organization that belongs to their cost center, and external contractors. FTA LSMs can also approve role requests from User Managers.

FTA **Validation Analyst** can only manage with **FTA LSM** roles users within their cost center, organization users within any organization that belongs to their cost center, and external contractors. Validation Analyst with LSM role can also approve role request from User Managers.

User Managers **(UMs)** can create, manage, and recertify users within their system.

Privileges	User Manager	Validation Analyst with LSM	LSM	GSM
Users authorized to manage	Users in same organization	Organization, FTA, and contractor users in same Cost Center	Organization, FTA, and contractor users in same Cost	All users in Platform System
Responsibility	**User Manager**	**Validation Analyst**	**LSM**	**GSM**
Create New Users	Yes	Yes	Yes	Yes
Assign and remove Bulk	No	Yes	Yes	Yes
Approve role requests*	No	Yes	Yes	Yes
Edit user profile	Yes	Yes	Yes	Yes
Manage role	Yes	Yes	Yes	Yes
Deactivate and Reactivate users	Yes	Yes	Yes	Yes
Unlock users	Yes	Yes	Yes	Yes
Recertify users	Yes	Yes	Yes	Yes

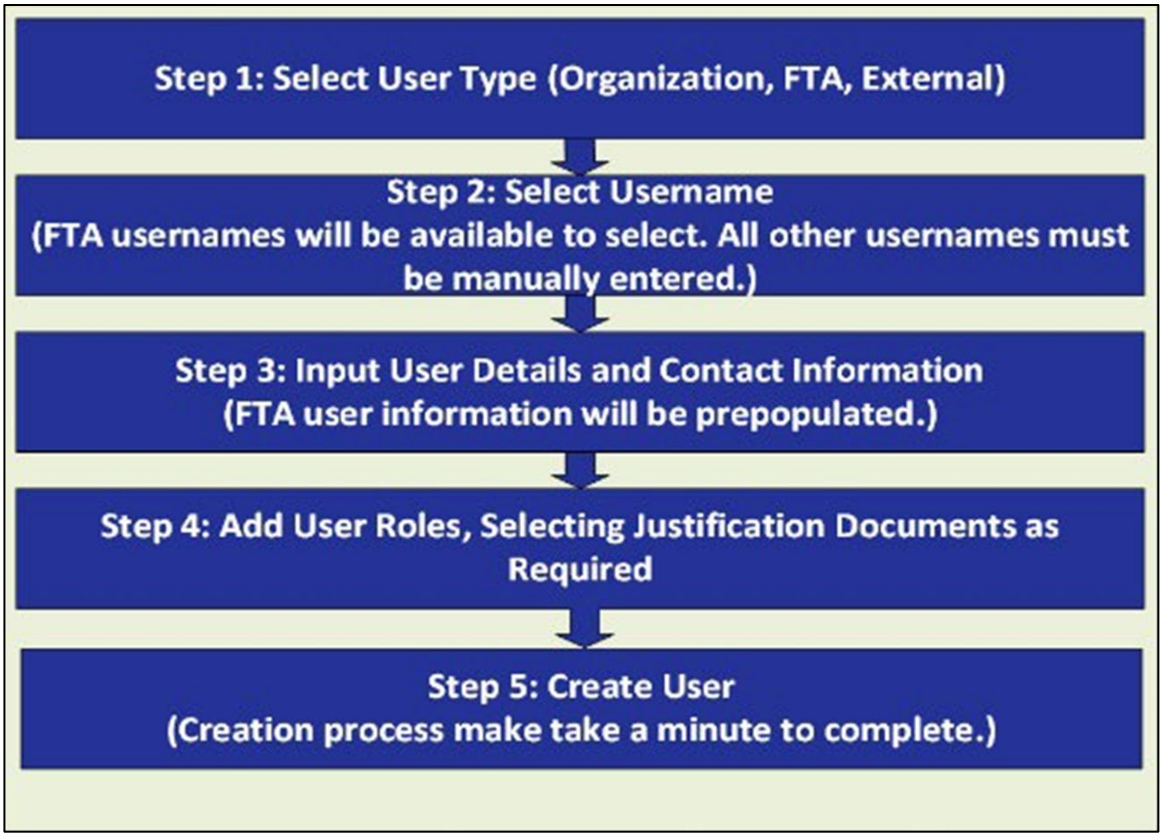
*User managers can assign roles, however certain roles (UM, Attorney, Submitter, Official) require approval from an LSM

The remainder of this section presents an overview of each of the user management activities and responsibilities.

Note:	*The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

6.2. User Creation

The following presents an overview of the six-step process required for creating a new user of any type:



There are explicit rules controlling user creation:

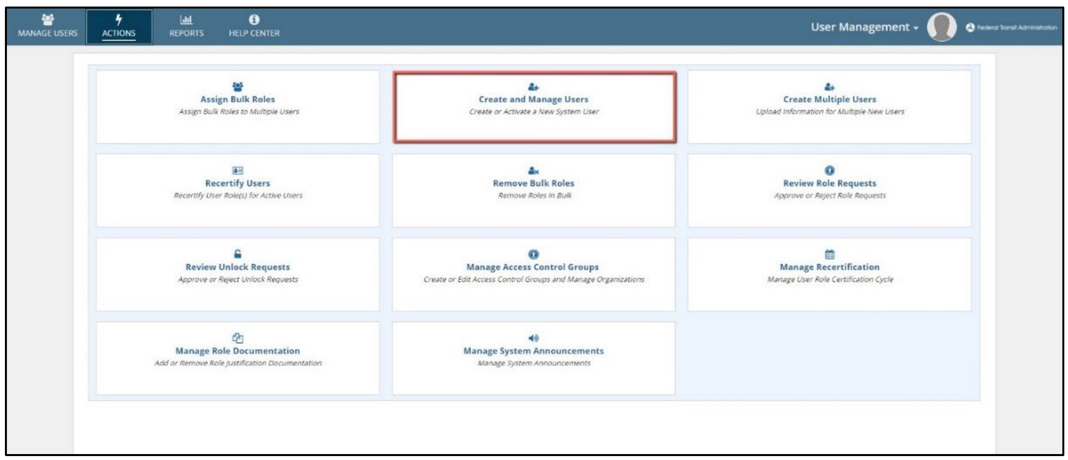
1) Only users with the roles **User Manager**, **Local Security Manager (LSM)**, and **Global Security Manager (GSM)** are approved to create users using the ***Create and Manage Users*** action.
2) Users can only create user and add roles for which they have privileges.
3) Organizational **User Managers** can create other organizational users.
4) External **User Managers** can create other external users (e.g., DOL).
5) **LSMs and GSMs** can create users of any type.
6) When a username is entered to create a new user, the system will flag any user that already exists and present the creator with the option of going to the ***Manage Roles*** action to add roles to that existing user.
7) A user's username must be a valid email address.
8) Name, contact, and business address information is required when creating a new user.
9) A user cannot be created unless at least one role is assigned to the user.
10) Some roles require approval by users with higher privileges.
11) Only roles matching the new user's type can be added to the user.

6.2.1 Action: Create and Manage Users

User Managers, Supervisors, Validation Analyst, LSM, and GSMs have access to the ***Create and Manage Users*** action. This action allows a new user of any type (Organization, FTA, and External) to be added to the system, however, individual ability to create users of different types is restricted. The process for creating organization and external users is slightly different from the process to create FTA users. The two main processes will be described in separate subsections so that appropriate screenshots can be shown.

To add a new user:

1) Log in to the system as a user manager and click ***Create and Manage Users*** from the **Actions** tab.



2) The user manager is presented with a short list of user types from which to select. Each type has its own set of role limitations. Depending on the user manager's privileges, the user type may be preselected and locked. DOT Users as shown in the following screenshot.

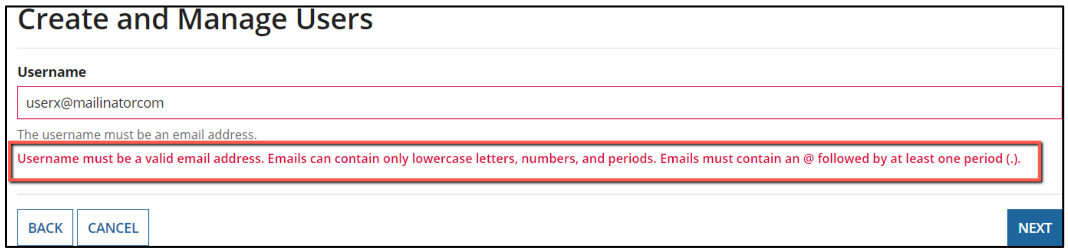
3) Select the appropriate user type (as applicable) and then click ***Next***.

4) The first information about a user required is their username, based on <u>a valid email address</u>. **This is a required field** and will function as the user's login. Email addresses should be provided in lowercase. Each Username field must be unique and <u>cannot be changed after creation</u>.

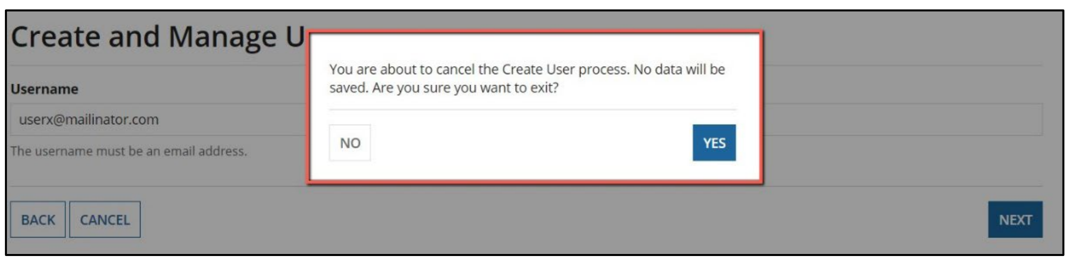
Validation checks will confirm uniqueness before moving to the next step.

5) Enter an email address and tab forward.

6) If the email is rejected as invalid, the page will display an error message.

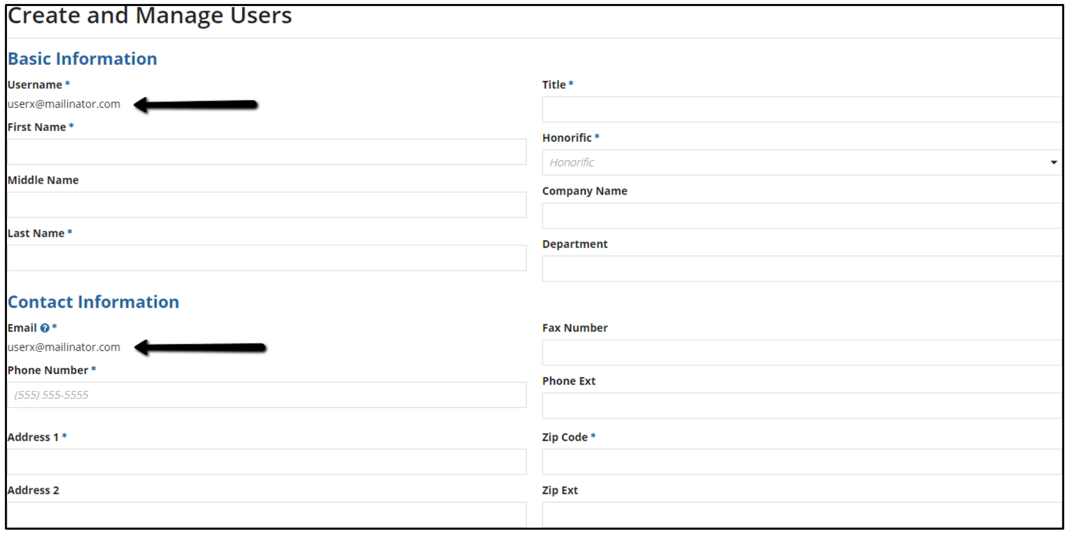


7) At any point in the ***Create and Manage Users*** process, the user may click ***Cancel*** to end the process. On cancelling the Create and Manage Users process, no data entered for that user will be retained.



8) If the email is accepted as valid, the ***Next*** button will be activated, allowing selection.

9) Click ***Next***, launching the ***Create User*** page. The Username and Email fields will be pre-populated.



10) Enter the Basic Information for the following fields:

a. The username just entered displays in the *Username* field but cannot be changed.

b. Enter the user's first name in the *First Name* field (35-character limit). This is a required field.

c. Enter the user's middle name in the *Middle Name* field (35-character limit).

d. Enter the user's last name in the *Last Name* field (35-character limit). This is a required field.

e. Enter the user's job title in the *Title* field. This is a required field.

f. Enter an honorific for the user in the *Honorific* field. This is a required field (i.e., Mr., Ms.).

g. Enter the user's company information in the *Company Name* field.

h. Enter the user's department in the *Department* field.

i. System information is entered only by the Global Security Manager.

11) The ***Create User*** page also provides data fields for Contact Information:

a. The valid email address displays once more in the *Email* field. Again, the email address cannot be altered or edited once the email has been accepted.

b. Enter the user's work business phone number in the *Work Phone* field. This is a required field (20- character limit).

c. Enter the user's <u>business phone number extension</u> in the *Phone Number Extension* field (10- character limit).

d. Enter the user's <u>business fax number</u> in the *Fax Number* field (20-character limit).

e. Enter the first line of the user's <u>business address</u> in the *Address 1* field (60-character limit).

f. Enter the second line of the user's <u>business address</u> in the *Address 2* field (60-character limit).

g. Enter the city for the user's <u>business address</u> in the *City* field (60-character limit; no numeric).

h. Select the state for the user's <u>business address</u> from the dropdown menu provided under the *State* field.

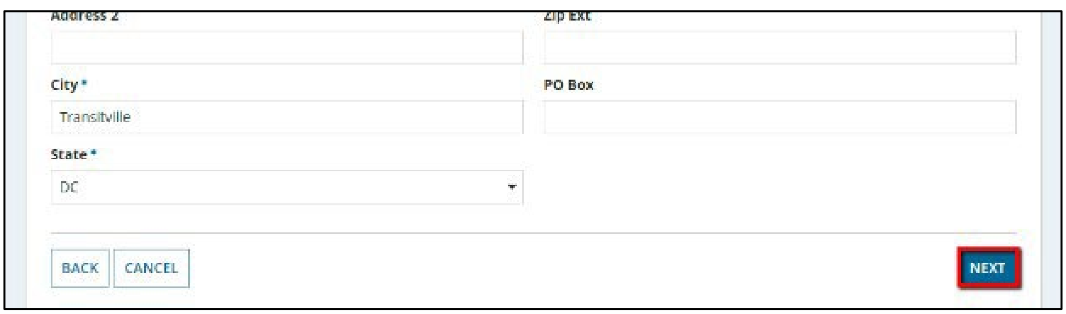
i. Enter the ZIP Code for the user's <u>business address</u> in the *ZIP Code* field (5-character limit).

j. Enter the ZIP Code Extension for the user's <u>business address</u> in the *ZIP Code Extension* field (4- character limit).

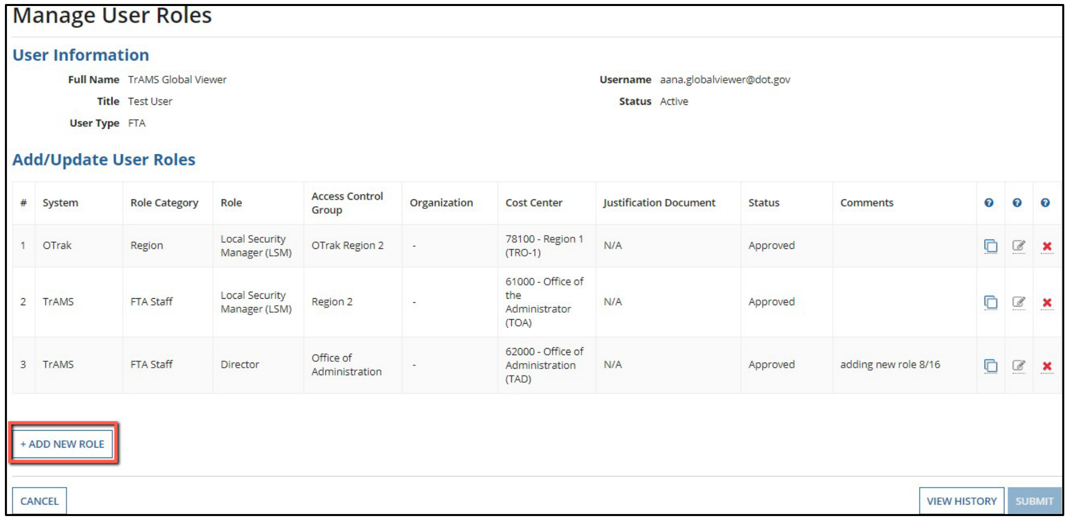
k. If necessary, enter the associated Post Office Box in the *PO Box* field (35-character limit).

Note:	*PO Box is limited to numeric values and cannot contain alphabetical characters.*

12) After all required details have been entered, click ***Next***.

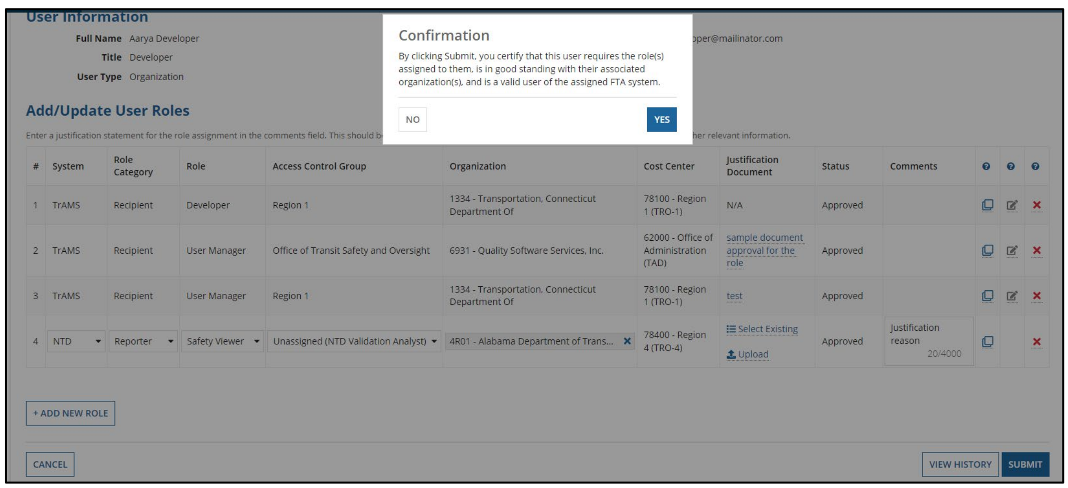


13) The **Manage Roles** page displays. Click ***Add New Role***.

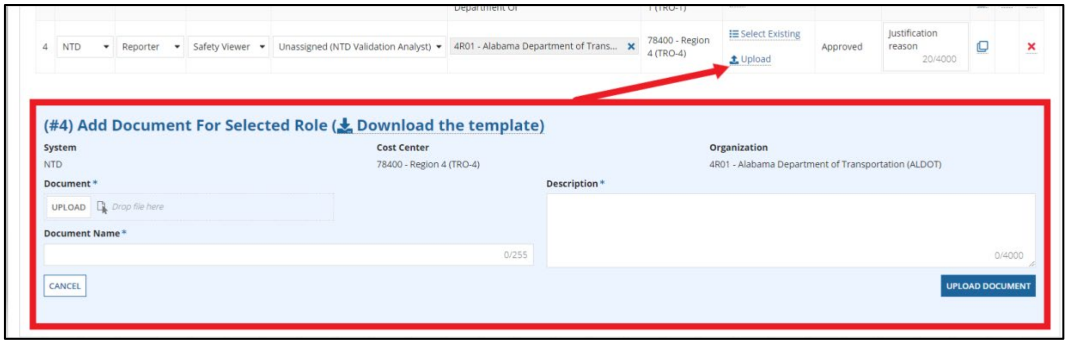


14) The following fields are required and must be populated before the role(s) can be submitted: System, Role Category, Role, Access Control Group, Organization, Cost Center, Comments.

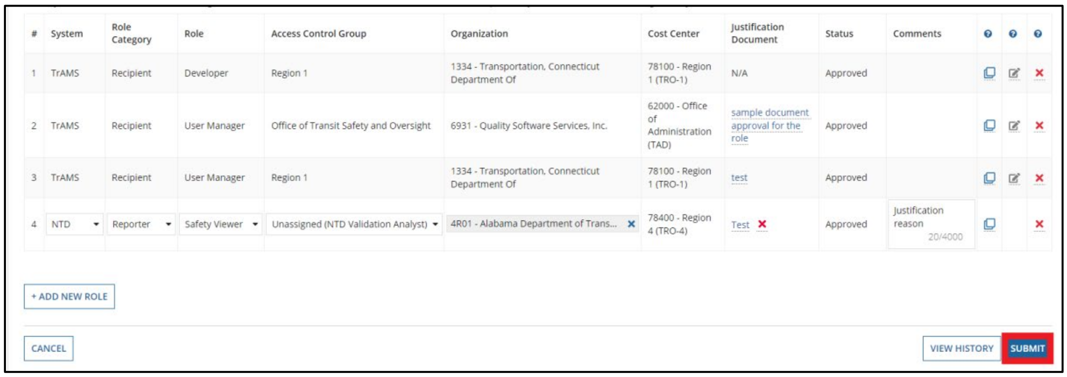
15) Click ***Submit*** and a confirmation screen will appear.



16) Users can upload a justification or delegation of authority document for any role, the **Add Justification Document** section will display. Users can download the Justification Document template using the link available in that section. Please follow the instructions within the document on how to complete the Justification Document.



17) When all roles have been added, click ***Submit*** to complete user setup.

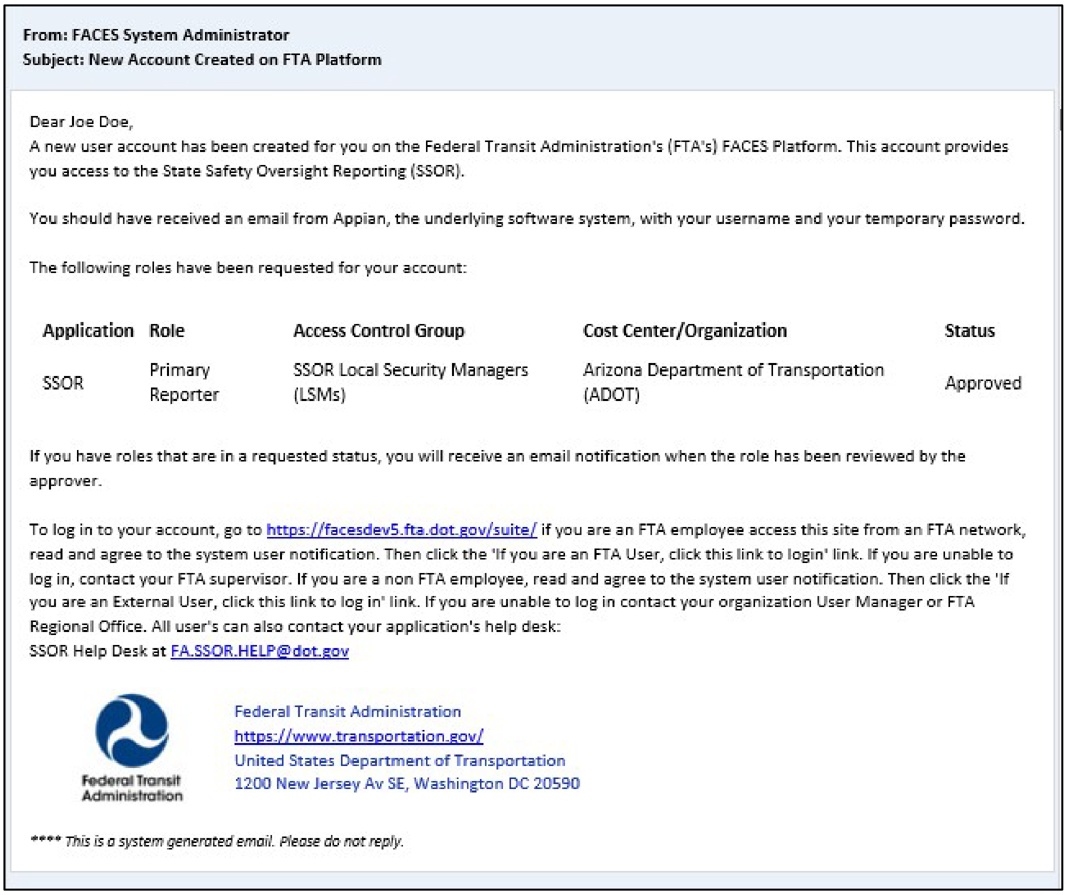


18) A **User Creation in Progress** page will display. You can click ***Close*** to leave the screen without impacting the user creation process. If you want to verify that the user record is created, wait about a minute, and then click ***Refresh.***

19) The **User Successfully Created** page displays the user's summary information. You can click the link below the user's last name to go directly to the user's profile.

20) Click ***Close*** to return to the **Actions** page instead.

21) The user will receive an automatic email alerting them of the account setup, like the one below.



From: FACES System Administrator
Subject: New Account Created on FTA Platform

Dear Joe Doe,
A new user account has been created for you on the Federal Transit Administration's (FTA's) FACES Platform. This account provides you access to the State Safety Oversight Reporting (SSOR).

You should have received an email from Appian, the underlying software system, with your username and your temporary password.

The following roles have been requested for your account:

Application	Role	Access Control Group	Cost Center/Organization	Status
SSOR	Primary Reporter	SSOR Local Security Managers (LSMs)	Arizona Department of Transportation (ADOT)	Approved

If you have roles that are in a requested status, you will receive an email notification when the role has been reviewed by the approver.

To log in to your account, go to https://facesdev5.fta.dot.gov/suite/ if you are an FTA employee access this site from an FTA network, read and agree to the system user notification. Then click the 'If you are an FTA User, click this link to login' link. If you are unable to log in, contact your FTA supervisor. If you are a non FTA employee, read and agree to the system user notification. Then click the 'If you are an External User, click this link to log in' link. If you are unable to log in contact your organization User Manager or FTA Regional Office. All user's can also contact your application's help desk:
SSOR Help Desk at FA.SSOR.HELP@dot.gov

Federal Transit Administration
Federal Transit Administration
https://www.transportation.gov/
United States Department of Transportation
1200 New Jersey Av SE, Washington DC 20590

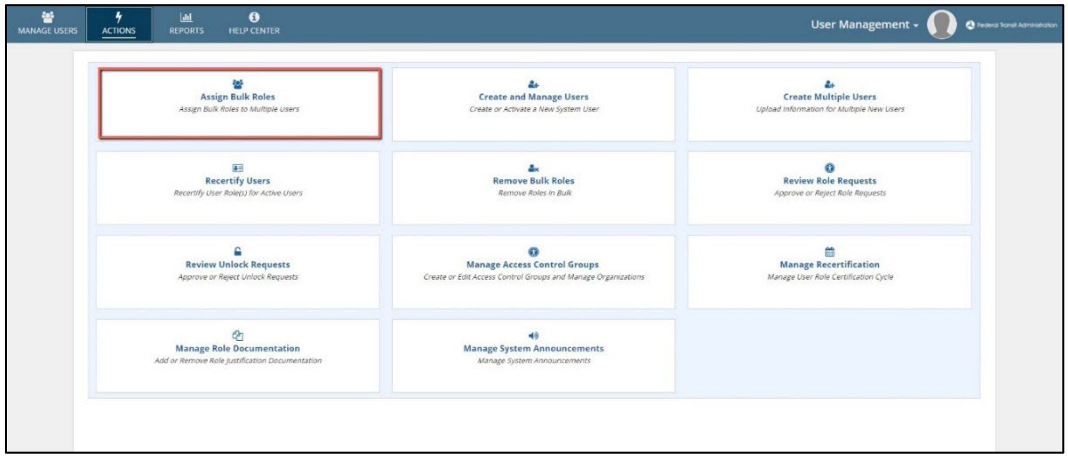
***** This is a system generated email. Please do not reply.*

6.2.2 Action: Assign Bulk Roles

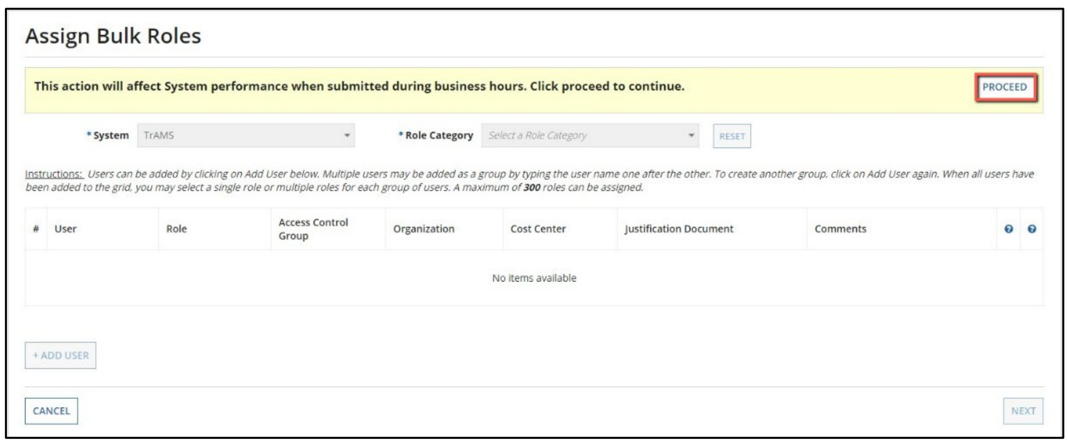
If more than one user or external user needs to be assigned to a new user role, the **User Manager**, **LSM**, or **GSM** may bulk assign user roles through this action. The assignment process will provide validations and will only allow users to be assigned roles that are valid for them. This action is useful when paired with the **Create Multiple Users** form or any other time where many users must be assigned to new roles.

To assign bulk roles at once:

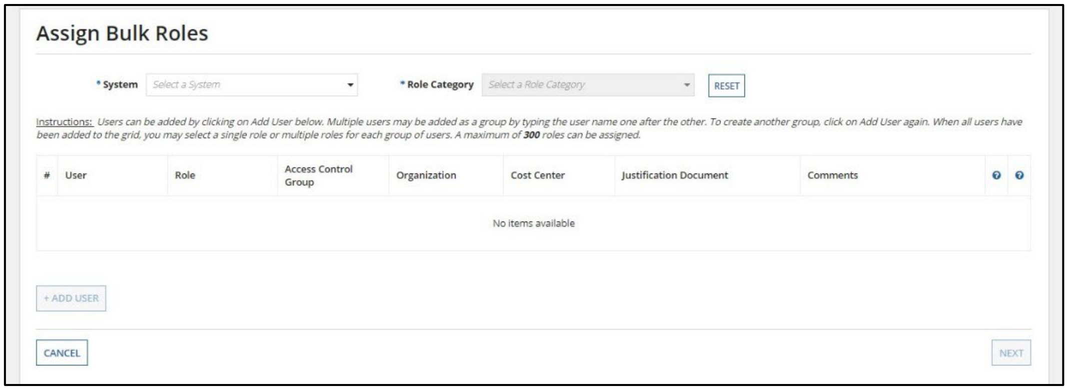
1) Click the ***Assign Bulk Roles*** from the **Actions** tab.



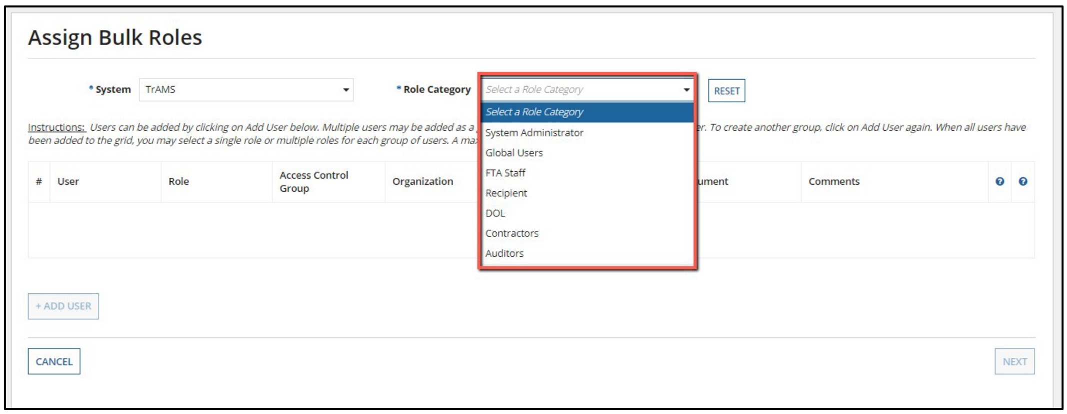
2) The Assign Bulk Roles page displays a yellow banner that requires the user to click the ***PROCEED*** button.



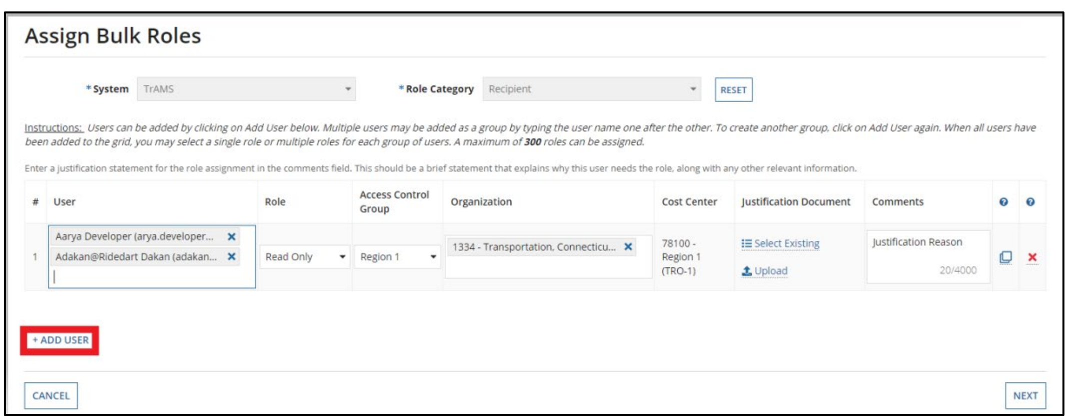
3) The **Assign Bulk Roles** page displays the available users to assign new roles based on the user assigning the roles, and the users to be assigned to a role.



4) The Assign Bulk Roles displays a short list of user roles from the Role Category. Select the relevant user role category to which the users will be assigned from.

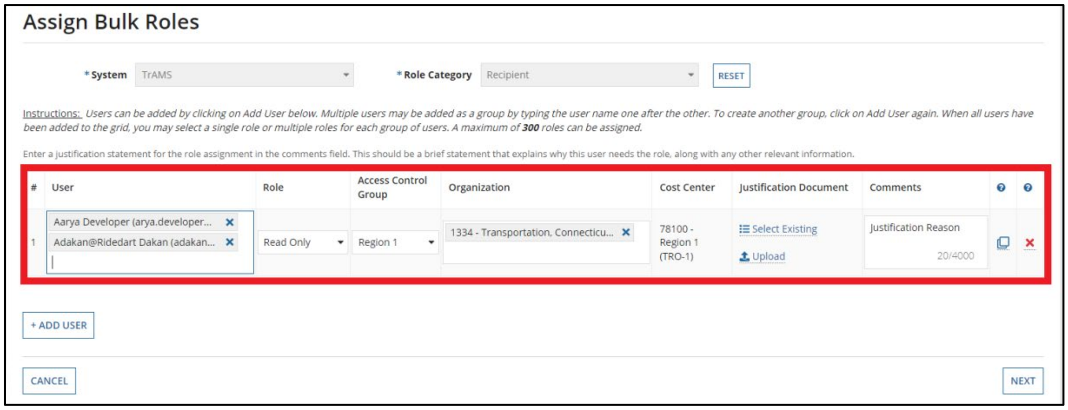


5) Once the role category is selected, the user manager can add users clicking on the link "**Add user**". Multiple users may be added as a group by typing the username one after other. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. To create another set of users, click on **Add User** again.

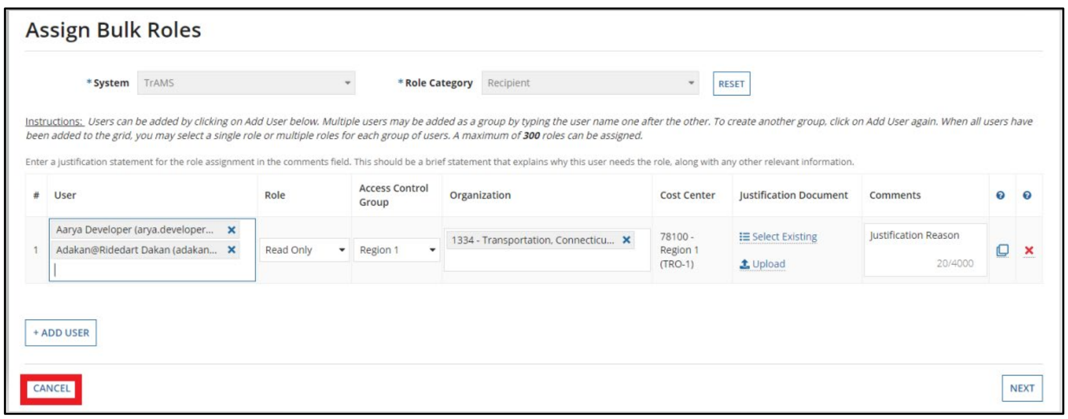


6) The logged in user is given an option to copy the same set of role combination in a new row and can add more roles or organizations in

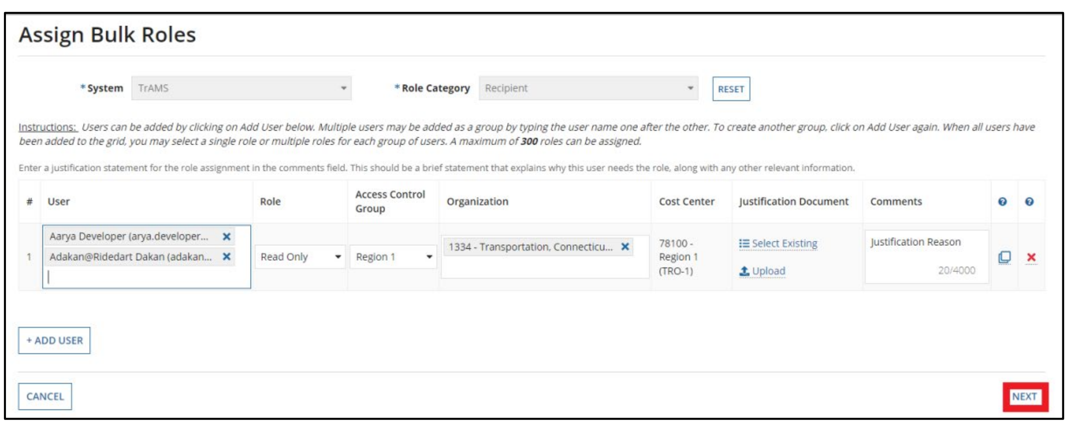
addition to the copied set. After that he can select the users in user column like step 4.



7) The logged in user will have the option to cancel this process at any time by pressing the cancel button in the lower left-hand corner of the screen.

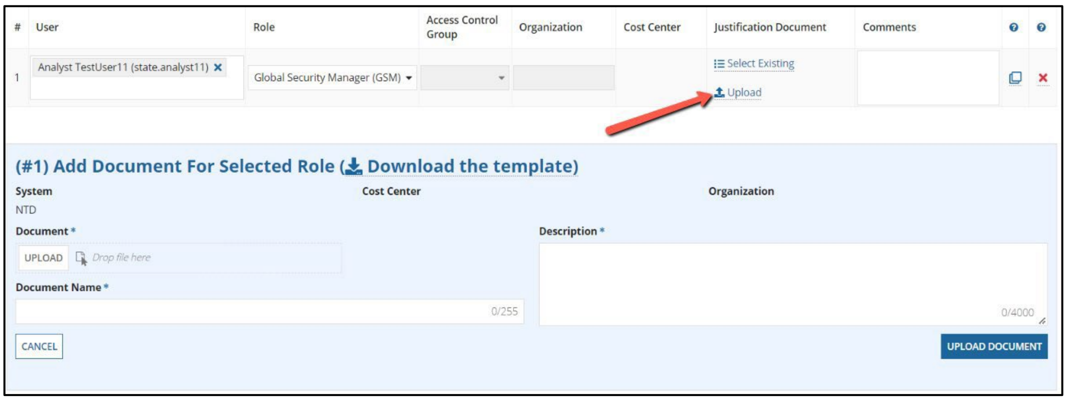


8) Once the logged in user has added all users to be assigned new roles, click the **Next** button to navigate to the **Confirm Bulk Role Assignment** page.

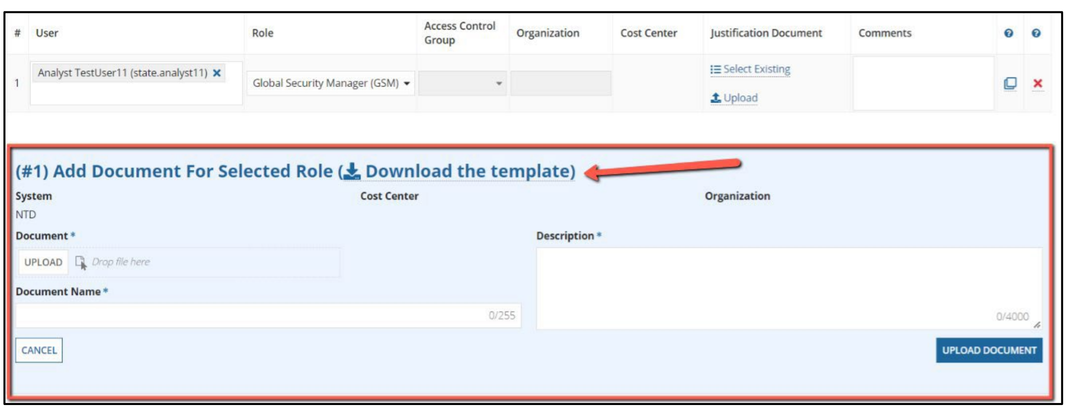


9) On the **Confirm Bulk Role Assignment** page, the logged in user will be able to confirm the bulk assignments. Should a user be assigned a role that they are not supposed to be assigned to, the user manager can go back to the **Assign Bulk Roles** page and remove any necessary users or roles by clicking the **Back** button.

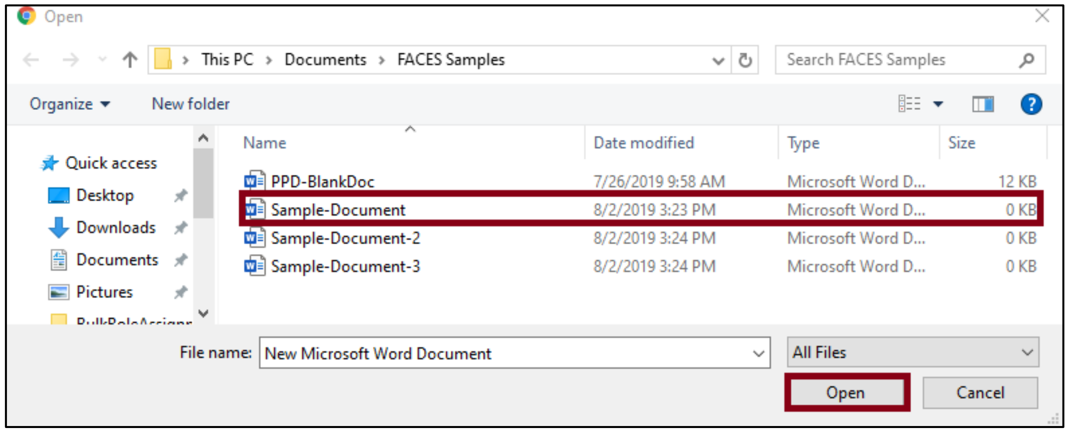
10) If desired, the **Confirm Bulk Role Assignment** page will prompt the user manager to upload a justification document to be attached for confirming the roles. Click the **Upload** button to select a single justification document to upload for all roles.



11) If a User wants to upload a justification or delegation of authority document, they can use the **Add Document for Selected Role** section. Users can download the Justification Document template using the link available in that section. Please follow the instructions within the document on how to complete the Justification Document.

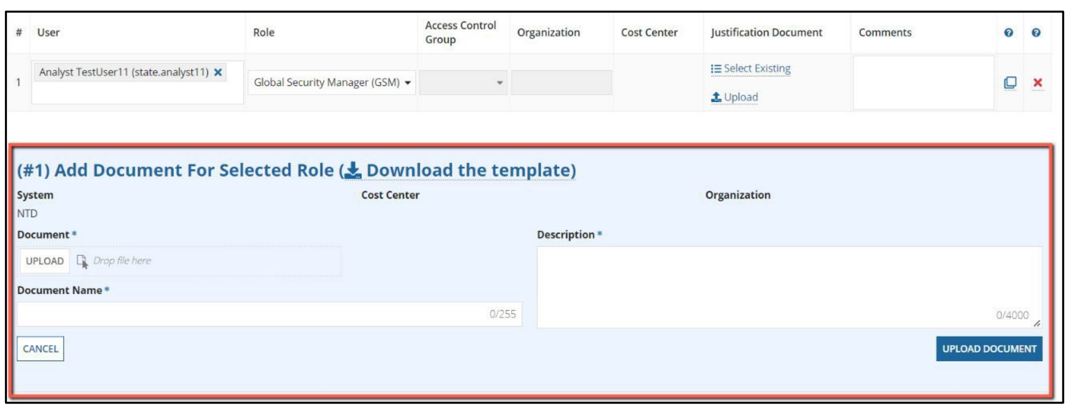


12) Click the **Upload** button in that section, select the justification document that you wish to upload in the Windows file browser and click open.



13) After selecting the justification document to upload, the user manager may delete that document upload and select again by hovering over the document icon and pressing the below displayed icon.

14) After the upload is finished, the user manager will have to give a title and brief description of the justification document before clicking the **Upload Document** button to finish the bulk role assignment.



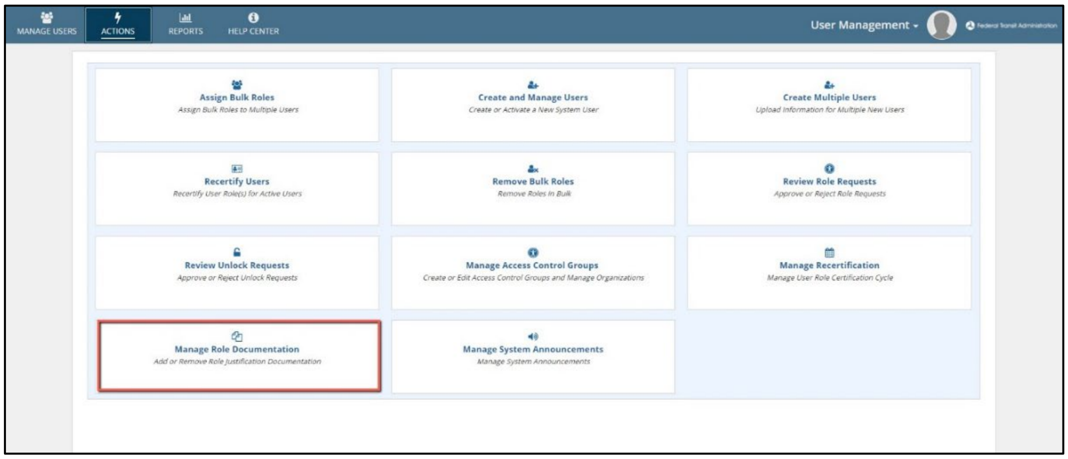
15) After clicking the **Upload Document** button, the request will be processed, and the user manager will be returned to the **Actions** page.

6.2.3 Action: Manage Role Documentation

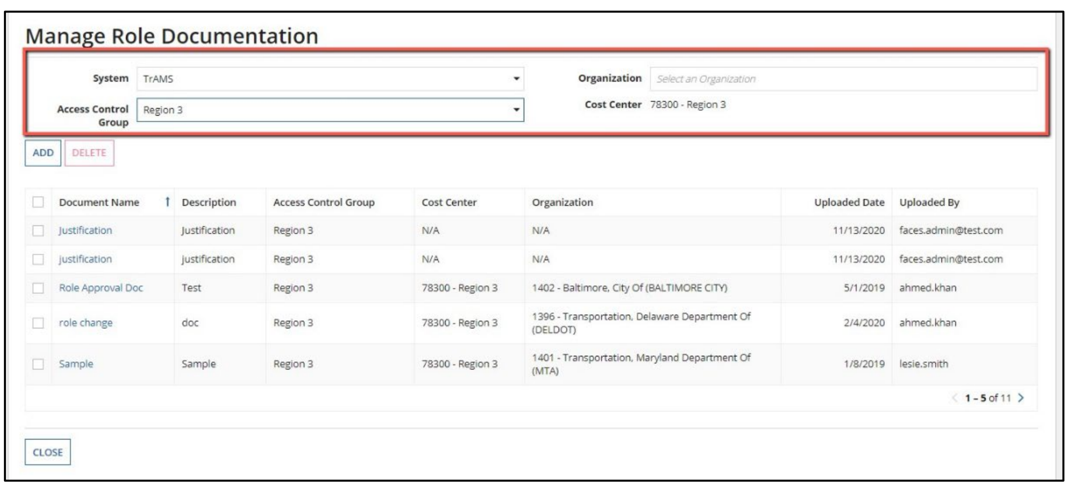
Roles can have an optional justification document for their assignment to a specific user. FACES has incorporated a Justification Document template that can be downloaded and completed. The Justification documentation can be uploaded in advance of role assignment via the ***Manage Role Documentation*** action or uploaded at the time the role is added on the ***Manage Roles*** form as shown in section 6.2.1. At the time of upload, documentation is tagged to the user's organization. During role assignment, the document is then tagged to the specific role and the specific user. A single document can be used for any combination of roles and users (presuming these roles and user are mentioned within the document).

To upload role documentation in advance of role assignment:

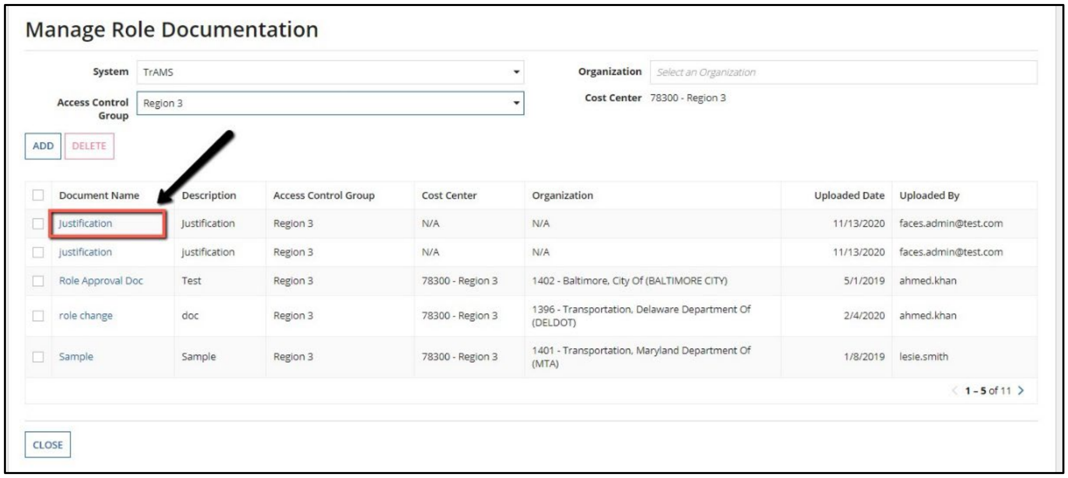
1) Select ***Manage Role Documentation*** from the **Actions** tab.



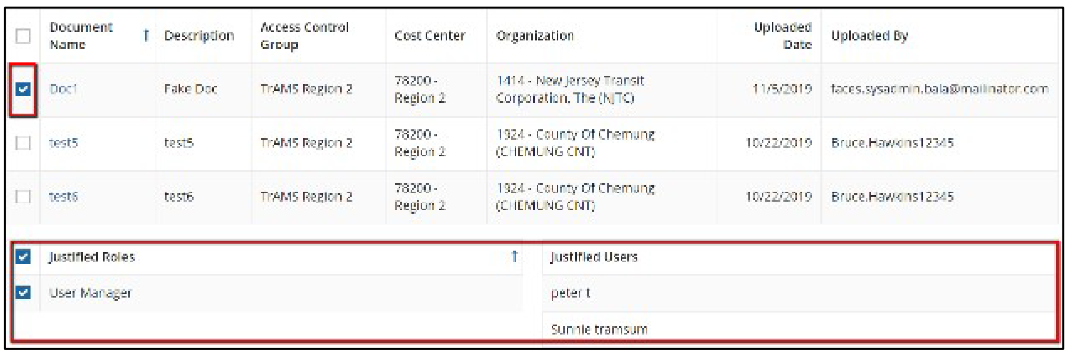
2) The **Manage Role Documentation** page displays available role documents. User Managers can view, add, or delete documents for their organization(s). Validation Analyst and LSMs can view, add, or delete documents for their Cost Center(s) and any organization(s) within their Cost Center(s).



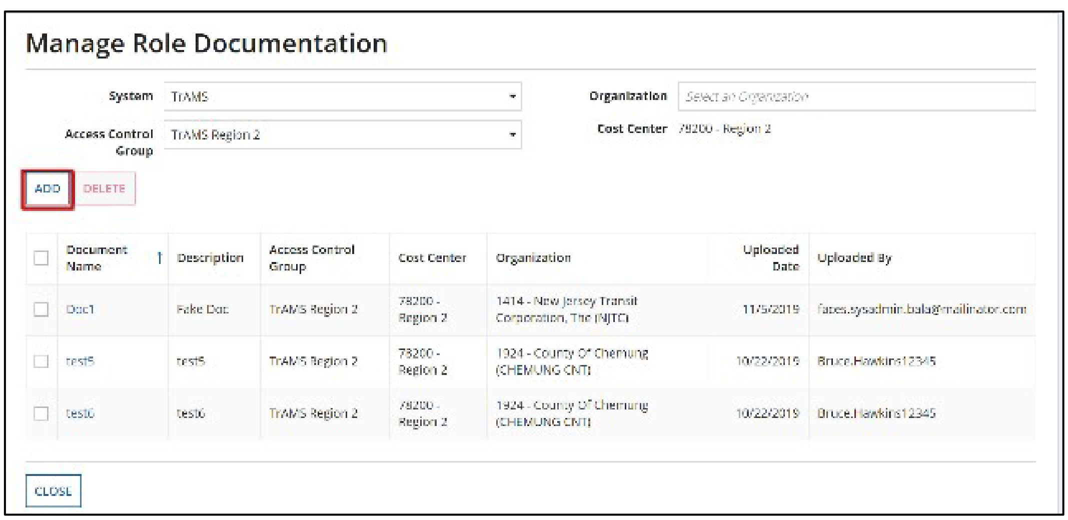
3) To download a copy of a document, simply click the document name link.



4) To view a list of user roles and user tied to an existing document, click the checkbox next to the document record. Beneath the document grid a list of justified roles will display. Click a specific role name to show all users with that role.

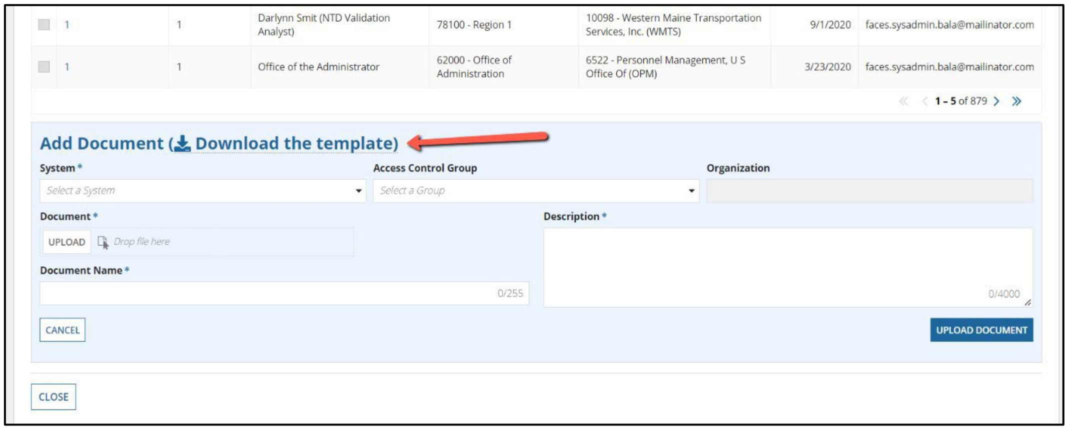


5) To upload a new document Click ***Add***.

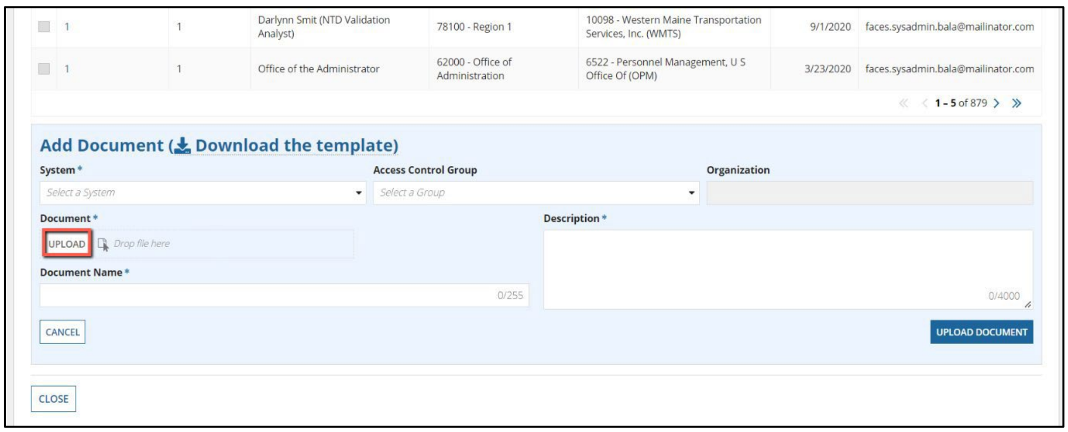


6) The ***Add Document*** section will display beneath the list of available documents. Users can download and use the Justification Document

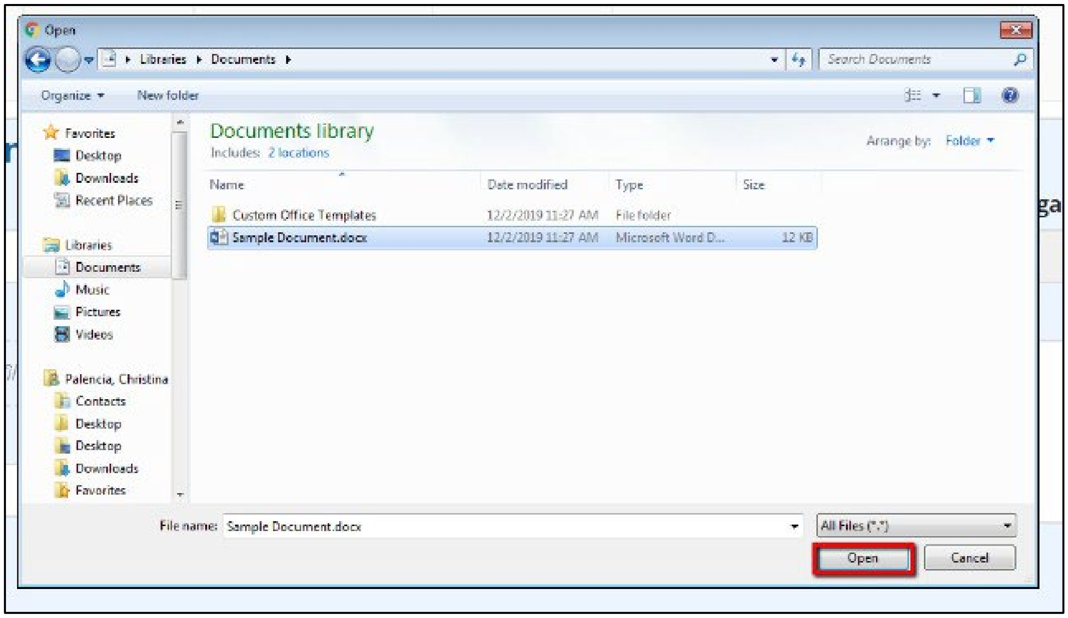
template link available. Please follow the instructions within the document on how to complete the Justification Document.



7) Click ***Upload*** to browse for justification documents to add to the document repository.



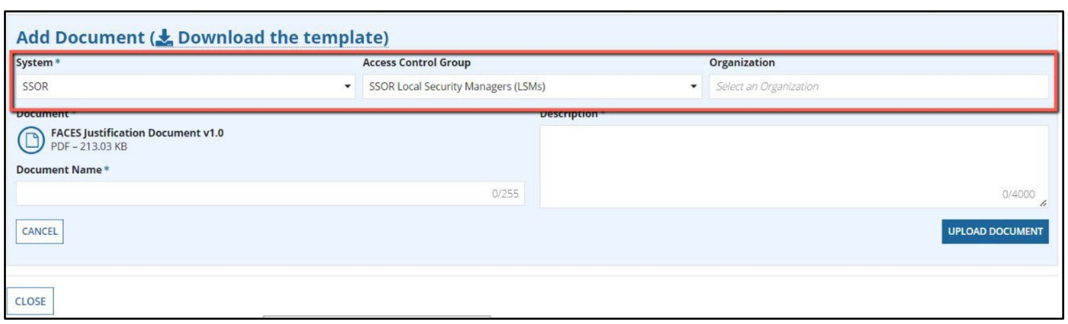
8) Using the Windows browse function, find and click the document to upload. Then click ***Open.***



9) The selected document will be uploaded.

10) To select a different document, hover over the document file name and click the "X" that displays. You can then click ***Upload*** to choose a new document.

11) If the user is a User Manager for a single organization, the **System**, **Access Control Group**, and **Organization** fields will be assigned by default to the user's organization. Validation Analyst, LSMs and GSMs may need to populate some of these fields.

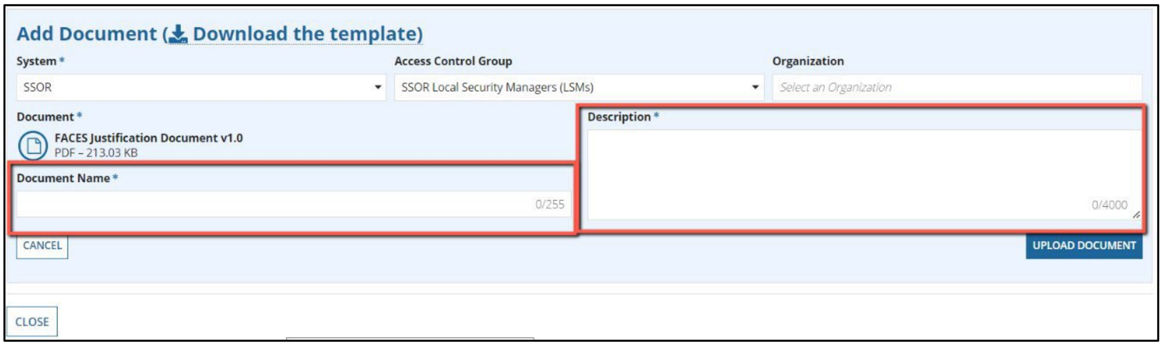


12) This page requires descriptive information to be entered to make the document accessible to other users and to explain the document contents.

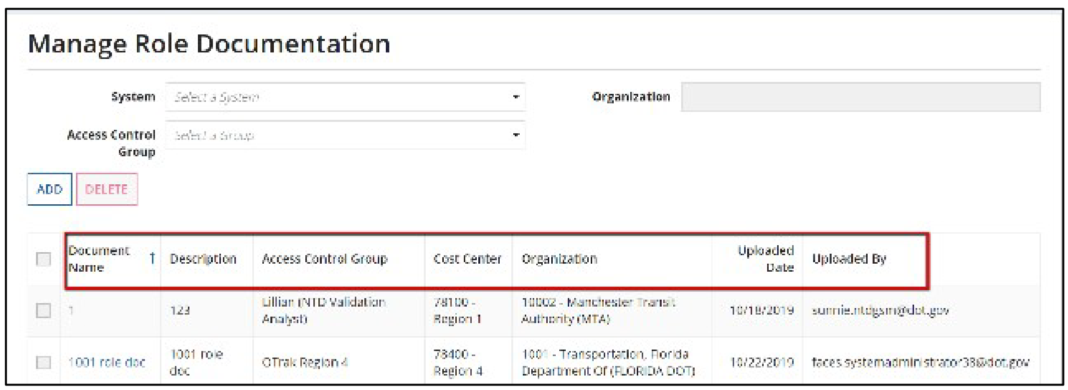
    a. Document Name: A clear document name is essential for other users to know what the document's purpose and coverage. Document names cannot exceed 255 characters.

b. A description that provides even more details about the document’s intent, content, etc., is also advisable. Descriptions cannot exceed 4000 characters.

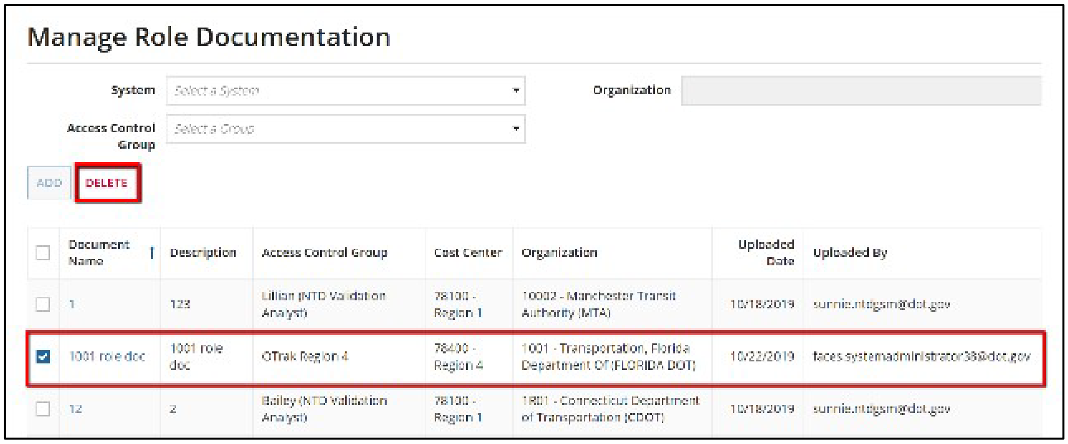
Once the information for the document is finalized, click ***Upload Document***.



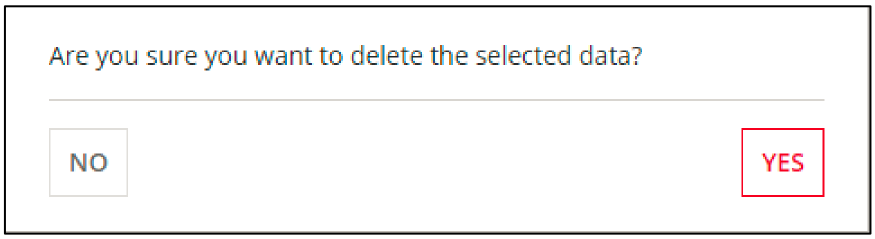
13) The document is added to the list of available documents with its Document Name, Description, Access Control Group, Cost Center, Organization, Upload Date, and the UserID of the person who uploaded it.



14) To remove a document from the system, the user simply highlights the document to be removed by selecting the check box associated with it and clicking ***Delete***. Users can only delete documents that have not yet been selected to support user role assignment. Only one document can be deleted at a time.



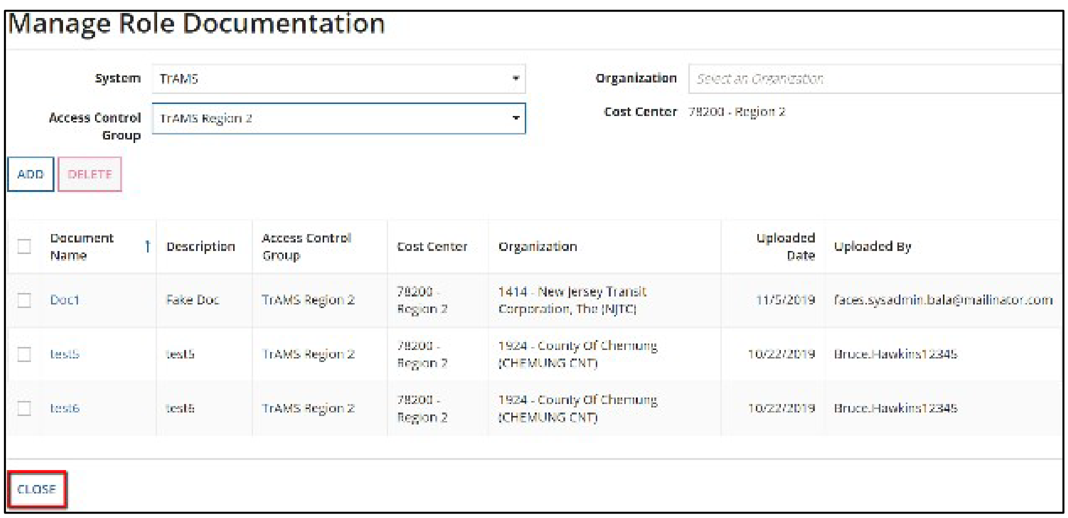
15) A dialog box displays that requires the user to confirm the deletion.



16) Click ***Yes*** to delete the document. Click ***No*** to cancel.

17) Once a document is deleted, the screen will refresh, and the remaining documentation displays on the **Manage Role Documentation** page.

18) If no further documentation needs to be uploaded or removed, click ***Close*** to return to the **Actions** tab.

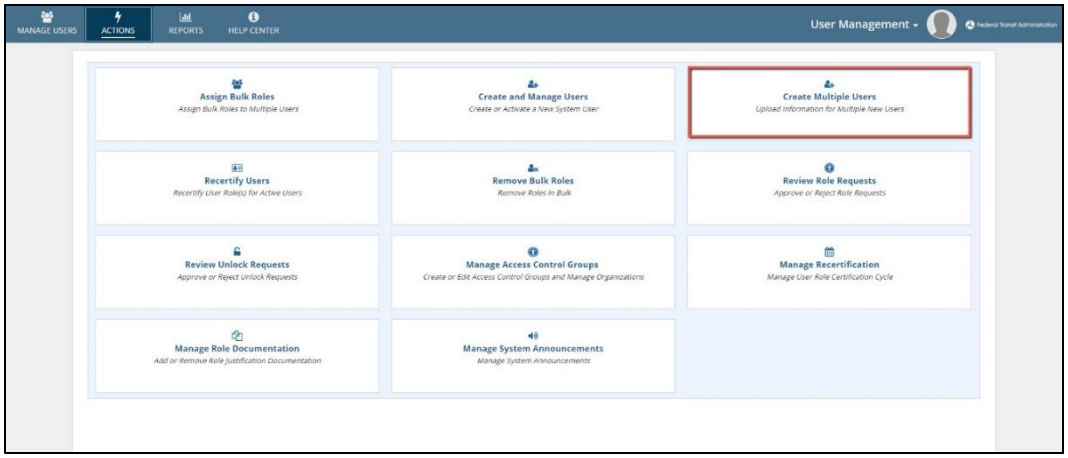


6.2.4 Action: Manage Role Documentation

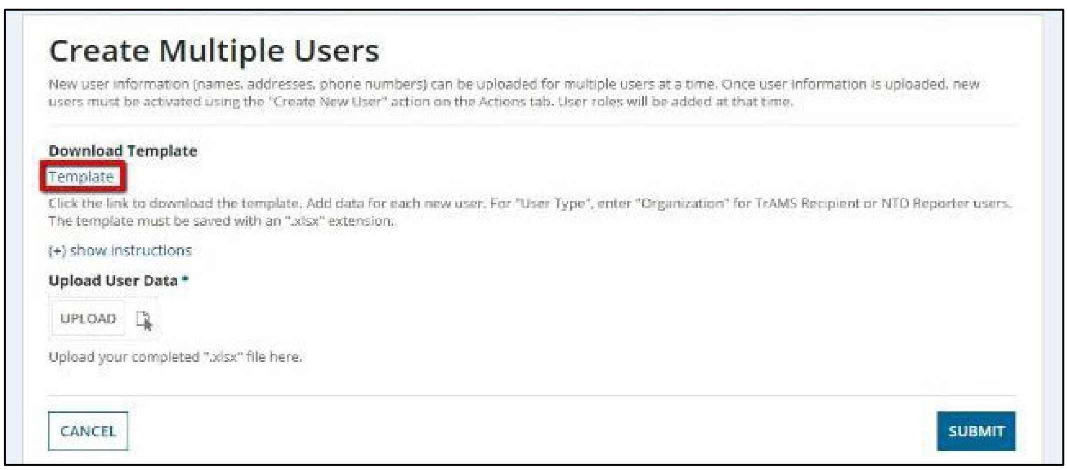
If more than one organization or external user needs to be created, the **User Manager**, **Validation Analyst, LSM,** or **GSM** may bulk load their profile information into the system using a Microsoft Excel file. A file template is provided by the system and must be used. FTA users cannot be uploaded through this action. The upload process will perform data validations and will only upload users that pass all validations. This action is useful when new organizations are added to your system and many users need to be imported at once. At this time, user roles must be added separately using the standard ***Manage Roles*** form.

To upload multiple user information at once:

1) Click the ***Create Multiple Users*** from the **Actions** tab.



2) Download the user information template by clicking the hyperlink that says ***Template***.

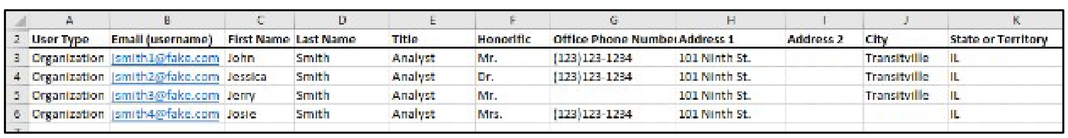


3) The template will contain the following fields for user data. Almost all fields are required. In the template for each user provide the following details for each new user:

Field	Required	Data Entry Rules
User Type	Yes	Must be Organization, DOL, Auditor, or Contractor.

Email (username)	Yes	Entry must be a valid email entered in all lowercase characters. This
First Name	Yes	Cannot contain any special characters (e.g. $) or numbers.
Last Name	Yes	Cannot contain any special characters (e.g. $) or numbers.
Title	Yes	Must not exceed 255 characters.
Honorific	Yes	Must be Mr., Mrs., Ms., or Dr. (*periods required*).
Office Phone Number	Yes	Must be formatted like a phone number (e.g., (555) 555-5555). Cannot be just a 10-digit number (e.g. 5555555555).
Address 1	Yes	Must begin with a street number (e.g., “1207 Maple St”) or a PO (e.g., “PO Box 412”).
Address 2	No	
City	Yes	Cannot contain special characters (e.g. $) or numbers.
State or Territory	Yes	Must be a verified 2-character US state or US territory abbreviation.
Zip Code (5 digits)	Yes	Must be a 5-digit number. If the leading zeros are being stripped from '.xlsx' document, begin the zip code with an apostrophe (e.g. '01234).
Company	No	Must not exceed 255 characters.
Department	No	Must not exceed 255 characters.

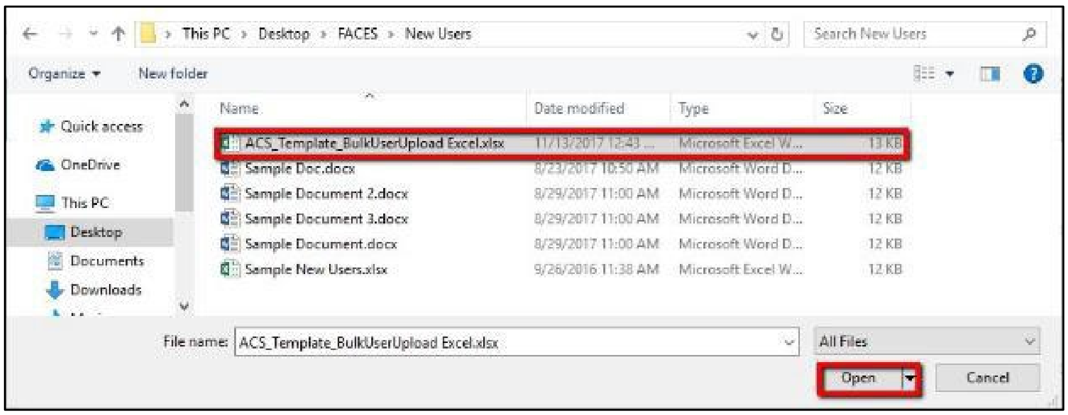
4) The file must be saved with an “.xlsx” file extension. (A sample file with four users is shown below.)



	A	B	C	D	E	F	G	H	I	J	K
2	User Type	Email (username)	First Name	Last Name	Title	Honorific	Office Phone Number	Address 1	Address 2	City	State or Territory
3	Organization	jsmith1@fake.com	John	Smith	Analyst	Mr.	(123)123-1234	101 Ninth St.		Transitville	IL
4	Organization	jsmith2@fake.com	Jessica	Smith	Analyst	Dr.	(123)123-1234	101 Ninth St.		Transitville	IL
5	Organization	jsmith3@fake.com	Jerry	Smith	Analyst	Mr.		101 Ninth St.		Transitville	IL
6	Organization	jsmith4@fake.com	Josie	Smith	Analyst	Mrs.	(123)123-1234	101 Ninth St.			IL

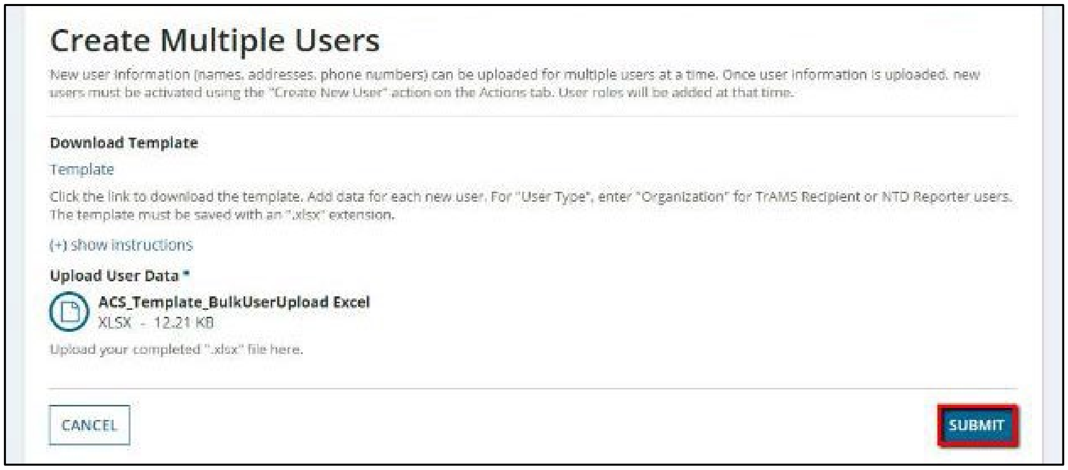
5) When the file is ready to be uploaded, click ***Upload*** on the **Create Multiple Users** page to locate the Excel (.xlsx) file.

6) Use the Windows browser capabilities to locate the file to be uploaded. Click ***Open*** to add the file to the system.

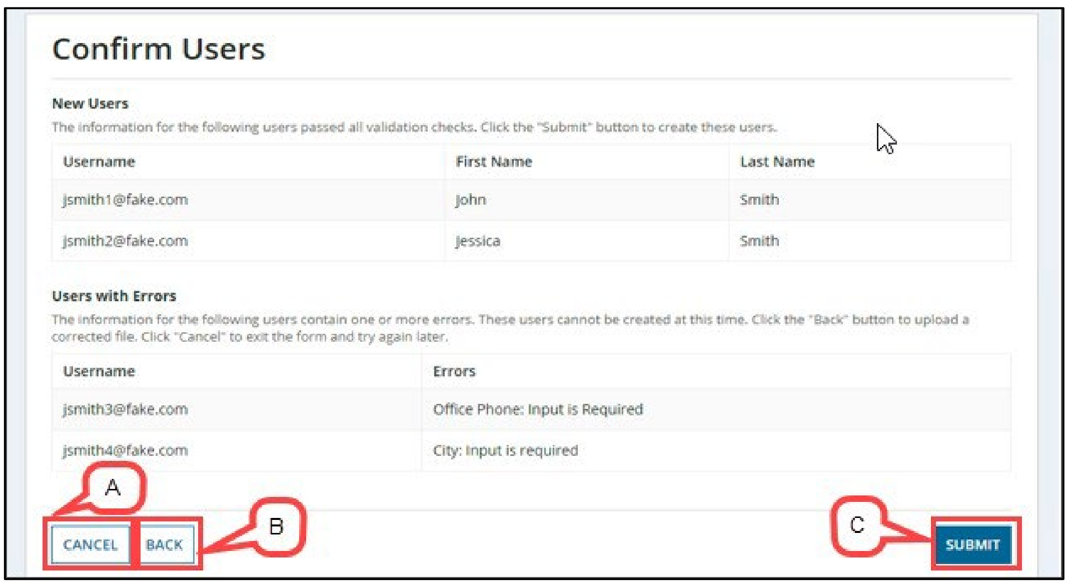


7) The file that was selected is listed on the upload page.

8) Click ***Submit***. This will begin the data upload and validation.

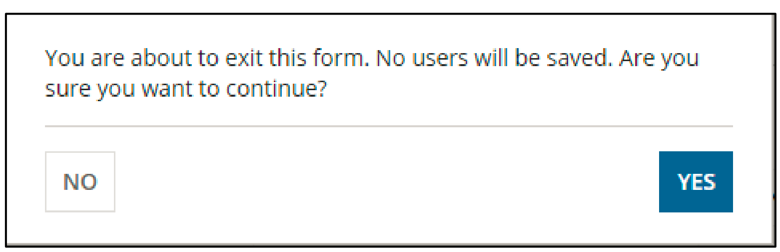


9) The ***Confirm Users*** page will open. The system will display the users in the file that can be uploaded (***New Users***) and the users that have data issues (***Users with Errors)***. For each user with issues, specific error messages will be given to help correct the user data.

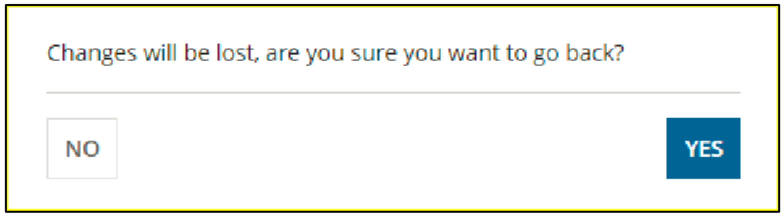


10) The user may:

   a. Select ***Cancel*** to return to the **Actions** page. Click ***Yes***.

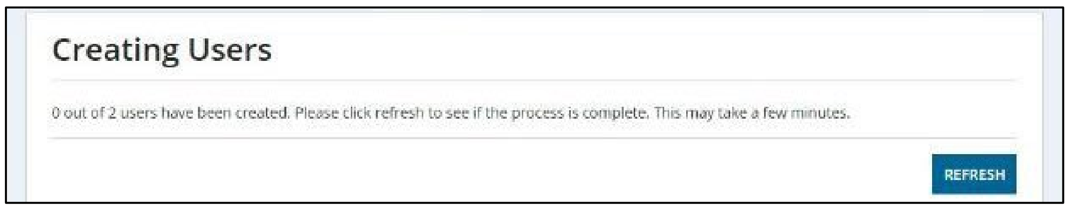


   b. Select ***Back*** to return to return to the previous page and select a new file. Click ***Yes***.

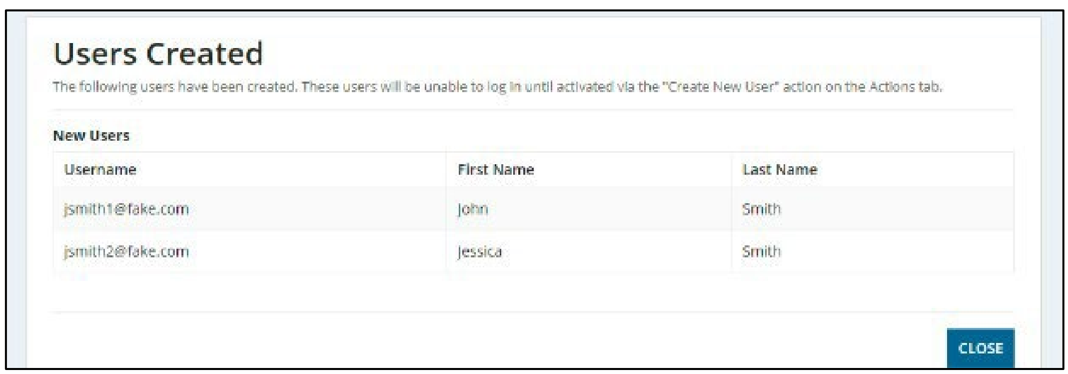


c. Click ***Submit*** to confirm the users and complete the upload of all users that passed validation checks. Only users that passed validation will have user records created.

11) The **Creating Users** form will display. Click ***Refresh*** to see how many users have been created. The process may take several minutes.

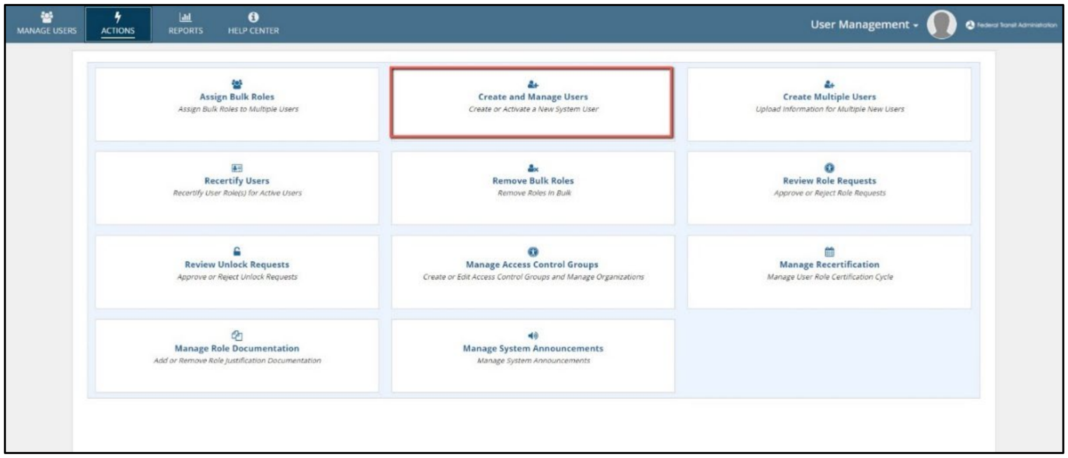


12) Once the users have been added to the system, clicking ***Refresh*** will display the **Users Created** screen. Click ***Close*** to return to the Actions tab.

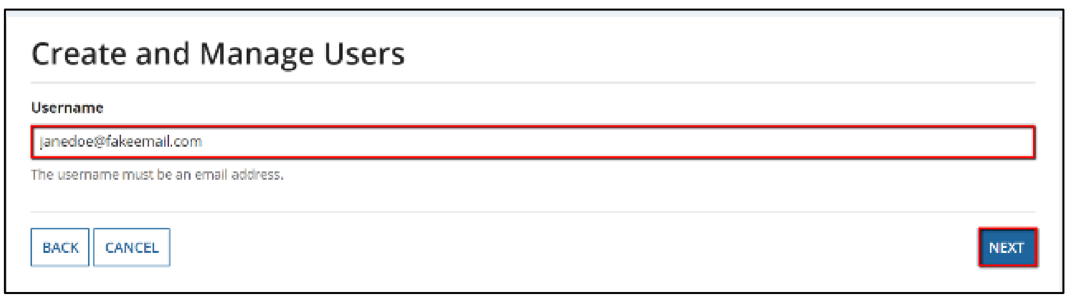


13) To finalize user setup, the **User Manager** will need to locate each user to add user roles. Users will be unable to login until roles are added. The same individual that uploaded the user data does not need to be the person to activate the accounts. If multiple user managers exist for an organization, this responsibility can be shared.

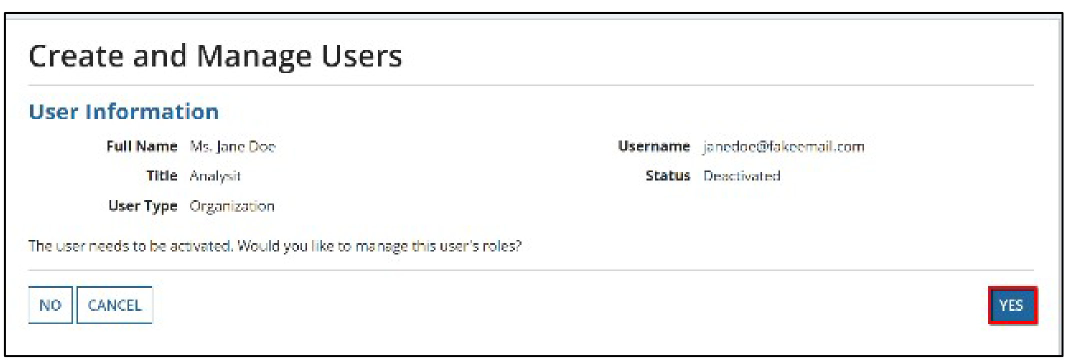
14) To locate a new user to finalize, go to the ***Create and Manage Users*** action.



15) Select the appropriate user type, enter the user's username, and click ***Next***.



16) A page will display a message that the user needs to be activated. You will be given the option to navigate to ***Manage Roles*** for that user. Click ***Yes*** to proceed to ***Manage Roles.***



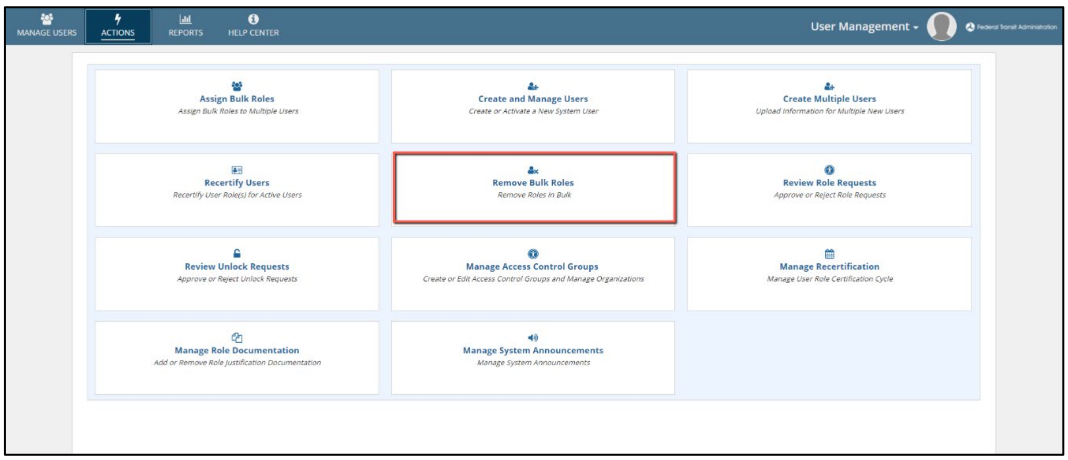
17) Follow the standard process for adding roles to the user and then click ***Activate.*** The user will be notified that their account has been established at this point.

6.2.5 Action: Remove Bulk Roles

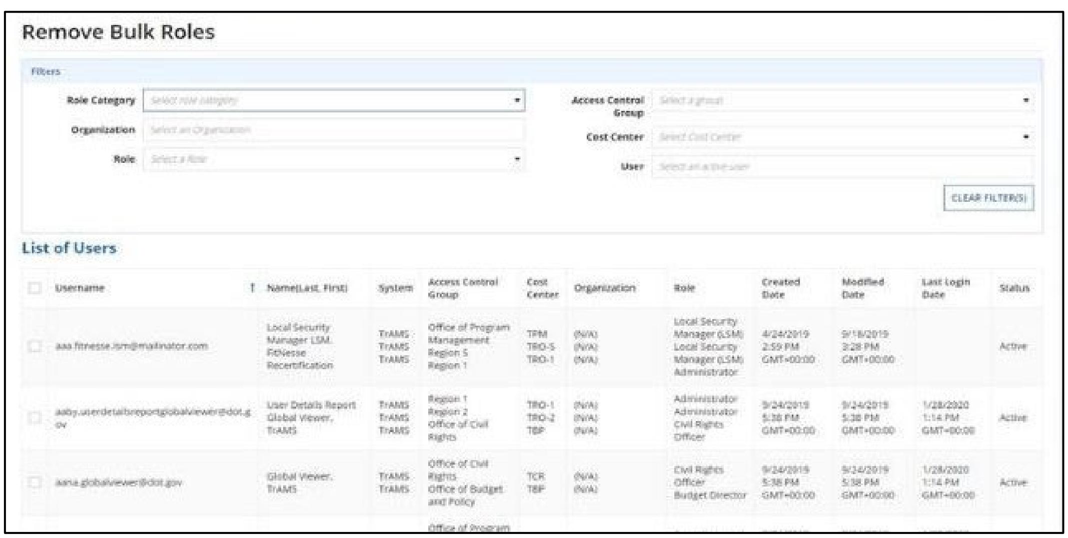
If more than one user or external user's user roles needs to be removed from the system, the **System Admin**, **Global Security Manager**, **Validation Analyst**, **LSM** may remove user roles through this action. The role removal process will provide validations and will only allow users to remove the user roles that are not valid for them anymore.

To remove bulk roles at once:

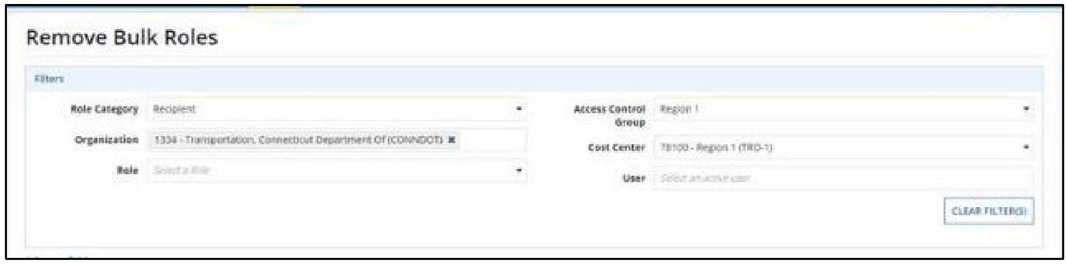
1) Click the ***Remove Bulk Roles*** from the **Actions** tab.



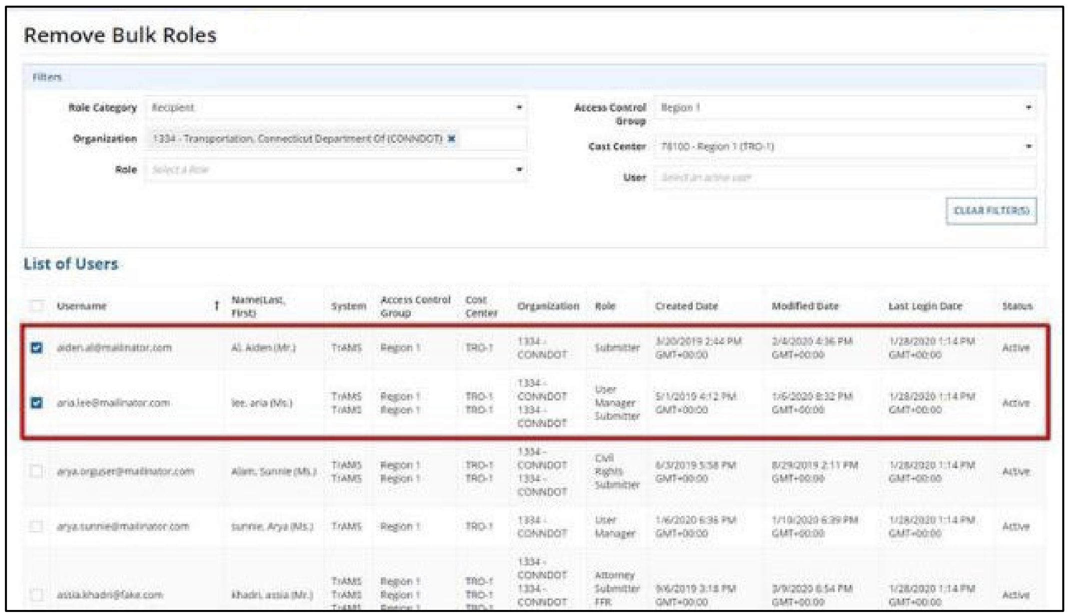
2) The **Remove Bulk Roles** page displays the available users with existing roles they are assigned with can be removed.



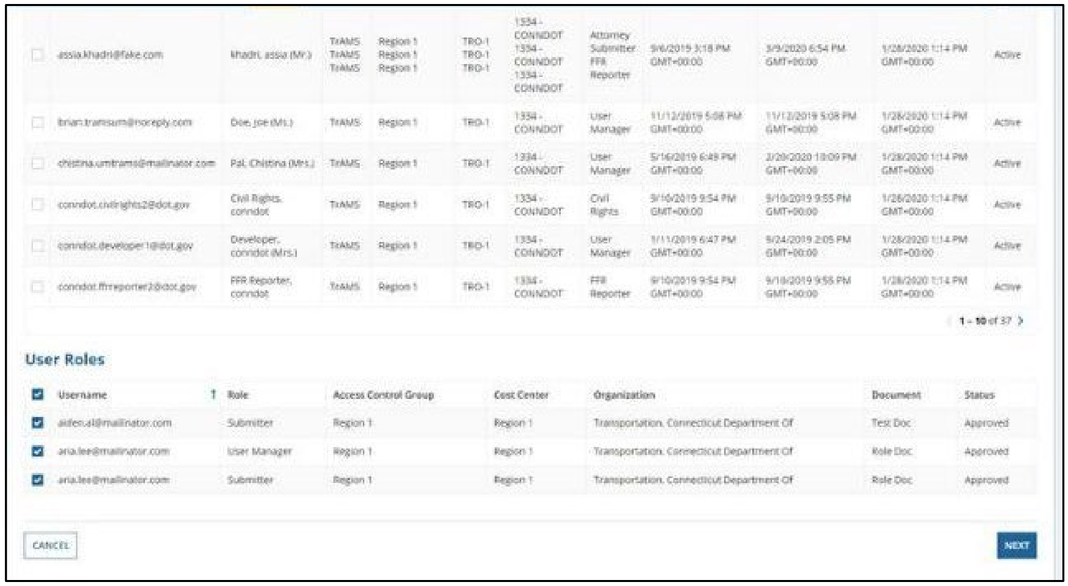
3) The user is provided with filters to narrow down specific users.



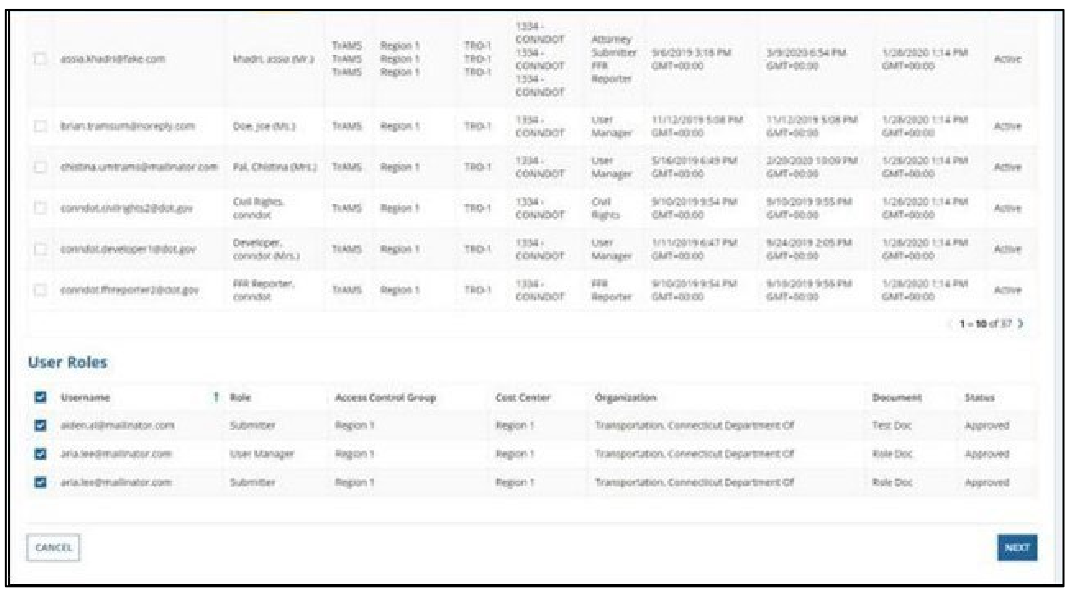
4) Once filters have been applied, the user can select multiple users by clicking anywhere on user record row from the **List of Users** grid to see what roles they currently have; selected users are highlighted blue. Clicking on a selected user record again will deselect that user.



5) The user will have the option to cancel this process at any time by pressing the **Cancel** button in the lower left-hand corner of the screen.



6) The user can select multiple roles for multiple users by clicking anywhere on the rows from **User Roles** grid to remove the roles from the system. Clicking on a selected user role again will deselect that user role. Once the user has selected the users and user roles, click **Next** to navigate to the **Confirm Role Removal** page**.**



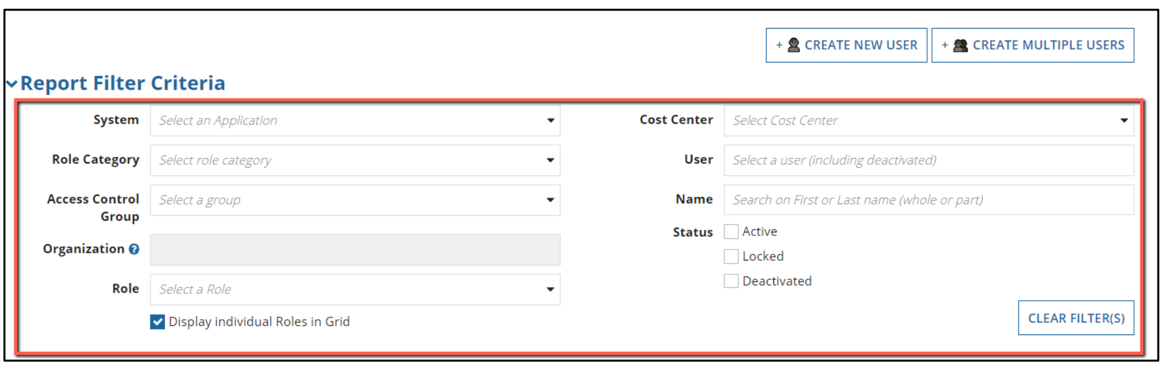
7) On the **Confirm Role Removal** page, the user will be able to confirm the bulk role removal by clicking **Confirm**. The logged in user can navigate back to **Remove Bulk Roles** page by clicking the **Back** button if the roles are not supposed to be removed or to remove some more roles. Clicking **Cancel** will not save any changes and take you back to the Actions home page.

8) Click on the **Confirm** button to confirm the changes and finish the Role removal process. The logged in user will now navigate back to the **Actions** page.

6.3. Managing User Records

Once a user has been created, the **User Manager** can manage details for existing users in their organization including managing the users' profiles, updating their roles/privileges, deactivating, and reactivating users, and unlocking user accounts.

1) Click on the **Manage Users** tab.
2) On the **Manage Users** page, enter the search criteria to locate the user that requires any number of changes and click the hyperlink for that user from the list presented. Partial text searches are allowed.



3) The user record will open to the **User Summary** screen. Click ***Related Actions***.

4) From this page, the **User Manager** may ***Edit Profile***, ***Manage User Roles***, or ***Deactivate User***. The ***Reactivate User*** related action will show if the user is deactivated. Likewise, the ***Unlock User*** related action will show if the user is locked and has submitted an unlock request.

6.3.1 Related Action: Edit User Profile

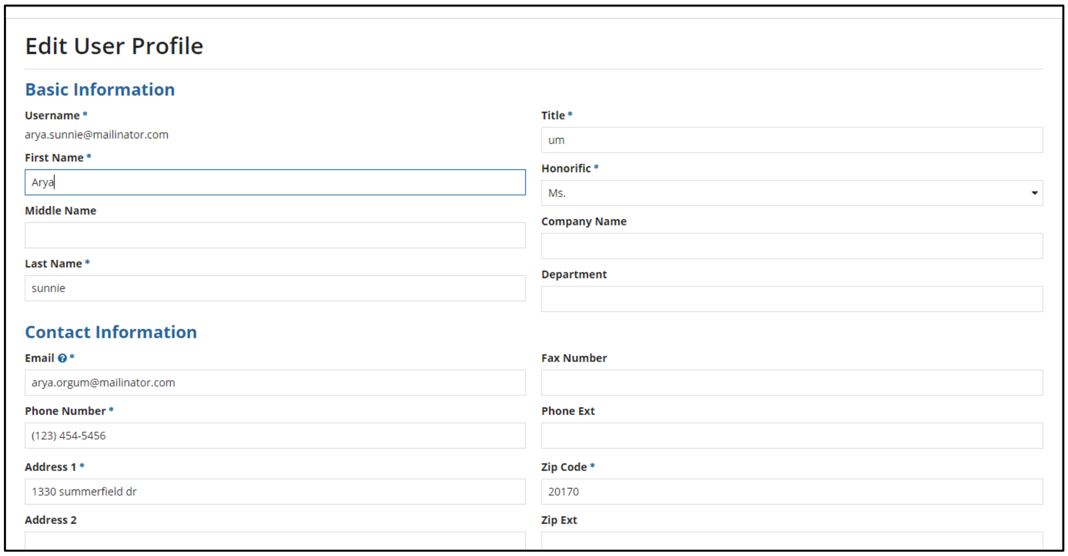
Organization and external user profiles can be edited by the users' management chains (User Manager, LSM, or GSM). All profile fields, except for username, email address and system, can be edited by a user manager.

Note:	*Organization and external users cannot edit email addresses.* If a user needs to update their email address, they need to contact FACEShelp@dot.gov.

To edit a user's profile:

1) Go to the user's record and select ***Related Actions***.
2) Click ***Edit Profile***.

The **Edit User Profile** page will display all previously saved user information details in editable fields.



3) Make any necessary changes. The same field validations that applied at the time of user creation will still apply (e.g., checks for phone number format).

4) Click ***Save*** to update the user's profile with the new and/or changed information. It may take a few minutes for all the information to save.

5) Select ***Cancel*** to return to the **Related Actions** page without saving any changes.

6) All changes should be visible on the ***User Details*** page. Additionally, an audit trail of all changes will be added to the user's ***History*** page.

6.3.2 Related Action: Manage User Roles

Once the user has been created, the **User Manager, LSM, Validation Analyst or GSM** can add or remove roles to adjust a user's access and permissions. Security rules govern which types of roles can be added or removed from a user. **User Managers** can only add or remove roles for their own organization(s). **LMSs and Validation Analyst** can only add roles within their Cost Centers. **GSMs** can add or remove any role within their associated system. To assign roles to a user in multiple organizations or across multiple systems, the **User Managers** from each organization will need to add the corresponding roles. The appropriate **GSMs or LSMs** can be contacted to facilitate role assignment or User Manager coordination. User roles can be added and deleted at the same time.

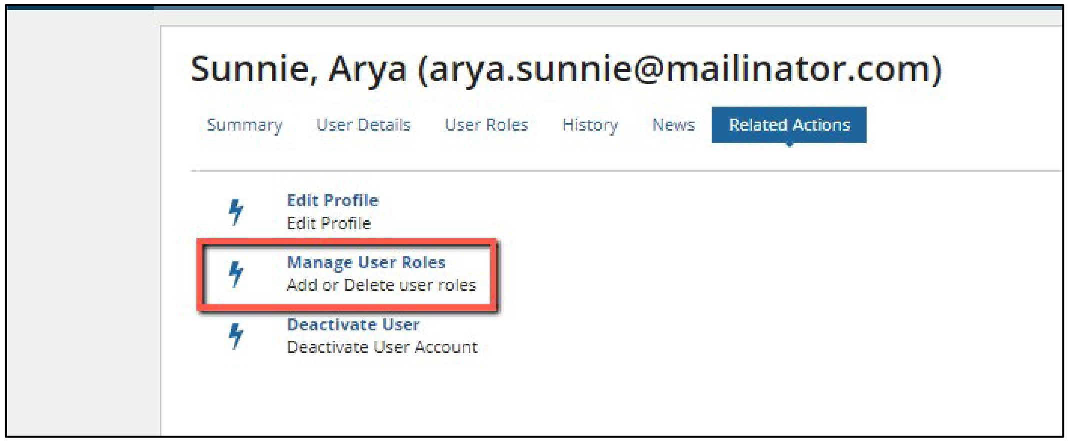
When adding/removing roles, note that users cannot have both Read Only and active roles in the same organization (or Cost Center for FTA users).

For ease in explaining, additions and deletions are presented separately within this document.

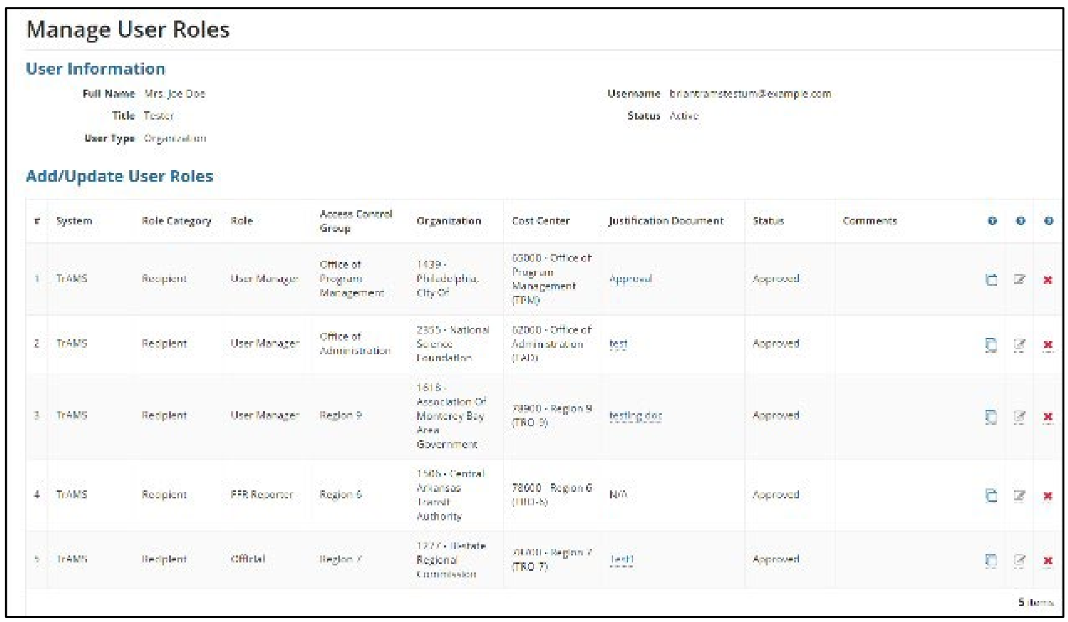
To add roles to a user:

a. Go to the user's record and click ***Related Actions***.

b. Click ***Manage User Roles***.



c. The ***Manage Roles*** page displays. Only roles that the user can manage are visible in the ***User Roles*** table.



d. Select ***Cancel*** at any point in this process to return to the previous page without saving any changes.

e. Click ***Add*** to add a new role to the user.

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments
1	TrAMS	Recipient	User Manager	Office of Program Management	1430 - Philadelphia, City Of	65000 - Office of Program Management (TPM)	Approval	Approved	
2	TrAMS	Recipient	User Manager	Office of Administration	2353 - National Science Foundation	62000 - Office of Administration (TAD)	test	Approved	
3	TrAMS	Recipient	User Manager	Region 9	1618 - Association Of Monterey Bay Area Government	78900 - Region 9 (TRO-9)	testing doc	Approved	
4	TrAMS	Recipient	FFR Reporter	Region 6	1306 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved	
5	TrAMS	Recipient	Official	Region 7	1277 - Bi-state Regional Commission	78700 - Region 7 (TRO-7)	Test1	Approved	

5 items

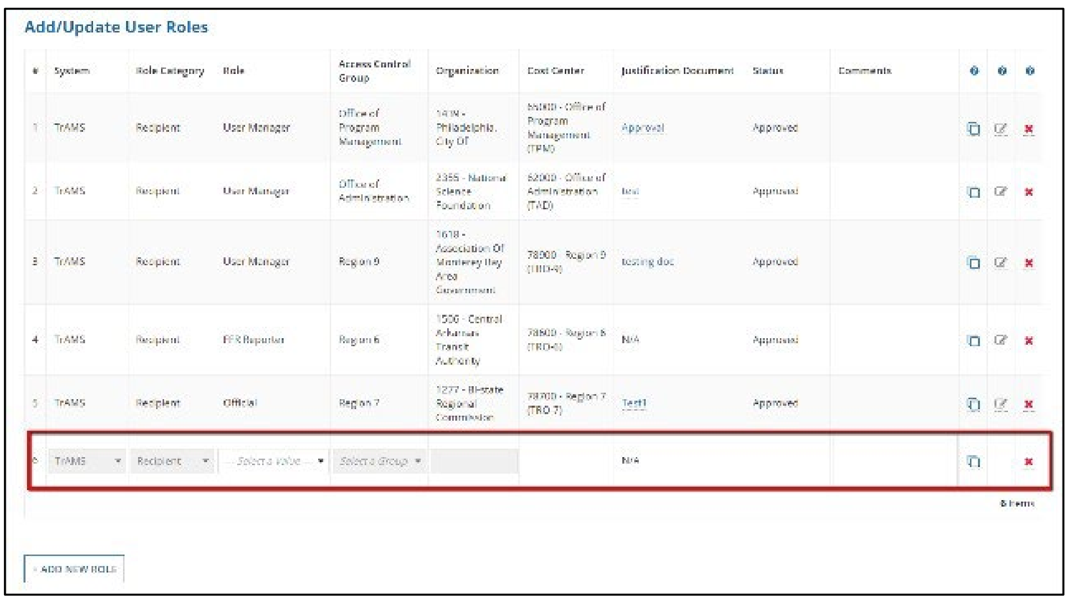
+ ADD NEW ROLE

CANCEL

VIEW HISTORY

SUBMIT

f. The role filters (System, Role Category, Access Control Group, Cost Center, Organization) must be populated for the available roles to display. For most User Managers, these filters will automatically populate, and the fields will be locked on the screen. LSMs, Validation Analyst and GSMs may need to select a Cost Center and Organization for the 'Available Roles' to display.



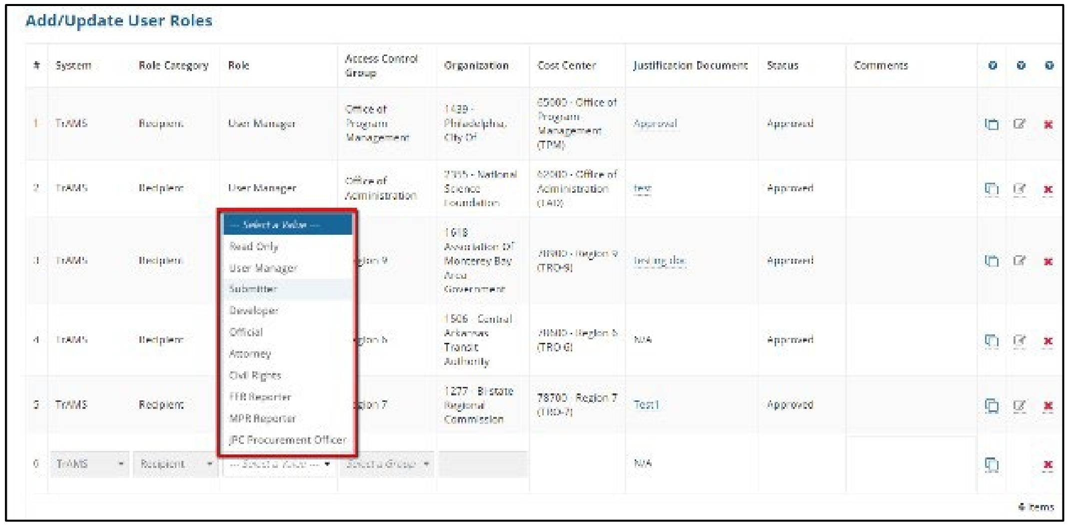
Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments
1	TrAMS	Recipient	User Manager	Office of Program Management	1430 - Philadelphia, City Of	65000 - Office of Program Management (TPM)	Approval	Approved	
2	TrAMS	Recipient	User Manager	Office of Administration	2355 - National Science Foundation	62000 - Office of Administration (TAD)	test	Approved	
3	TrAMS	Recipient	User Manager	Region 9	1618 - Association Of Monterey Bay Area Government	78900 - Region 9 (TRO-9)	testing doc	Approved	
4	TrAMS	Recipient	FFR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved	
5	TrAMS	Recipient	Official	Region 7	1277 - Bi-state Regional Commission	78700 - Region 7 (TRO 7)	Test1	Approved	
6	TrAMS	Recipient	-- Select a Value --	Select a Group			N/A		

6 items

+ ADD NEW ROLE

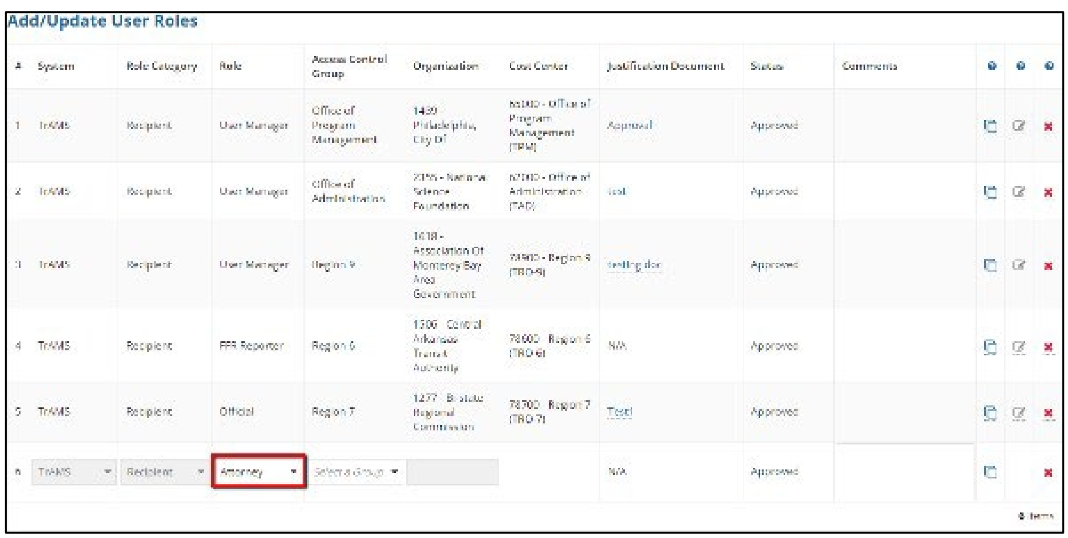
g. Potential roles for the user are listed along with default information about the user's system, role, cost center, etc. In the screenshot below, only roles available to TrAMS Recipients are listed. These roles will be granted only for the Organization that is listed.



h. Roles are further distinguished in terms of whether they require **Approval** and/or a **PIN** for completing select actions within their system(s). Roles that require **Approval** must be approved at a level above the User Manager.

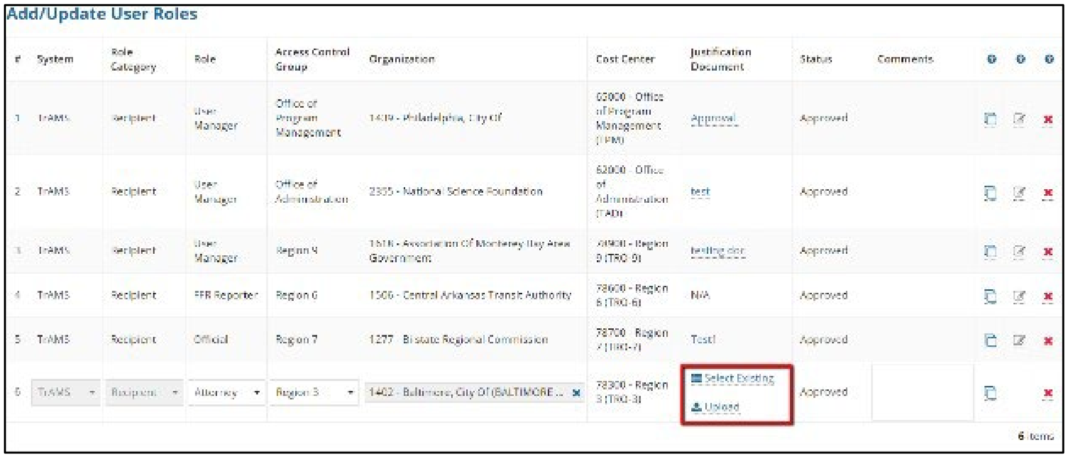
Note:	*Users cannot have a Read Only role and an active role in the same organization. If your user has a Read Only role and needs an active role, you will need to* ***first*** *delete the Read Only role.*

i. Select **one** of the roles presented. Only one (1) role can be added at a time. System specific rules will be enforced. See Appendix B for a list of system specific rules. Click ***Add*** to complete the assignment of a role to the individual user.



j. The user and the updated roles will display. Justification Documentation is optional to upload before a role assignment can be submitted. In those cases, the Add Justification Document section will be displayed. A

Delegation of Authority letter template is available on the FTA public website.



Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments
1	TrAMS	Recipient	User Manager	Office of Program Management	1419 - Philadelphia, City Of	63000 - Office of Program Management (TPM)	Approval	Approved	
2	TrAMS	Recipient	User Manager	Office of Administration	2355 - National Science Foundation	62000 - Office of Administration (TAD)	test	Approved	
3	TrAMS	Recipient	User Manager	Region 9	1618 - Association Of Monterey Bay Area Government	78900 - Region 9 (TRO-9)	testing doc	Approved	
4	TrAMS	Recipient	FFR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved	
5	TrAMS	Recipient	Official	Region 7	1277 - Bi-state Regional Commission	78700 - Region 7 (TRO-7)	Test!	Approved	
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE ...	78300 - Region 3 (TRO-3)	Select Existing Upload	Approved	

6 items

k. To associate a document with the added role, select from the list of available documents by clicking on ***Select Existing*** button.

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments
1	TrAMS	Recipient	User Manager	Office of Program Management	1419 - Philadelphia, City Of	63000 - Office of Program Management (TPM)	Approval	Approved	
2	TrAMS	Recipient	User Manager	Office of Administration	2355 - National Science Foundation	62000 - Office of Administration (TAD)	test	Approved	
3	TrAMS	Recipient	User Manager	Region 9	1618 - Association Of Monterey Bay Area Government	78900 - Region 9 (TRO-9)	testing doc	Approved	
4	TrAMS	Recipient	FFR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved	
5	TrAMS	Recipient	Official	Region 7	1277 - Bi-state Regional Commission	78700 - Region 7 (TRO-7)	Test!	Approved	
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE ...	78300 - Region 3 (TRO-3)	Select Existing Upload	Approved	

6 items

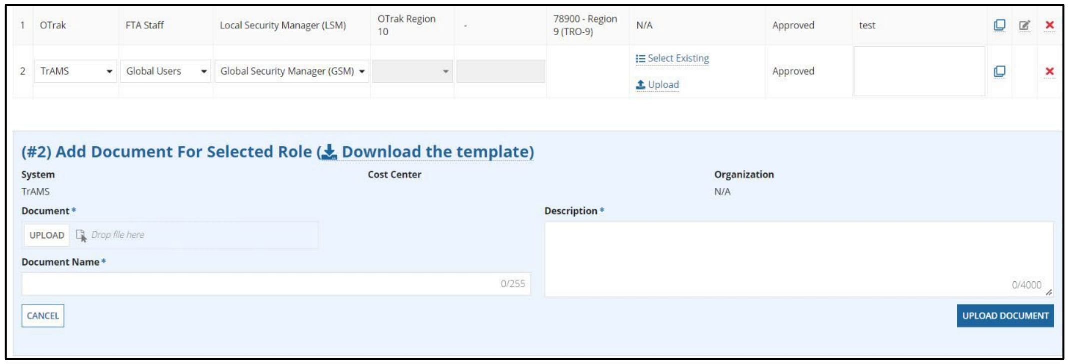
l. If the proper document isn't available, click the ***Upload*** button.

Add/Update User Roles

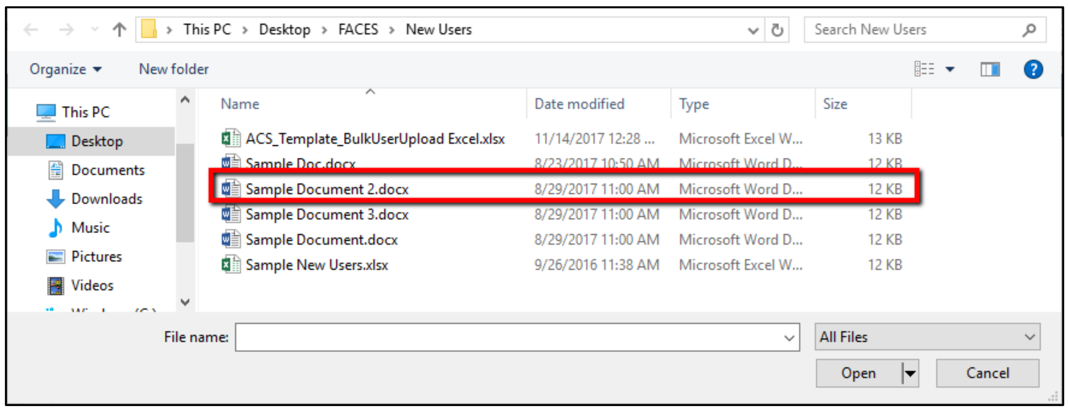
#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments
1	TrAMS	Recipient	User Manager	Office of Program Management	1419 - Philadelphia, City Of	63000 - Office of Program Management (TPM)	Approval	Approved	
2	TrAMS	Recipient	User Manager	Office of Administration	2355 - National Science Foundation	62000 - Office of Administration (TAD)	test	Approved	
3	TrAMS	Recipient	User Manager	Region 9	1618 - Association Of Monterey Bay Area Government	78900 - Region 9 (TRO-9)	testing doc	Approved	
4	TrAMS	Recipient	FFR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved	
5	TrAMS	Recipient	Official	Region 7	1277 - Bi-state Regional Commission	78700 - Region 7 (TRO-7)	Test!	Approved	
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE ...	78300 - Region 3 (TRO-3)	Select Existing Upload	Approved	

6 items

m. Click ***Upload*** to browse for the document to add. Using the Windows browse function, find and select the document to upload. Once the document has been identified, click ***Open***.

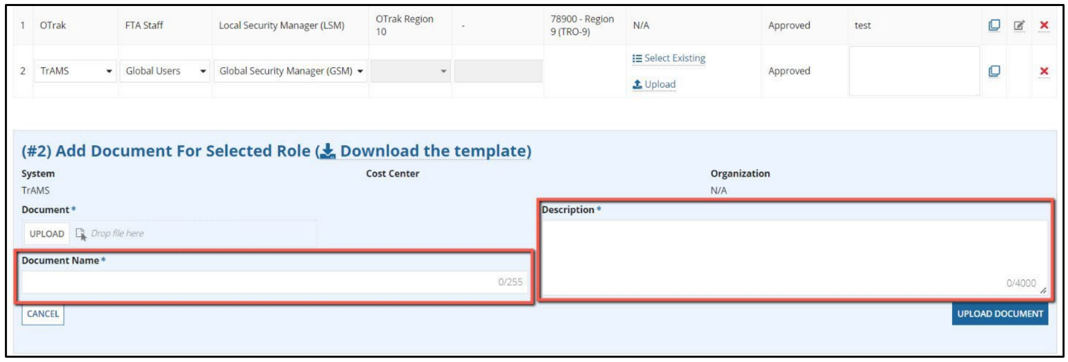


n. Click ***Upload*** to browse for the document to add. Using the Windows browse function, find and select the document to upload. Once the document has been identified, click ***Open***.



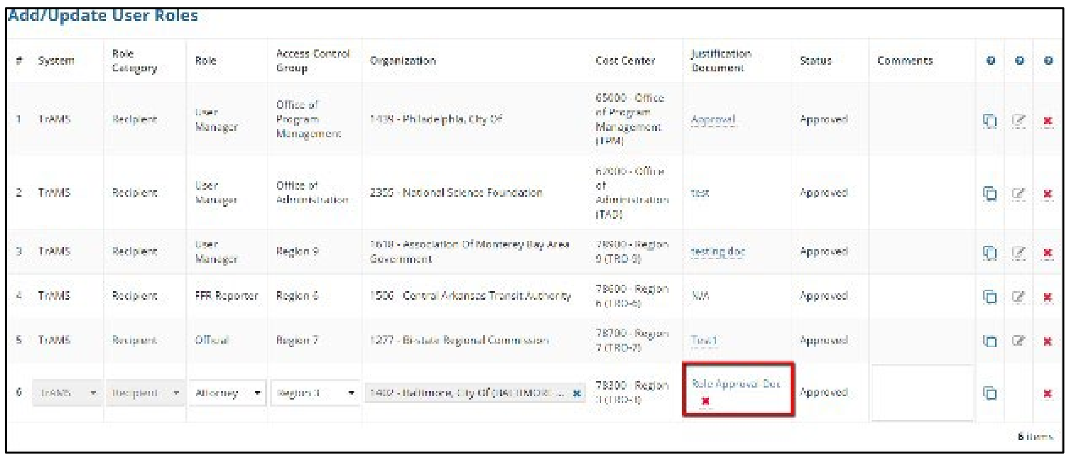
o. The appropriate document will be uploaded.

p. Descriptive information must be entered to make the justification document accessible to other users and to explain what the document contains. A clear document name is essential for other users to know the document's purpose and coverage. A description that provides even more details about the document's intent, content, etc., is also advisable. The maximum characters remaining will show beneath the document name and description fields.



q. Once the information for the document is finalized, click ***Upload Document***.

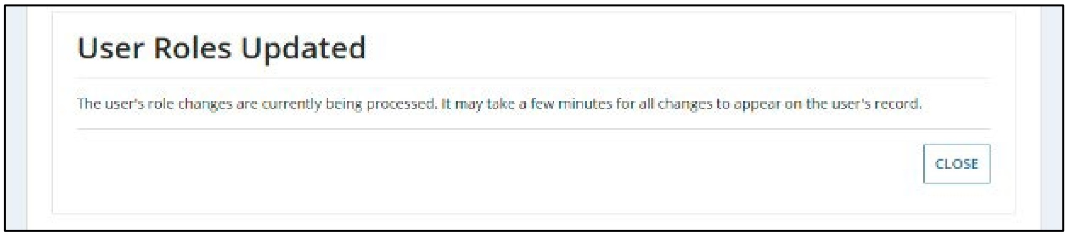
r. The document is added to the list of available documents and is pre-selected as the appropriate document to tag to the new user role.



s. At this point, comments are required to be added into the **Comments** data entry box to complete the use of the document for that role, especially if the document is not obviously associated with the role. Then click ***Save***.

t. Click ***Submit*** to finalize the assignment of the role(s).

u. The **User Roles Updated** page displays a message that the roles are being processed within the system.



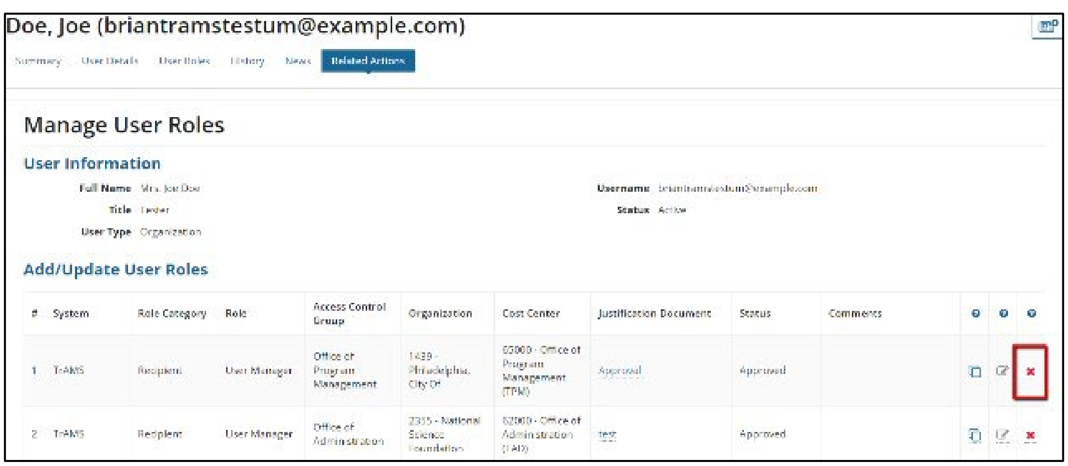
v. Click ***Close***. The **Related Actions** page displays.

6.3.3 Delete A Role

To remove a role from a user:

1) Go to the user's record and click ***Related Actions***.
2) Click ***Manage User Roles***.

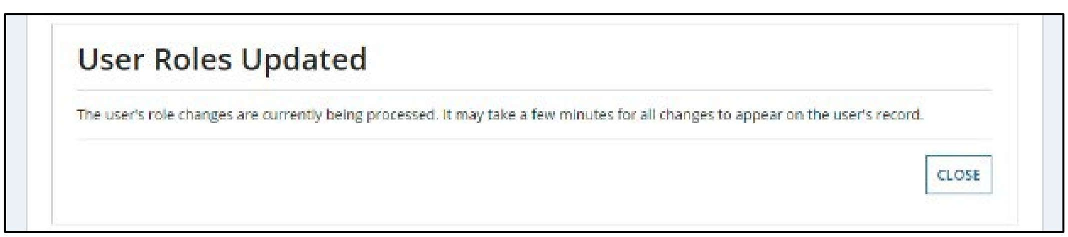
3) Click on the red "X" at the end of the row for roles you want to delete.



4) The *Status* column will change from *Approved* to *Deleted* for each role that is deleted.

5) Once all desired roles have been removed from the user's role list, click ***Submit*** to save the deletions. Click ***Cancel*** to undo any deletions and leave the form.

6) The **User Roles Updated** page will display. Click ***Close*** to return to the **Related Actions** page.



6.3.4 Update Role Documentation

The **User Manager** may further need to manage role documentation or add a role comment for a user. Role documentation can only be updated for roles in “Requested” status. These updates may be necessary if the wrong document was uploaded or additional documentation was requested by the LSM, Validation Analyst or GSM reviewing the role request.

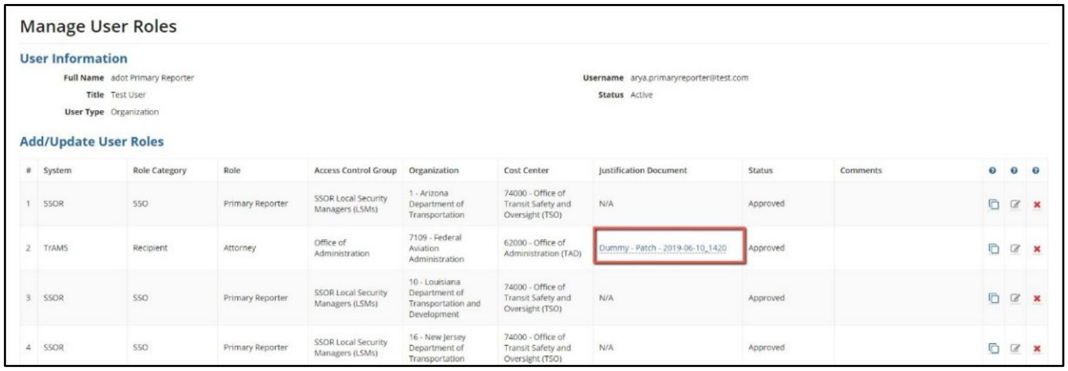
To manage role documentation for a user:

a. Go to the user’s record and click ***Related Actions***.

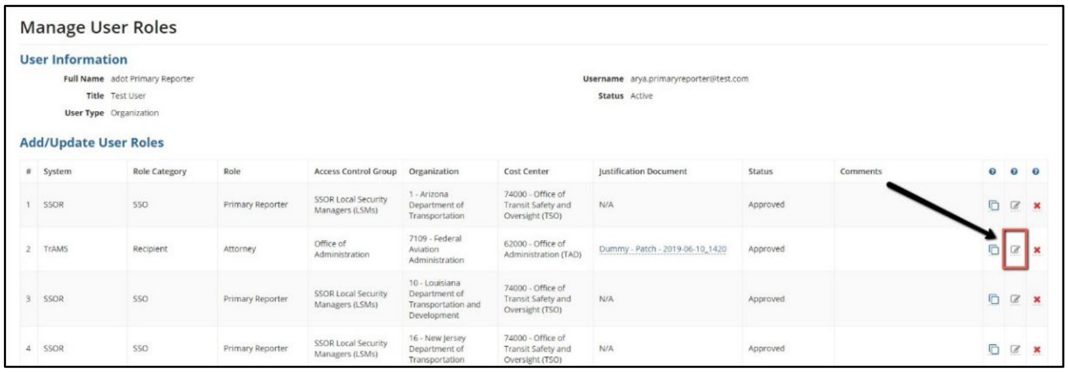
b. Click ***Manage User Roles***.

c. The **Manage Roles** page is displayed, allowing the **User Manager** to manage documentation.

d. The **User Manager** may select the hyperlink for any document to view the contents. The associated document will open within the appropriate application for viewing. Selecting the hyperlink for the document will download the document for review.



e. To switch a justification document for a specific role, click on the **Edit** button next to the appropriate role and then click on the red “X” for the document (s) you wish to delete.

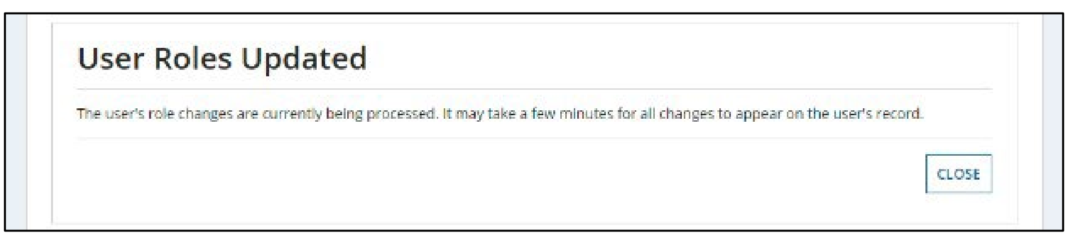


f. At this point, either select an existing document to assign to the role by clicking the required document or click the ***Upload*** button to upload a new document. A Justification Document Template. For more details on how to upload a new document, see either ***Manage Role Documentation*** action or the Add Role section.

g. ***Role Comments*** can be directly added or edited. *Changes will overwrite the existing comment.*

h. Once all changes have been made, click ***Submit***.

i. The **User Roles Updated** page will display. Click ***Close*** to return to the **Related Actions** page.



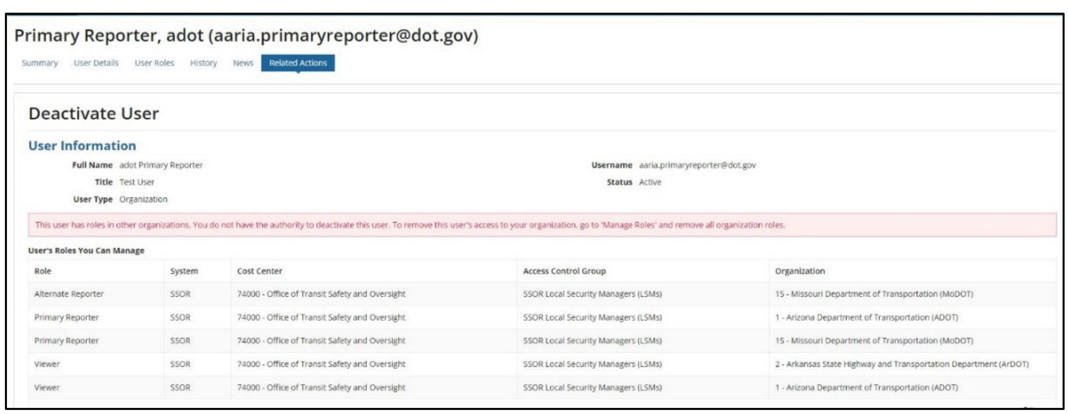
6.3.5 Related Action: Deactivate User

Deactivating a user will deactivate the user across the entire FTA platform – the user will be unable to log in and will have access to all systems (e.g., TrAMS, NTD and DGS) terminated. As part of deactivation, user roles are removed. Users can only be deactivated by individuals who have permission to delete all the assigned roles. For example, if a user is associated with multiple organizations, the **User Manager** for any single organization will not be able to deactivate the user. Instead, the **User Manager** can remove user roles to remove the user's access to their organization, or, in an extreme situation, the **User Manager** can contact their **LSM or Validation Analyst** for further support. *Only users with account status Active or Active (Locked) can be deactivated. A user's status can be found on their User Details page.*

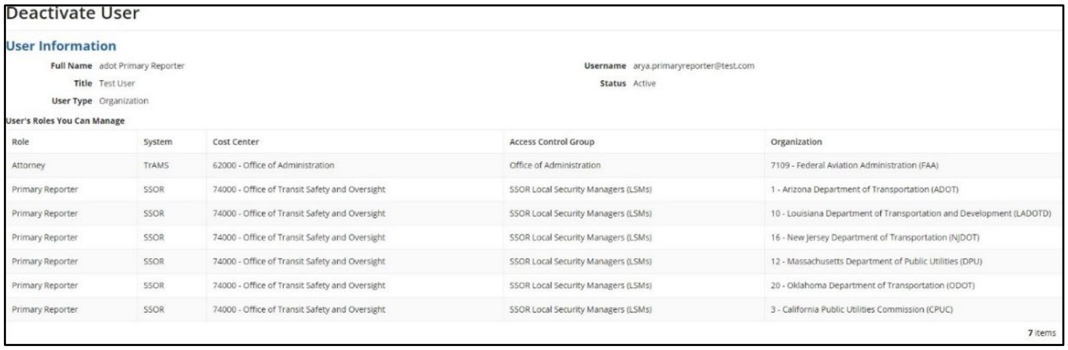
To deactivate a user:

1) Go to the user's record and Click ***Related Actions*** and then click ***Deactivate User***.

2) If the User Manager, LSM, Validation Analyst or GSM does not have approval to deactivate the user, the **Deactivate User** page will display a ribbon message. In this case, you can remove the user's access to your organization by going to ***Manage Roles*** and removing all roles for your organization(s).



3) Otherwise, the **Deactivate User** page will display with a presentation of basic **User Information**, the **User's Roles You Can Manage**, and the **Tasks Assigned Directly** to the user.

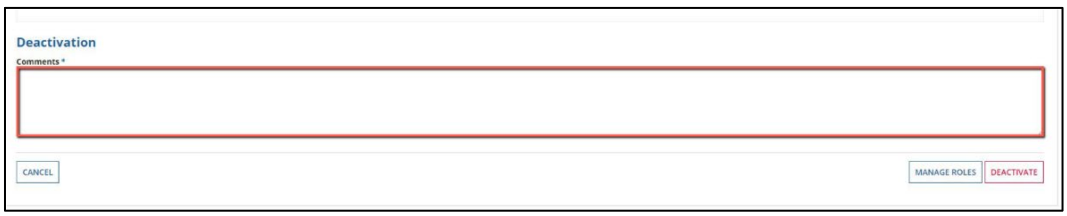


Role	System	Cost Center	Access Control Group	Organization
Attorney	TrAMS	62000 - Office of Administration	Office of Administration	7109 - Federal Aviation Administration (FAA)
Primary Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	1 - Arizona Department of Transportation (ADOT)
Primary Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	10 - Louisiana Department of Transportation and Development (LADOTD)
Primary Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	16 - New Jersey Department of Transportation (NJDOT)
Primary Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	12 - Massachusetts Department of Public Utilities (DPU)
Primary Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	20 - Oklahoma Department of Transportation (ODOT)
Primary Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	3 - California Public Utilities Commission (CPUC)

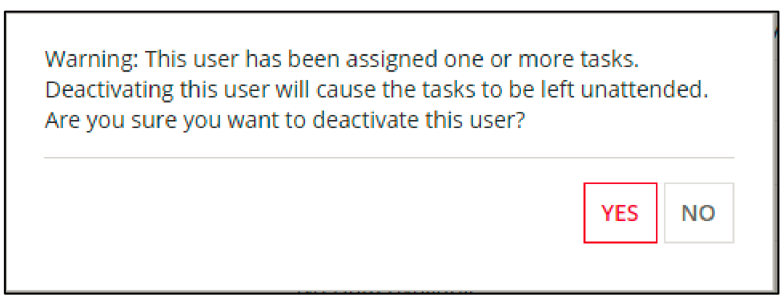
7 items

4) Click ***Cancel*** at the bottom of the page to return to the **Related Actions** page without saving any changes.

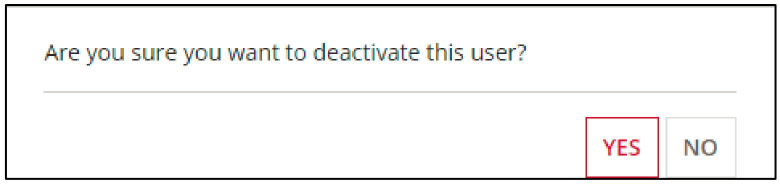
5) Enter any comments/justification for the deactivation and click ***Deactivate*** to proceed with the user deactivation. Comments are **required**.



6) If any open tasks are directly assigned to the user (not to the user's role groups), the following prompt will appear: "Warning: This user has been assigned one or more tasks. Deactivating this user will cause the tasks to be left unattended. Are you sure you want to deactivate this user?" Select ***Yes*** to proceed with user deactivation. Select ***No*** to cancel the deactivation.

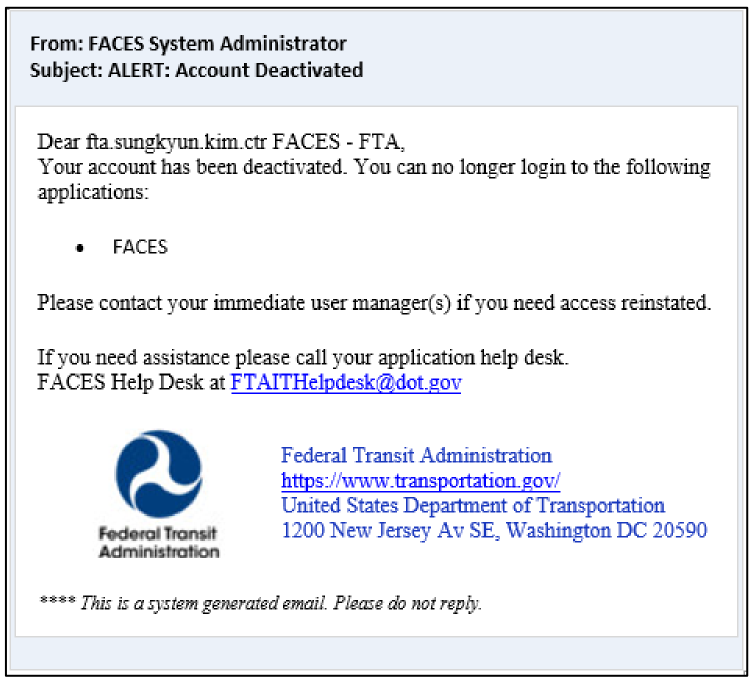


7) The user also needs to confirm the deactivation in the case where there are no unattended tasks. Select ***Yes*** when prompted with the question "Are you sure you want to deactivate this user?" to proceed with the user deactivation. Select ***No*** to cancel the deactivation:



8) On selecting ***Yes***, the system will proceed with deactivation. The **Deactivation in Progress** page will display. Click ***CLOSE*** to go back to the ***Related Actions*** or ***REFRESH*** to refresh the page.

9) The user and all the user's assigned managers within the system will receive an automatic email that will alert them that the account has been deactivated.



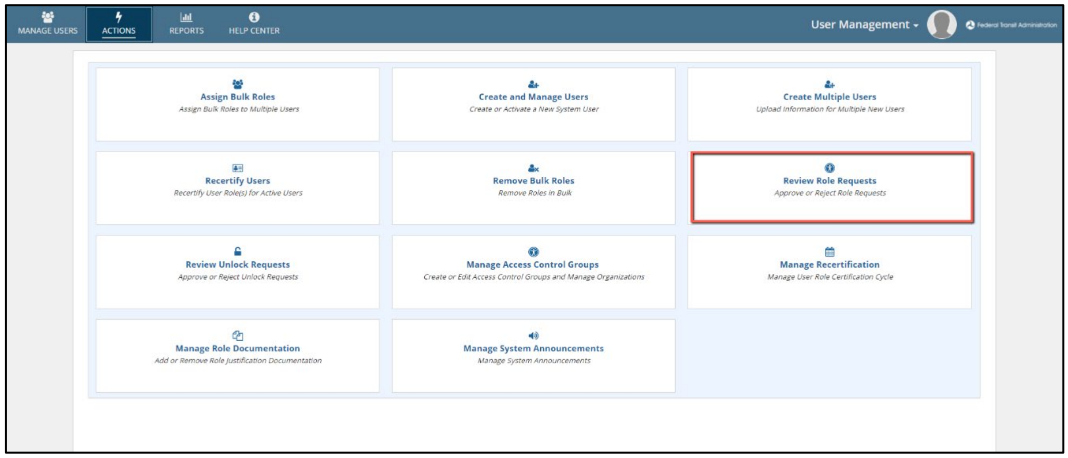
6.3.6 Action: Review Role Requests

Some roles added by **User Managers** require elevated approvals. This includes the TrAMS Recipient roles (Submitter, Official, and Attorney). *No NTD or DGS roles require elevated approvals currently.* When these roles are added on the ***Manage Roles*** page, a role request is generated. The appropriate **LSMs or Validation Analyst** will receive an email notification with a link to the ***Review Role Requests*** action. Role requests can be reviewed by any **LSM or Validation Analyst** within the appropriate Cost Center. In extreme cases,

GSMs can also complete the role request review. **GSMs** will see all active role requests for their system.

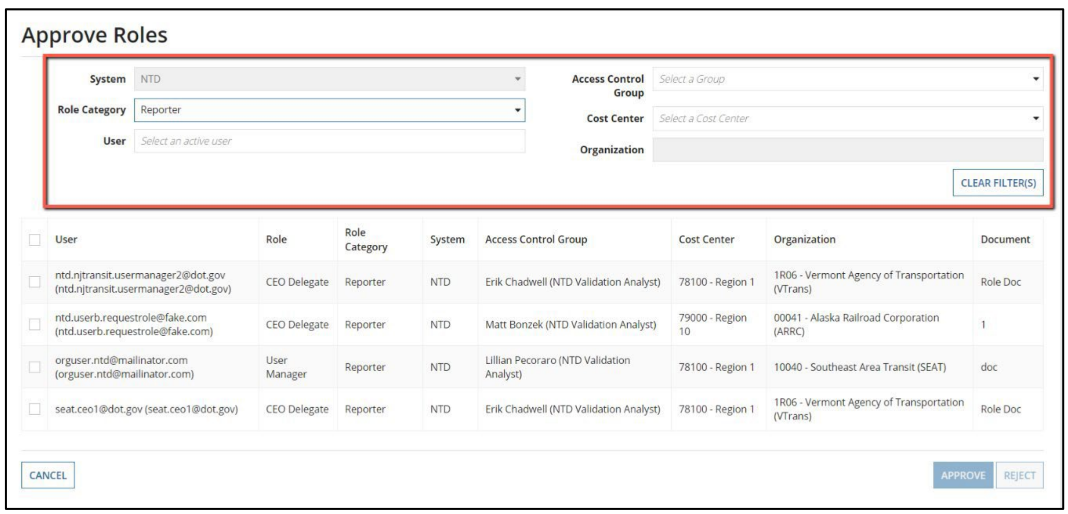
To review a role request:

1) Go to the Actions tab and click ***Review Role Requests.***



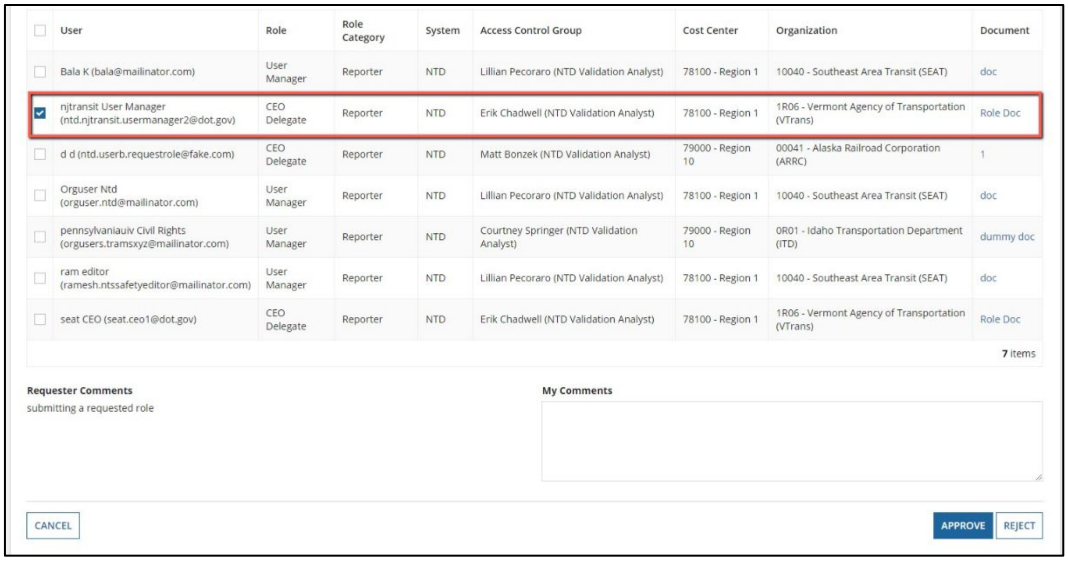
2) The ***Approve Roles*** form will open.

3) Use the filters to narrow down role requests.



4) The pending role requests that the viewer has permissions to approve will be visible. For each request, the user's name, username, role, a link to the justification document, and other key details will be included.

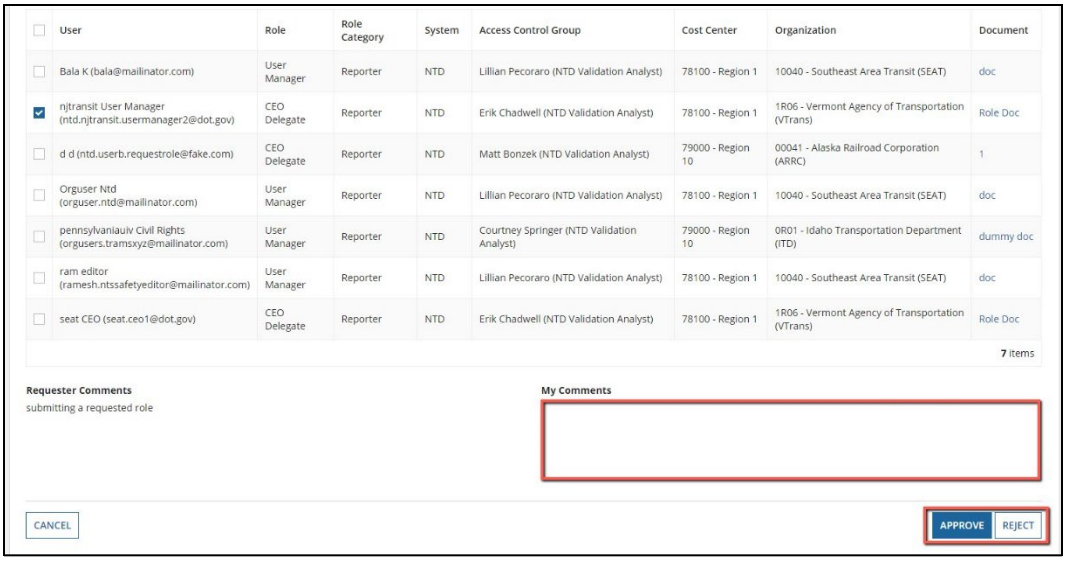
5) To review a role request, click the checkbox next to the user's name.



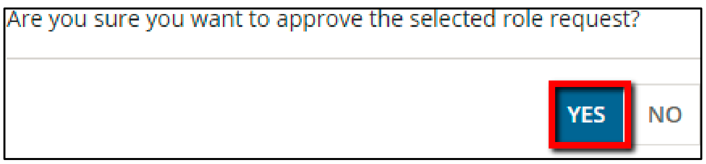
6) Additional details about the request will be displayed beneath the table of requests. The reviewer can see any comments made by the requestor.

7) To review the associated justification document, click the document hyperlink in the table. The document will be downloaded.

8) When the reviewer has reached a decision, enter any comments in the *My Comments* box and then click either ***Approve*** or ***Reject***. Comments must be 4000 characters or less. Comment are required to be added.



9) You will be prompted to confirm your decision "Are you sure you want to approve the selected role request?" Click ***Yes*** to approve. Select ***No*** to cancel and return to the form. (If you clicked ***Reject***, a similar prompt will be given "Are you sure you want to reject the selected role request?")



10) Once a decision is submitted, the role request will disappear from the table. The User Manager and impacted user will be notified of the decision via email. If the role was approved, the role will be added to the user's account.

6.3.7 Action: Review Unlock Requests

FTA is required to comply with U.S. DOT Information Technology (IT) Security guidelines. One key feature of this compliance includes automatic account locks after 60 days of user inactivity. Since the FTA systems all reside on the same software platform and use the common FACES access mechanism, this security feature applies to all software systems on the FTA platform.

FACES automatically locks user accounts if the user has not signed into their account within 60 days. The account lock prevents users from accessing any of the software systems on the FTA platform. Automated warning emails are issued to inactive users 15, 10, and 5 days prior to lockout.

Users are notified that their accounts have been locked via automated emails. Users who are locked out will still be able to log into their FACES account, but their access will be severely restricted. The standard Appian tabs (***News***, ***Tasks***, ***Records***, ***Reports***, and ***Actions***) will contain a limited amount of data and security-related actions. For example, no tasks will be available.

Locked users can unlock their accounts via one of two methods: 1) correctly answer previously set up security questions; or 2) submit an unlock request. Both methods are available from the **Actions** tab. It is preferred that all users attempt to self-unlock their accounts by answering their previously setup security questions before submitting an unlock request; this is the quickest and most efficient route to unlock an account. Once an account is unlocked, the user's access will be fully restored.

If Security Questions were not previously set up or the answers could not be remembered, user will submit an **Unlock Request** by selecting ***Unlock Account*** from their **Actions** tab. An email for the **Unlock Request** is automatically routed to the appropriate **User Manager**.

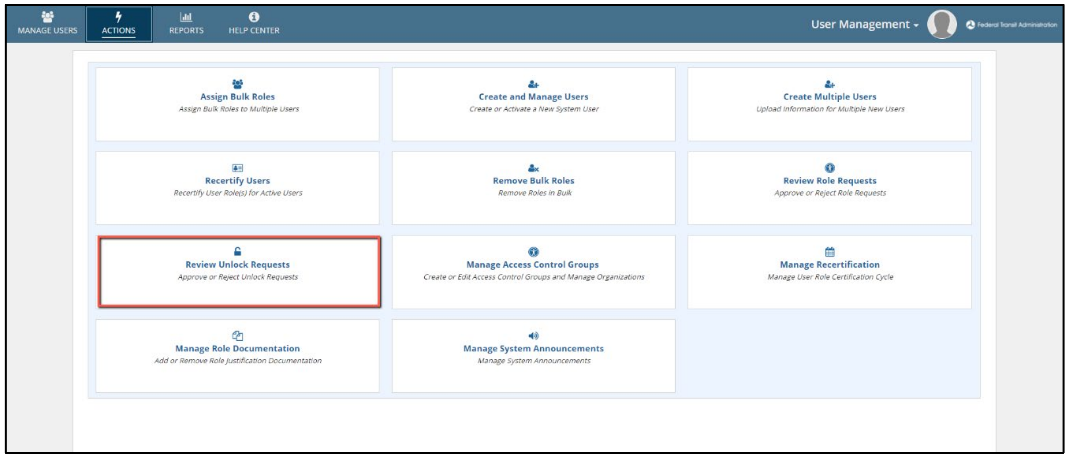
After submitting the **Unlock Request**, the **User Manager (UM), Local Security Manager (LSM) or Validation Analyst** will receive an email notification of the unlock request with a hyperlink to review the request. Upon receiving the **Unlock Request**, the **UM, LSM or Validation Analyst** can either approve or deny the request. The user will receive an email notification confirming either decision.

If the request is approved, the account will unlock, and all previous permissions will be restored. If the request is denied, the account will remain locked. If the account remains locked, the user should call their User Manager directly to resolve the issue. If the appropriate User Manager is not known, the user can call the Help Desk.

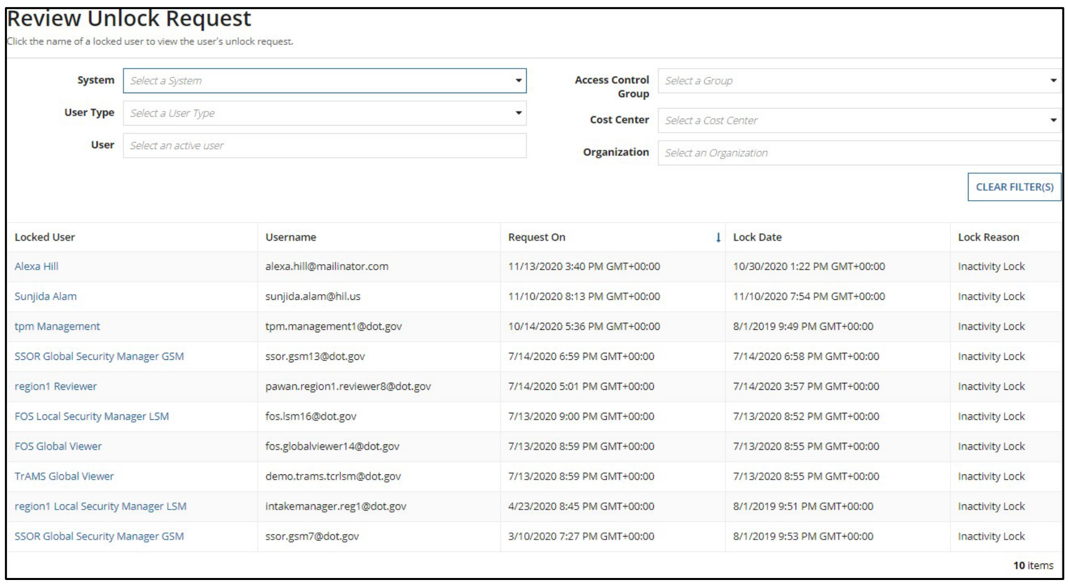
Note:	*If the organization does not have a **User Manager** or the user is a User Manager, the **Unlock Request** will go to the appropriate **Local Security Manager (LSM)** for resolution. If the user belongs to multiple organizations, the request will go to the appropriate **User Manager** of each organization.*

To reply to an **Unlock Request**:

1) Navigate to the **Actions** tab and click ***Review Unlock Requests***.



2) System Displays **Review Unlock Request** Page with locked user's information.



Review Unlock Request

Click the name of a locked user to view the user's unlock request.

System: Select a System
User Type: Select a User Type
User: Select an active user
Access Control Group: Select a Group
Cost Center: Select a Cost Center
Organization: Select an Organization

CLEAR FILTER(S)

Locked User	Username	Request On	Lock Date	Lock Reason
Alexa Hill	alexa.hill@mailinator.com	11/13/2020 3:40 PM GMT+00:00	10/30/2020 1:22 PM GMT+00:00	Inactivity Lock
Sunjida Alam	sunjida.alam@hil.us	11/10/2020 8:13 PM GMT+00:00	11/10/2020 7:54 PM GMT+00:00	Inactivity Lock
tpm Management	tpm.management1@dot.gov	10/14/2020 5:36 PM GMT+00:00	8/1/2019 9:49 PM GMT+00:00	Inactivity Lock
SSOR Global Security Manager GSM	ssor.gsm13@dot.gov	7/14/2020 6:59 PM GMT+00:00	7/14/2020 6:58 PM GMT+00:00	Inactivity Lock
region1 Reviewer	pawan.region1.reviewer8@dot.gov	7/14/2020 5:01 PM GMT+00:00	7/14/2020 3:57 PM GMT+00:00	Inactivity Lock
FOS Local Security Manager LSM	fos.lsm16@dot.gov	7/13/2020 9:00 PM GMT+00:00	7/13/2020 8:52 PM GMT+00:00	Inactivity Lock
FOS Global Viewer	fos.globalviewer14@dot.gov	7/13/2020 8:59 PM GMT+00:00	7/13/2020 8:55 PM GMT+00:00	Inactivity Lock
TrAMS Global Viewer	demo.trams.tcrlsm@dot.gov	7/13/2020 8:59 PM GMT+00:00	7/13/2020 8:55 PM GMT+00:00	Inactivity Lock
region1 Local Security Manager LSM	intakemanager.reg1@dot.gov	4/23/2020 8:45 PM GMT+00:00	8/1/2019 9:51 PM GMT+00:00	Inactivity Lock
SSOR Global Security Manager GSM	ssor.gsm7@dot.gov	3/10/2020 7:27 PM GMT+00:00	8/1/2019 9:53 PM GMT+00:00	Inactivity Lock

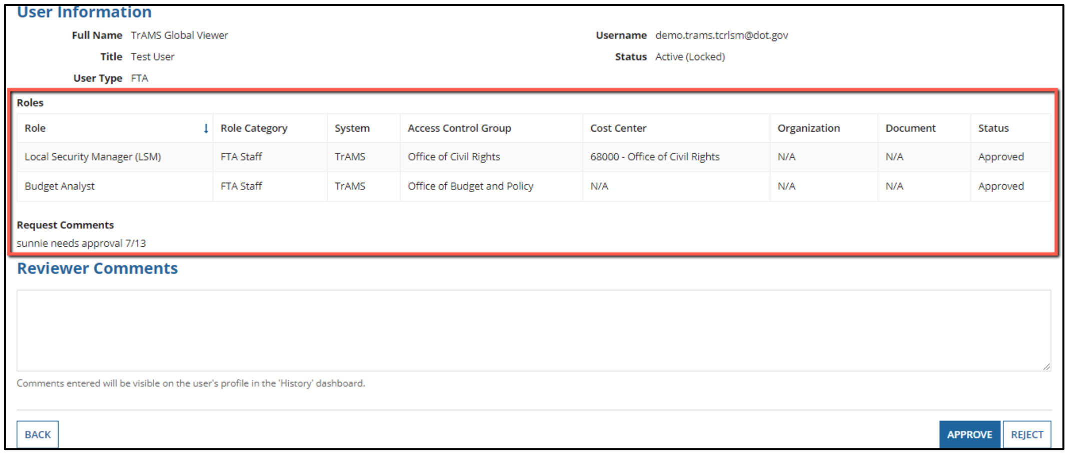
10 items

3) Click ***Close*** if no action is necessary to return to the **Actions** page.

4) If not, select the link representing the name of the user that needs to be unlocked.

5) The **Review Unlock Request** page will display the user's detailed information.

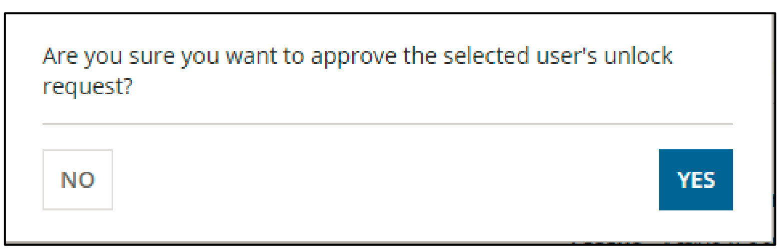
6) Validate the **User Information** and review the **Request Comments** section.



7) If no action is necessary or more information/justification is needed, select ***Back*** to return to the **Review Unlock Request** page without acting on the **Unlock Request**.

8) Otherwise, enter any text pertinent to the unlock of this user in the **Reviewer Comments** window. Click ***Approve*** to approve the request and click ***Reject*** to reject the unlock request.

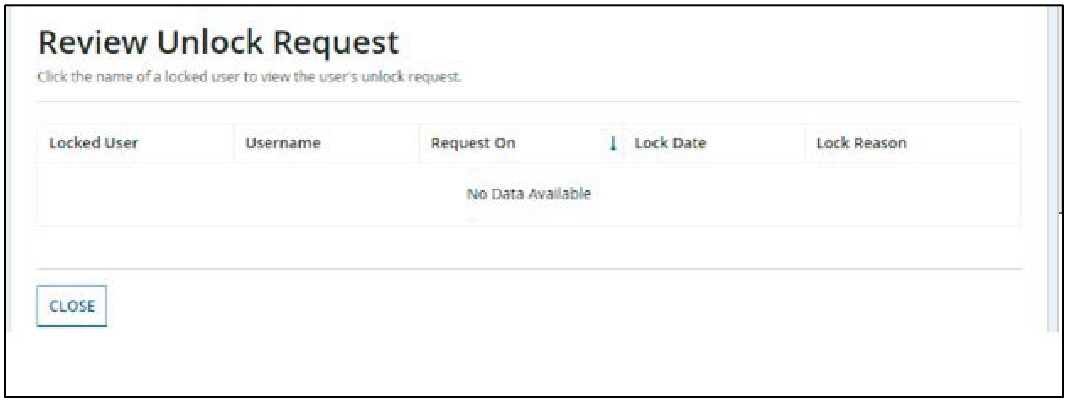
9) A message will display asking the user to confirm his or her decision. Select ***Yes*** to proceed or select ***No*** to remain on the review unlock request page.



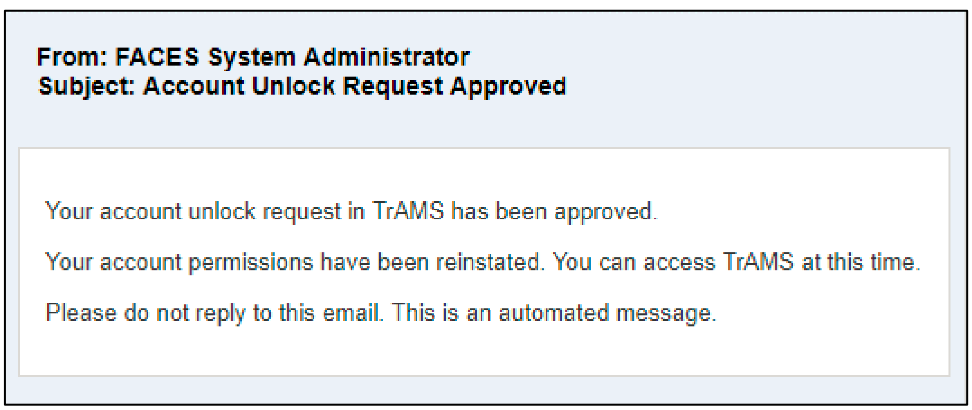
10) A message will display that indicates the decision for the Unlock Request is being processed. Click ***Close.***

11) The **Review Unlock Request** page displays. The **Unlock Request** is no longer listed.

Note:	*There may be other Unlock Requests in the queue. Select **Close** to return to the **Actions** tab.*



12) The user will receive a confirmation email regarding the approval or rejection of their request.

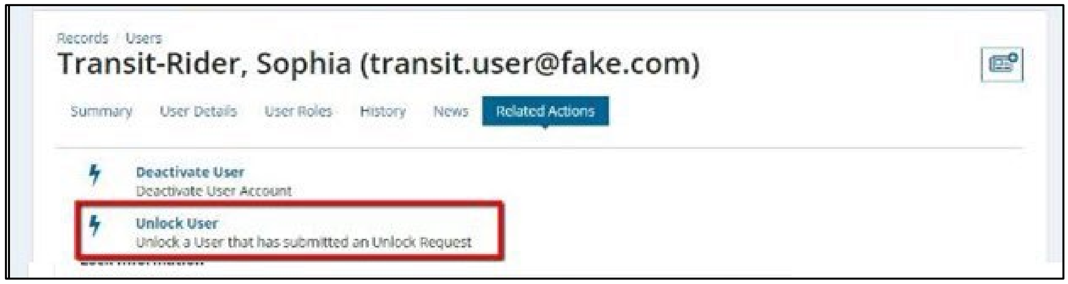


6.3.8 Related Action: Unlock User

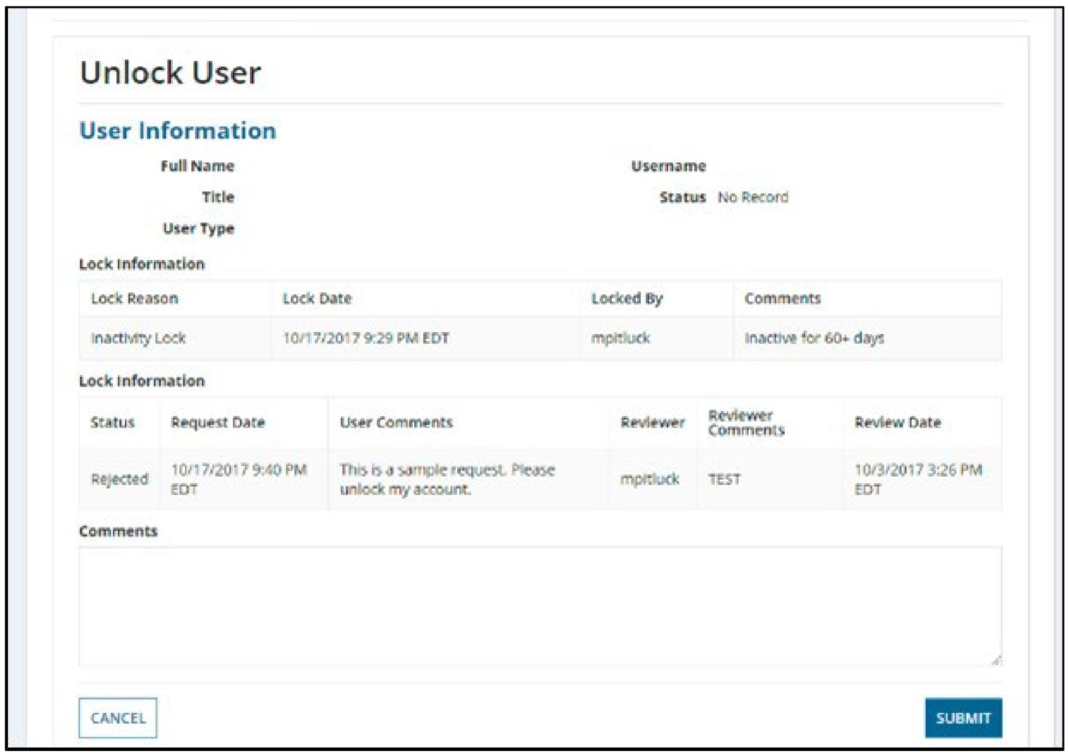
If any user is locked in the system, an additional related action will become available on the user's record, ***Unlock Account.*** This related action allows a **User Manager, LSM, Validation Analyst** or **GSM** (as appropriate) to unlock a user directly from the user's profile. This related action will remain visible if the user's record is locked. It is intended as a backup method of unlocking an account.

To unlock a user's account from the profile related action:

1) Navigate to the user’s record and click the “Unlock User” related action.

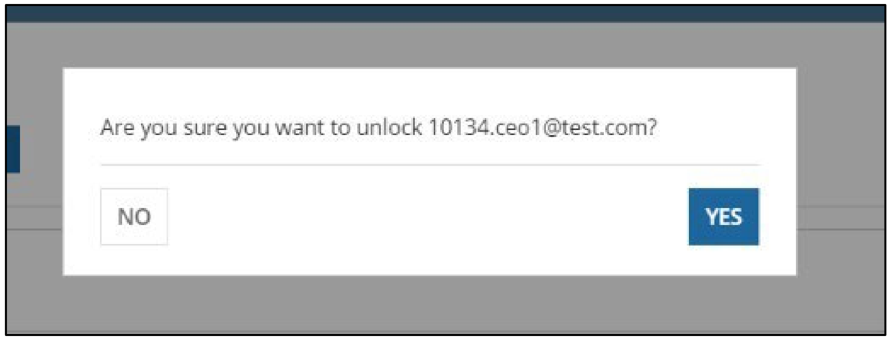


2) A page will display information about the user’s account, the reason for the account lock, and the user’s unlock request.



3) Enter a comment justifying the unlock action, as needed, and then click ***Submit***.

4) In the confirmation screen confirm you want to unlock user.



5) On selecting ***Yes***, the system will proceed with deactivation. The **Unlock in Progress** page will display. Click ***CLOSE*** to go back to the ***Related Actions*** or ***REFRESH*** to refresh the page.

Note:	Whenever any user is unlocked after being locked due to re-certification then all that user's active roles will be automatically re-certified.

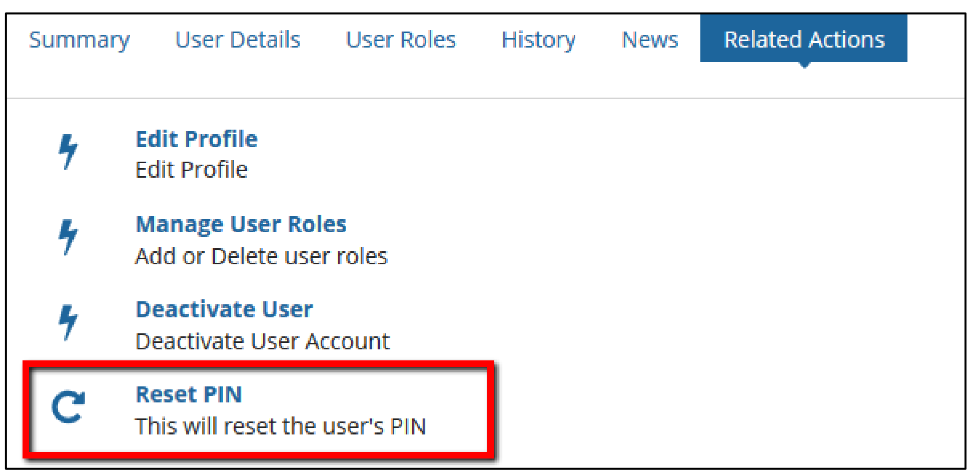
6.3.9 Related Action: Reset PIN

If a user cannot remember either their existing PIN or security question answers, the user can contact someone in their users' management chains (User Manager, LSM, or GSM) to reset their PIN.

Note:	The Reset PIN action only appears for User Managers, LSMs or GSMs.

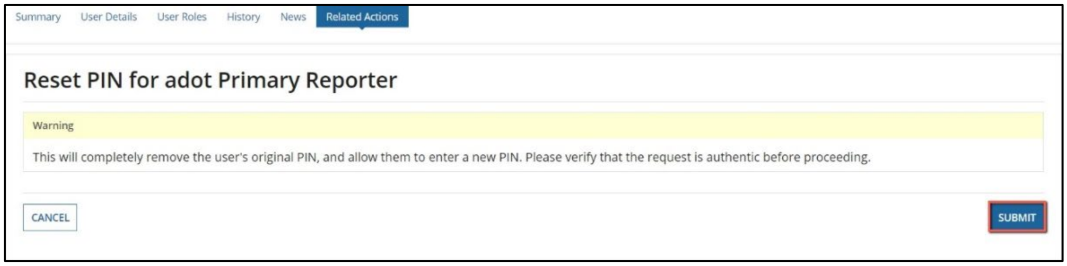
How to reset a user's PIN:

1) Navigate to the user's record and select **Related Actions**.
2) Click ***Reset PIN.***



3) The Reset PIN page displays a warning message and notifies the user management chain that they are about to reset a user's PIN and please verify that request to reset the user's pin came from the intended user.

Note:	There is no verification in the system for PIN Reset requests. Once the PIN is reset, the previous user PIN is no longer valid.



4) Select ***Cancel*** to return to the previous page without saving any changes.
5) Select ***Submit*** to finalize resetting the user's PIN.
6) The ***Related Actions*** page displays.

6.4. Reviewing Monthly User Comparison Report

The User Comparison Report script generates a report that displays all users that hold both an account in the same system with supervisory roles and an account with non-supervisory roles.

It collates user data across several tables - including contact and address information, then compares users with supervisory roles against those with non-supervisory roles. The resulting report shows a row for each pair of roles across two different accounts held by the same person:

- Supervisory, and
- Non-supervisory.

The recipients of the report are the Global Security Managers (GSMs).

Once the report is received, the expectation is to investigate any items in question within the report.

7. Recertification

Recertification is a process that requires the user's manager to review and recertify (or reject) a user's system roles to satisfy DOT security requirements. The recertification process happens annually, and the user's managers must review and re-certify all users that report to them.

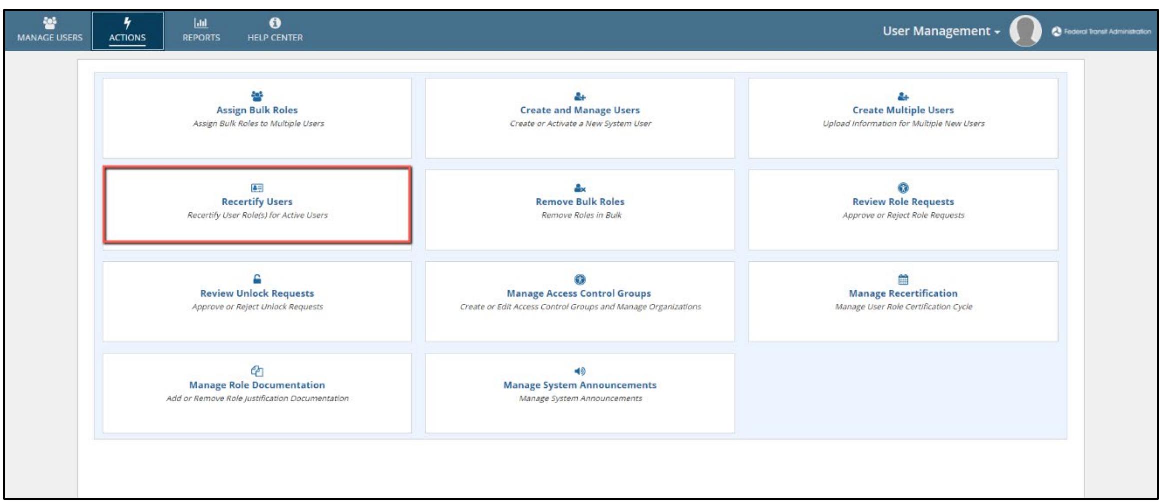
7.1. Help Desk Information

The recertification process trigger systems on the TrIAD platform to send email notifications to role management users (Certifiers) alerting them when they are required to recertify users. After receiving the email notification, each Certifier has a certain number of days to recertify the user group specified in the email. The email will provide this timeline. Users who are not recertified will have their roles removed; users with no roles will be automatically locked out of the system. Users who have multiple roles will have to have each role recertified by their Certifier; the Certifier may elect to only recertify some of a user's roles. In this situation, the user will lose only those roles and will not be locked out of the system. Users who have lost roles or have been locked out of the system will have to contact their Certifier to reinstate their roles. The Certifiers (GSMs, LSMs, User Managers) are required to recertify users with a specific period, depending on the system. This period is called the recertification window.

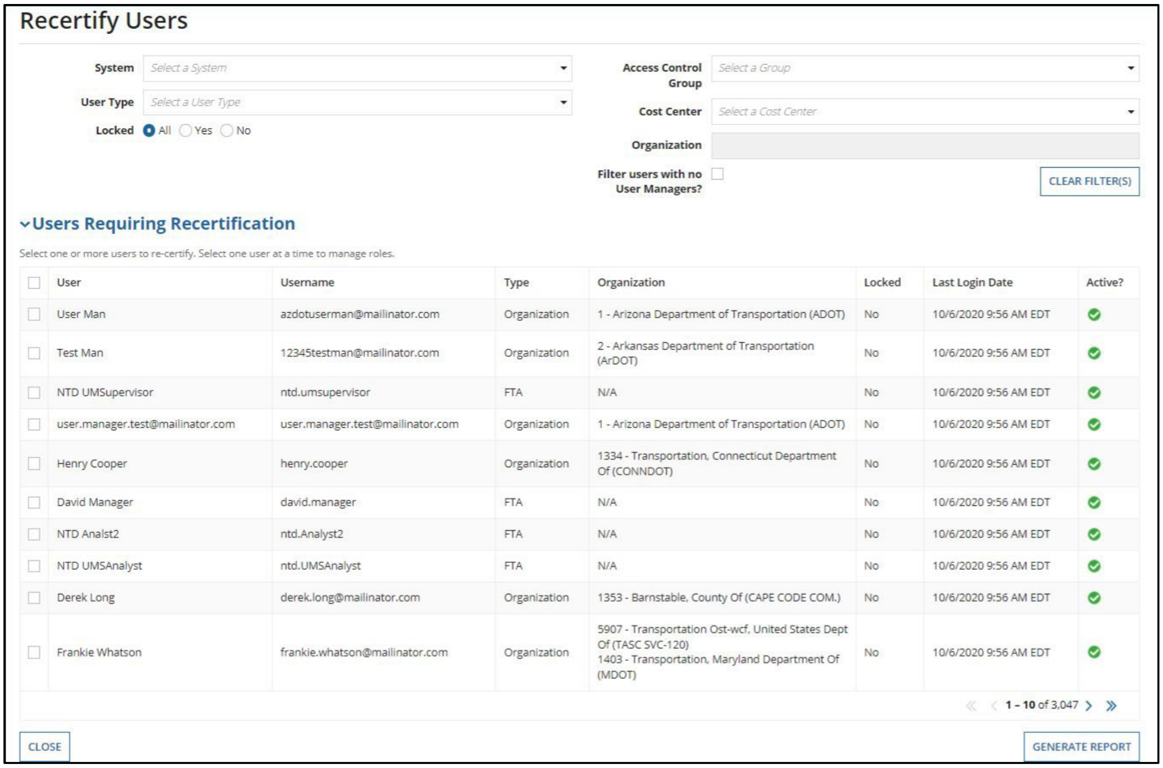
Note:	If a user becomes locked, they can self-unlock themselves or submit unlock requests as detailed in Section 7.2.

How to recertify a user role:

1) **Certifier** logs into System and clicks Actions.
2) Click ***Recertify Users.***



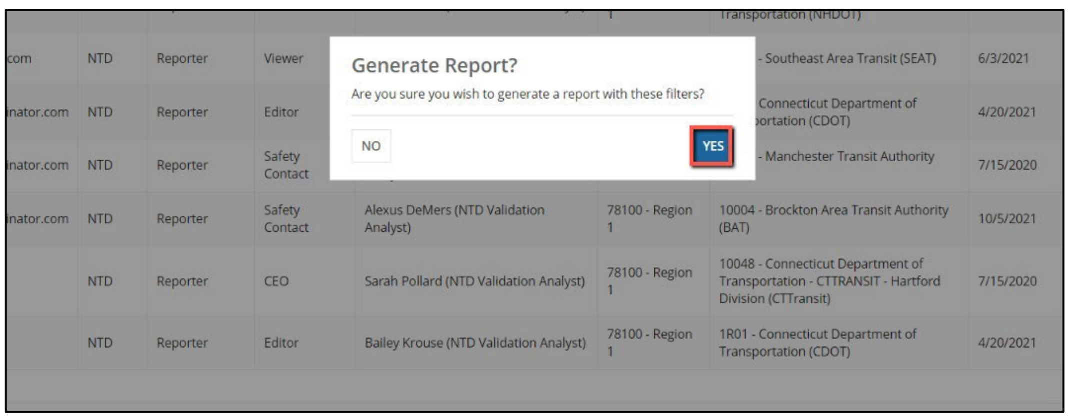
3) The **Recertify Users** page is displayed, allowing the **Certifier** to filter users to recertify.



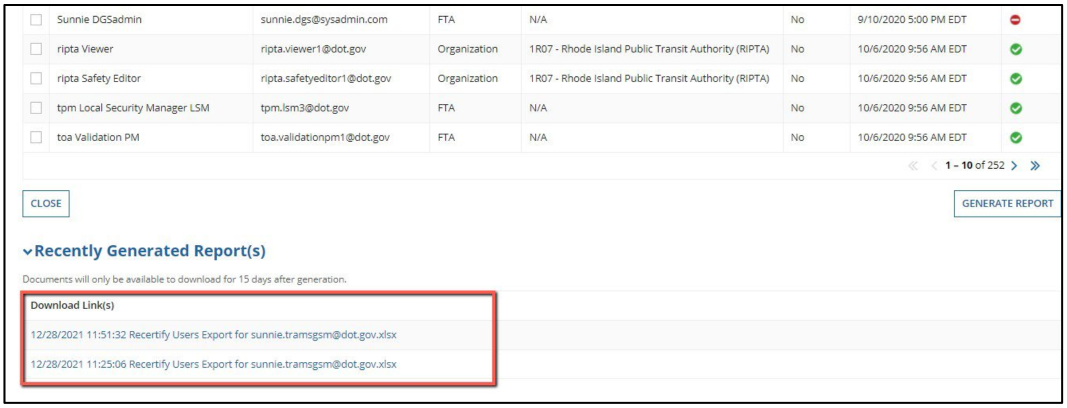
User	Username	Type	Organization	Locked	Last Login Date	Active?
User Man	azdotuserman@mailinator.com	Organization	1 - Arizona Department of Transportation (ADOT)	No	10/6/2020 9:56 AM EDT	
Test Man	12345testman@mailinator.com	Organization	2 - Arkansas Department of Transportation (ArDOT)	No	10/6/2020 9:56 AM EDT	
NTD UMSupervisor	ntd.umsupervisor	FTA	N/A	No	10/6/2020 9:56 AM EDT	
user.manager.test@mailinator.com	user.manager.test@mailinator.com	Organization	1 - Arizona Department of Transportation (ADOT)	No	10/6/2020 9:56 AM EDT	
Henry Cooper	henry.cooper	Organization	1334 - Transportation, Connecticut Department Of (CONNDOT)	No	10/6/2020 9:56 AM EDT	
David Manager	david.manager	FTA	N/A	No	10/6/2020 9:56 AM EDT	
NTD Analst2	ntd.Analyst2	FTA	N/A	No	10/6/2020 9:56 AM EDT	
NTD UMSAnalyst	ntd.UMSAnalyst	FTA	N/A	No	10/6/2020 9:56 AM EDT	
Derek Long	derek.long@mailinator.com	Organization	1353 - Barnstable, County Of (CAPE CODE COM.)	No	10/6/2020 9:56 AM EDT	
Frankie Whatson	frankie.whatson@mailinator.com	Organization	5907 - Transportation Ost-wcf, United States Dept Of (TASC SVC-120) 1403 - Transportation, Maryland Department Of (MDOT)	No	10/6/2020 9:56 AM EDT	

4) A **Certifier** can download a report for users that require recertification, based on the filters applied, by clicking on **Generate Report.**

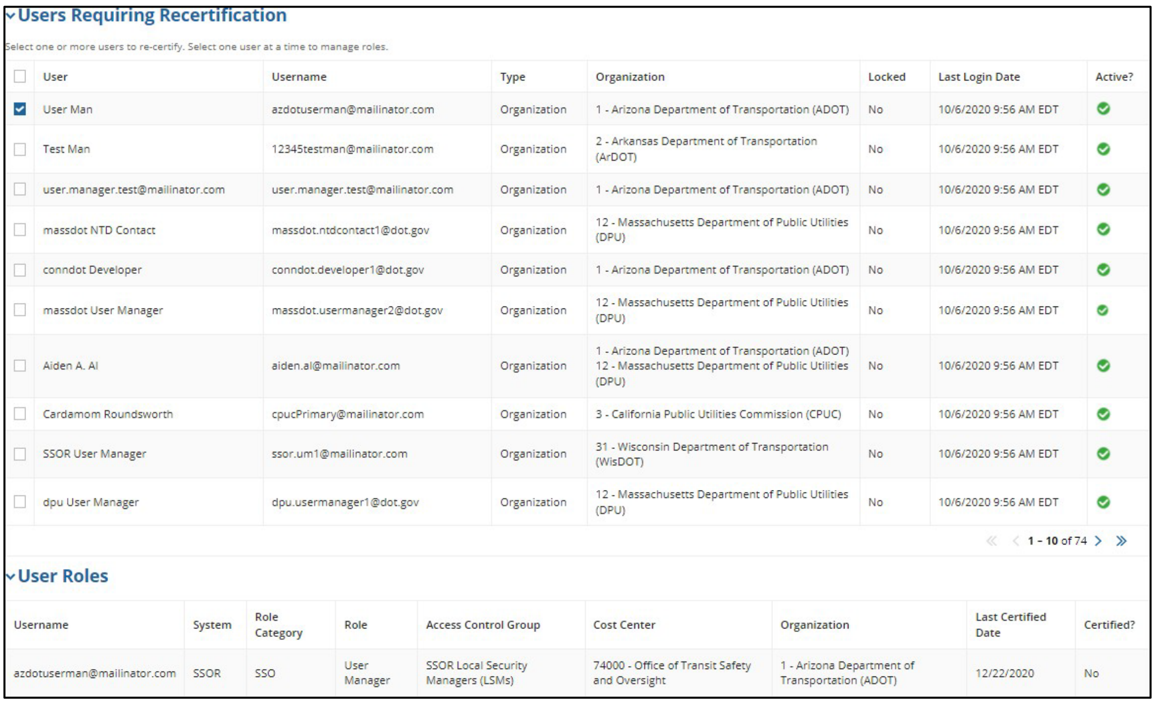
   a. The system displays a confirmation message.



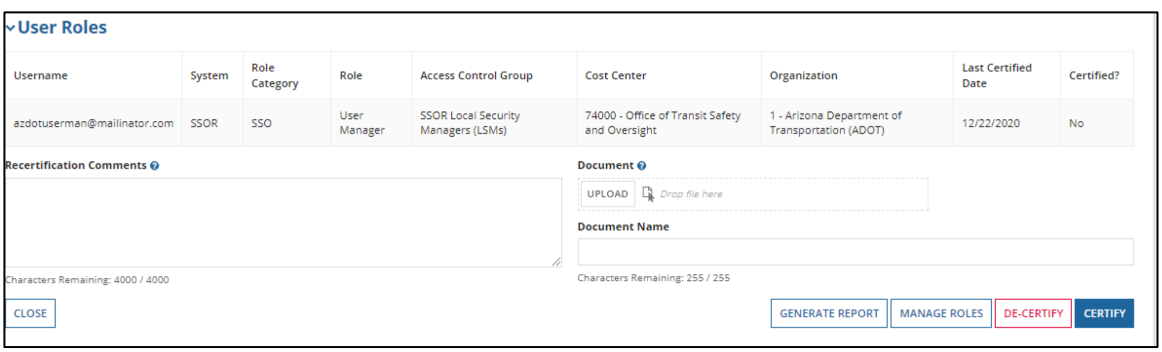
   b. A link to the report will be available to download shortly after as well as emailed to the **Certifier**.



5) The **Certifier** can select a user or users to recertify roles.



6) The **Certifier** reviews user(s) details and roles in the User Roles section of the page.



a. Username with user details is displayed on the table.

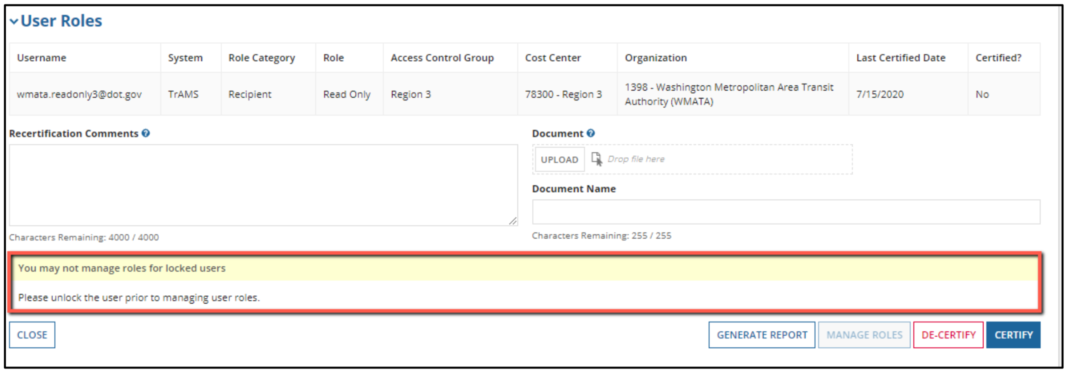
b. **Certifier** then enters Recertification Comments. Recertification Comments are required.

c. Can upload any supporting documentation.

d. Enter Document Name.

e. If a user is active and needs recertification of role(s) and mange role(s) at the same time, the **Certifier** can use the **Manage Roles** button.

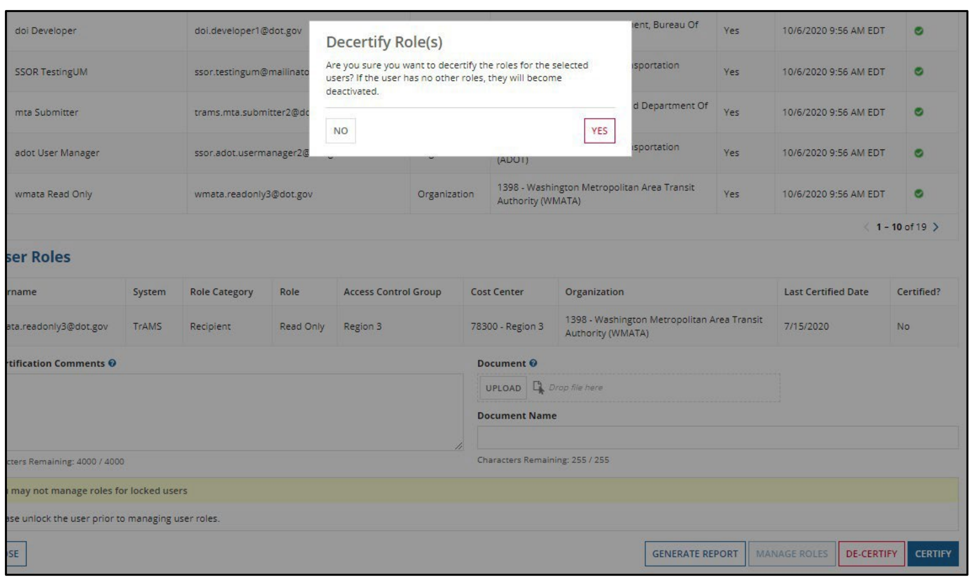
f. If a User is locked, the **Certifier** can click on the **Close** button and return to the **Action** Page or navigate to the **Manage Roles** Related Actions if needed to recertify and manage roles:



See Section [Manage User Role]() for how to manage user's roles.

g. Click on the **De-Certify** button:

   i. The system displays a confirmation message.



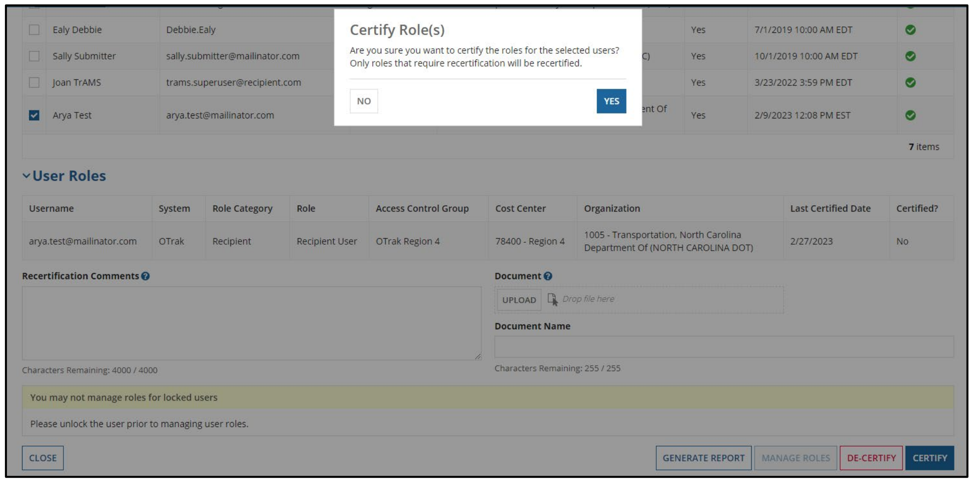
   ii. The **Certifier** will click the ***Yes*** button.

   iii. The user's role is de-certified.

- If a user has any existing roles, then roles that are de-certified will be deleted.
- If a user has no other existing certified roles the decertify action will deactivate the user.

h. Can click on the **Certify** button:

i. The system displays a confirmation message.



ii. The **Certifier** will click the ***Yes*** button.

iii. User's role is certified until next year.

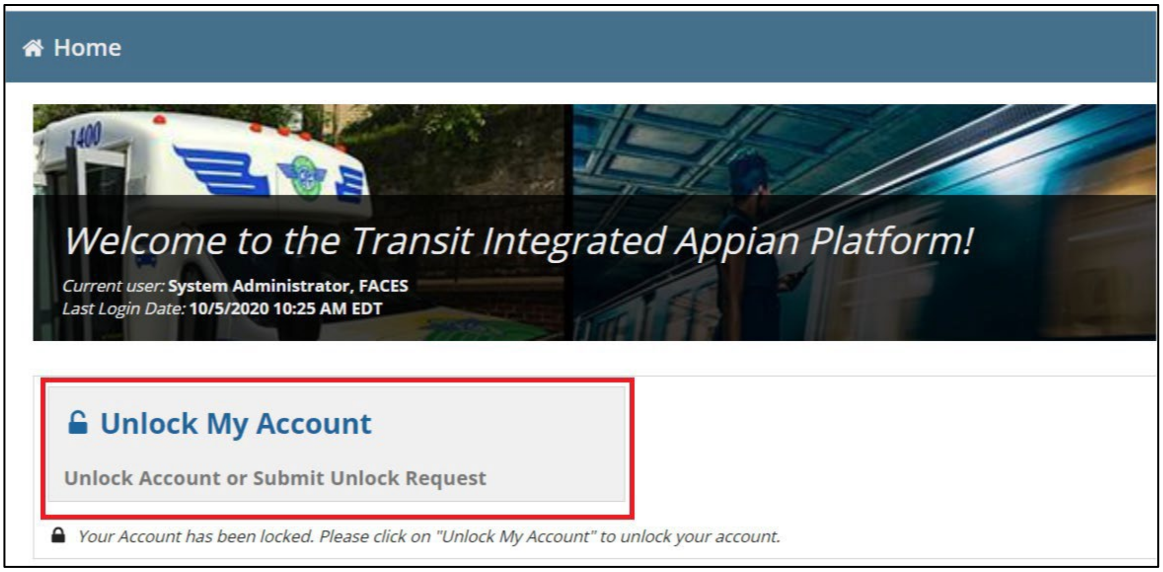
Note:	*If the certifier does not recertify their assigned users before the end of the recertification window, all the uncertified users will be locked. Users locked because of recertification activities will receive an email to inform them, they no longer have access to the system. If they are not unlocked within two weeks, users locked because of recertification activities will be deactivated.*

7.2. User Lock/Unlock Request Process

A user account can be locked if a Certifier does not recertify the user's role during the recertification period. The user will be required to submit an Unlock My Account request from his or her system. A locked user cannot perform any action on the system until his or her account is unlocked.

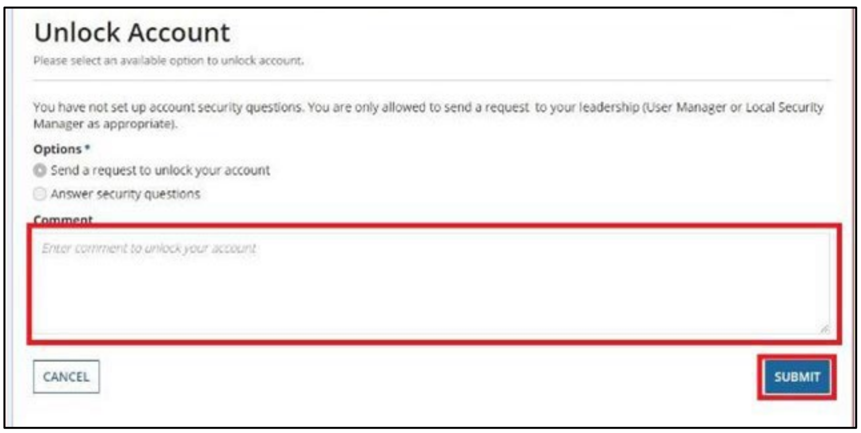
How a user can request to have his or her account unlocked:

1) **User** logs into System.
2) **User** clicks ***Unlock My Account***.



3) The **System** displays the **Unlock Account** page.

4) **User** enters comment and clicks ***Submit*** button.



Note:	*The user will not be able to select the Answer Security Questions option.*

7.3. Certifier Unlocking User's Locked Account

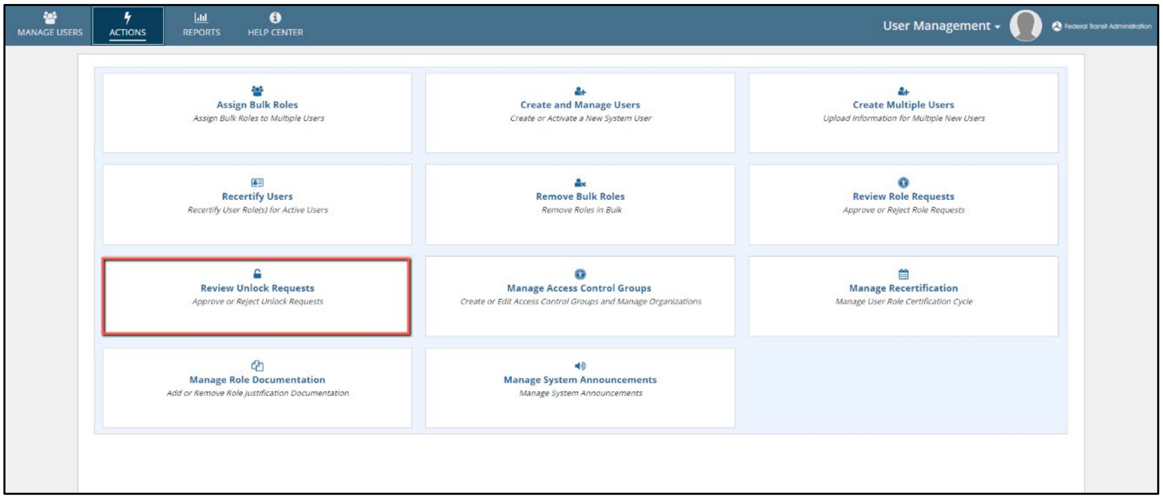
If a user submits an unlock request during recertification, their Certifier will receive an email notification to unlock the account. A user account locked during recertification will be deactivated two weeks after the end of the recertification window if the Certifier does not unlock the account.

Hint: Alternatively, a certifier can use Unlock related action to unlock locked users. There is no mandate for users to submit unlock request in this case.

How a **Certifier** can unlock a user's account:

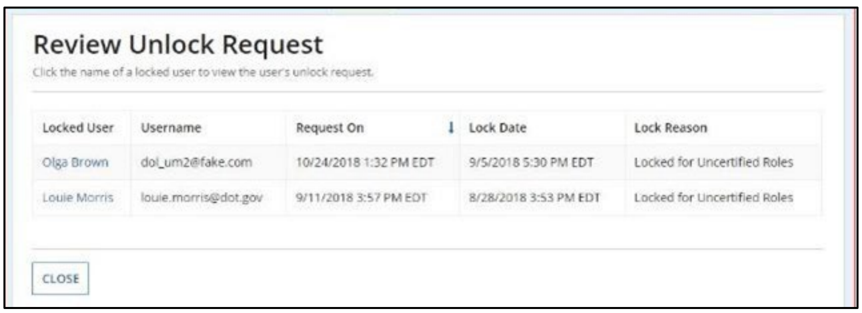
1) **Certifier** logs into System and clicks Actions.

2) **Certifier** clicks ***Review Unlock Request.***



3) The **System** displays Review Unlock Request page.

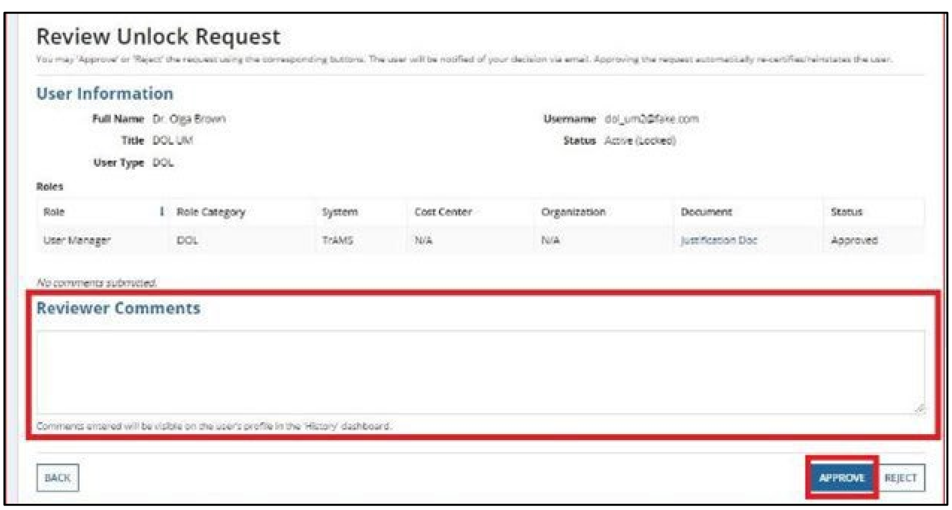
4) **Certifier** clicks on locked username.



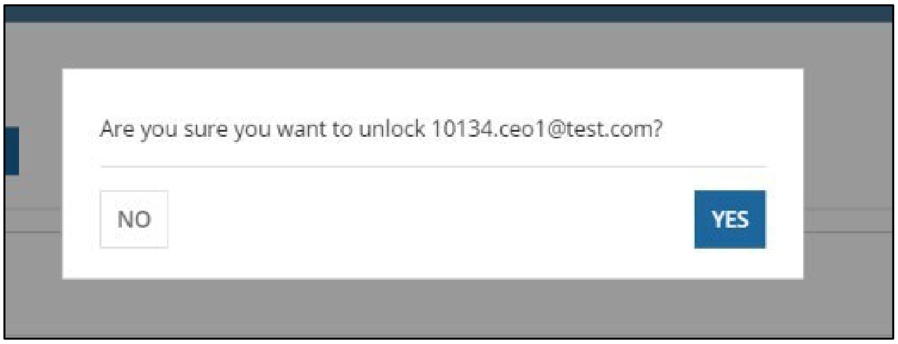
5) The **System** displays User information page.

6) **Certifier** may enter text to explain the unlock action in the Reviewer Comments section.

7) **Certifier** clicks on Approved button.



8) In the confirmation screen confirm you want to unlock user.



9) On selecting ***Yes***, the system will proceed with deactivation. The **Unlock in Progress** page will display. Click ***CLOSE*** to go back to the ***Related Actions*** or ***REFRESH*** to refresh the page.

Note:	*Approving the request automatically re-certifies/reinstates the user's role. Certifier can reject the unlock request and the user account will continue to remain locked.*

Appendix A: Acronyms and Definitions

The following table provides definitions for abbreviations and acronyms used in this document.

Acronym	Definition
DGS	Discretionary Grant System
DOL	Department of Labor
DOT	Department of Transportation
ECHO-Web	Electronic Clearing House Operation Web
FACES	FTA Access Control and Entry System
FTA	Federal Transit Administration
GSM	Global Security Manager
LSM	Local Security Manager
NTD	National Transit Database
SSOR	State Safety Oversight Reporting
TrAMS	Transit Award Management System
UM	User Manager
URL	Universal Resource Locator (i.e., web address)

Appendix B: User Role Rules

This appendix contains user role assignment rules by system (e.g., TrAMS, NTD or DGS). For information about the privileges a role confers, see the appropriate user guide for the system in question.

1. FTA Platform Rules

1) FTA user type is platform wide.
2) FTA users can only be assigned roles that match their platform user type.
3) FTA Users can only be assigned FTA user roles.
4) Organization users can only be assigned organization user roles.
5) External users can only be assigned roles that match their external user subtype.
    a. Auditors can only be assigned auditor roles.
    b. Contractors can only be assigned contractor roles.
    c. DOL Users can only be assigned DOL roles.

2. NTD Rules

General Rule: Each reporter user can have up to two roles per Reporter organization (if a user has two (2) roles, one role must be User Manager.)

NTD Reporter Role	Rules
User Manager	• The User Manager role can be held in combination with any NTD Reporter role except Viewers. • User Managers can create all other users within a Reporter organization.
CEO	• The CEO role must be assigned by an FTA user. • The maximum number of CEOs within a single Reporter organization is one (1).
NTD Contact	• The maximum number of NTD Contacts within a single Reporter organization is one (1).
Editor	• Multiple users can be assigned the Editor role.
Viewer	• Multiple users can be assigned the Viewer role. • Viewers cannot also be assigned the User Manager role.
Safety Contact	• The maximum number of Safety Contacts within a single Reporter organization is one (1).
Safety Editor	• Multiple users can be assigned the Safety Editor role.
Safety Viewer	• Multiple users can be assigned the Safety Viewer role.

CEO Delegate	• Multiple users can be assigned the CEO Delegate role. • Only CEOs and CEO delegates can assign the CEO delegate role.

3. TrAMS Rules

TrAMS Recipient Roles	Rules
Read Only	• The Read Only role cannot be assigned at the same time as any other recipient roles within a single recipient organization.
User Manager	• The User Manager assignment must be approved by an LSM or GSM.
Submitter	• The Submitter assignment must be approved by an LSM or GSM. • Role assignment requires attachment of Delegation of Authority letter.
Developer	• No rules apply to this assignment
Official	• The Official assignment must be approved by an LSM or GSM. • Role assignment requires attachment of Delegation of Authority letter.
Attorney	• The Attorney assignment must be approved by an LSM or GSM. • Role assignment requires attachment of Delegation of Authority letter.
Civil Rights	• No rules apply to this assignment
FFR Reporter	• No rules apply to this assignment
MPR Reporter	• No rules apply to this assignment
JPC Procurement Officer	• No rules apply to this assignment

TrAMS FTA Roles

The table below shows which roles are applicable to each Cost Center

	Office of Administrator	Office of Administration	Office of the Chief Counsel	Office of Communication and Congressional Affairs	Office of Program Management	Office of Budget and Policy	Office of Research, Demonstration, and Innovation	Office of Civil Rights	Office of Planning and Environment
	TOA	TAD	TCC	TCA	TPM	TBP	TRI	TCR	TPE
TrAMS Roles - FTA	**61000**	**62000**	**63000**	**64000**	**65000**	**66000**	**67000**	**68000**	**71000**
Supervisor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local Security Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intake Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pre-Award Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Post-Award Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reservationist	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Director	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Director of Operations	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Initial Reviewer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Technical Reviewer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Environmental Reviewer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Civil Rights Officer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Legal Counsel	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Read Only	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Budget Director	No	No	No	No	No	Yes	No	No	No
Budget Analyst	No	No	No	No	No	Yes	No	No	No
Vendor Setup	No	No	No	No	No	Yes	No	No	No
Apportionment Manager	No	No	No	No	Yes	No	No	No	No
Transit Director	No	No	No	No	Yes	No	No	No	No
Discretionary Admin	No	No	No	No	Yes	No	No	No	No
TCA Recorder	No	No	No	Yes	No	No	No	No	No
DBE Approver	No	No	No	No	No	No	No	Yes	No
Dataset Administrator	No	No	Yes	No	Yes	No	No	No	Yes

4. DGS Rules

DGS Recipient Roles	Rules
Program Admin/Manager	• The Program Admin/Manager role can be held in combination with any DGS role except. • Program Admin/Manager with the GSM role can create all other users within the DGS system. • Multiple users can be assigned the Program Admin/Manager with/without the GSM role.

GSM	• The Program Admin/Manager with the GSM role must be assigned by an FTA user.
Team Lead	• Multiple users can be assigned the Team Lead role.
Reviewer	• Multiple users can be assigned the Reviewer role.

5. SSOR Rules

SSOR Roles	Rules
Program Management Lead	• The Program Management Lead role can be held in combination with SSOR GSM role.
GSM	• The Program Management Lead with the GSM role can create all other users within the SSOR system.
LSM	• Any of the FTA SSOR role can be conjunction with LSM (example: Validation Lead)
Program Management Team Member	• Multiple users can be assigned the Program Management Team Member
User Manager	• User Manager role be held with Primary or Alternate Reporter.

6. CRM Rules

CRM Roles	Rules
GSM	• Has access to all FACES functionality to manage, create, and recertify global users.
Global Viewer	• No rules apply to Global Viewer.
FTA User	• Created by GSM and has only access to reports and view privilege of all the global users.

7. FACES Rules

FACES Roles	Rules
GSM	• Has access to all FACES functionality to manage, create and recertify global users.
User Details Report Global Viewer	• Only has access to User Details, User Deactivation History, and Supervisor Hierarchy reports

FACES Tier-1 Helpdesk Viewer	• Only has access to User Details, User Deactivation History, Recertification Status, and Supervisor Hierarchy reports
FACES Tier-1 Helpdesk Lead	• Has access to Manage System Announcements, Send ad-hoc emails, and reports

8. ECHO-Web Rules

ECHO-Web Roles	Rules
GSM	• Has access to all FACES functionality to manage, create, and recertify global users.
Global Viewer	• Has read only access to payment requests and account management.
Grantee	• A maximum of 2 grantee role(s) can be assigned to an organization
Approving Official	• A maximum of 1 grantee role can be assigned to an organization

Appendix C: FTA Cost Centers

FTA is organized into 10 Regional FTA offices and 11 FTA Headquarters offices. These "cost centers" have acronyms and numbers that are used throughout FACES. Each organization is tagged to a cost center. The FTA cost centers are:

Cost Center Name	Acronym	Number
FTA Regional 1 Office	TRO-1	78100
FTA Regional 2 Office	TRO-2	78200
FTA Regional 3 Office	TRO-3	78300
FTA Regional 4 Office	TRO-4	78400
FTA Regional 5 Office	TRO-5	78500
FTA Regional 6 Office	TRO-6	78600
FTA Regional 7 Office	TRO-7	78700
FTA Regional 8 Office	TRO-8	78800
FTA Regional 9 Office	TRO-9	78900
FTA Regional 10 Office	TRO-10	79000
Office of Administrator	TOA	61000
Office of Administration	TAD	62000
Office of the Chief Counsel	TCC	63000
Office of Communication and Congressional Affairs	TCA	64000
Office of Program Management	TPM	65000
Office of Budget and Policy	TBP	66000
Office of Research, Demonstration and Innovation	TRI	67000
Office of Civil Rights	TCR	68000
Office of Planning and Environment	TPE	71000
Office of Transit Safety and Oversight	TSO	74000
Office of Regional Services	TRS	78000

Table 1: FTA Cost Centers