



FEDERAL TRANSIT ADMINISTRATION

FTA Access Control and Entry System (FACES)

User Guide

version 6.3.7





Document Revision History

Version	Date	Summary of Changes	Author
6.3.0	8/09/2021	Updated with Login.gov instructions	Christina Palencia
6.3.1	10/29/2021	Updated OTrak user roles table	Christina Palencia
6.3.2	11/15/2021	Updated section 7.1	Christina Palencia
6.3.3	12/07/2021	Updated Sections 6.3 and 7.3	Christina Palencia
6.3.4	12/17/2021	Updated Screenshots to 6.3.4	Christina Palencia
6.3.5	1/10/2021	Updated email screenshots throughout	Christina Palencia
6.3.6	2/25/2022	Updated Sections 6.2.1, 6.2.2, 6.2.3, 6.3.2	Christina Palencia
6.3.7	3/28/2022	Added Section 3.3.1	Christina Palencia



TABLE OF CONTENTS

Contents

1	Introduction.....	4
2	User Access.....	5
2.1	Account Setup.....	5
2.2	Logging In.....	14
2.3	Account Information.....	23
2.4	Passwords.....	24
3	System Layout.....	28
3.1	Account Information.....	28
3.2	Manage Users.....	28
3.3	Actions.....	29
3.4	Reports.....	33
3.5	Help Center.....	37
4	System Users.....	40
4.1	User Types.....	40
4.2	User Roles.....	41
4.3	User Visibility.....	46
4.4	User Record Content.....	47
5	Managing the User’s Own Record.....	50
5.1	Related Actions.....	50
5.2	A Locked Account.....	67
6	User Management.....	73
6.1	User Management Responsibilities.....	73
6.2	User Creation.....	74
6.3	Managing User Records.....	109
7	Recertification.....	138
7.1	Recertification Process.....	138
7.2	User Lock/Unlock Request Process.....	143
7.3	Certifier Unlocking User’s Locked Account.....	144
	Appendix A – Abbreviations, Acronyms, and Terms.....	147
	Appendix B – User Role Rules.....	148
	FTA Platform Rules.....	148
	NTD Rules.....	148
	TrAMS Rules.....	149
	DGS Rules.....	151
	SSOR Rules.....	151
	CRM Rules.....	152
	FACES Rules.....	152



Appendix C – FTA Cost Centers	152
-------------------------------------	-----



1 Introduction

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

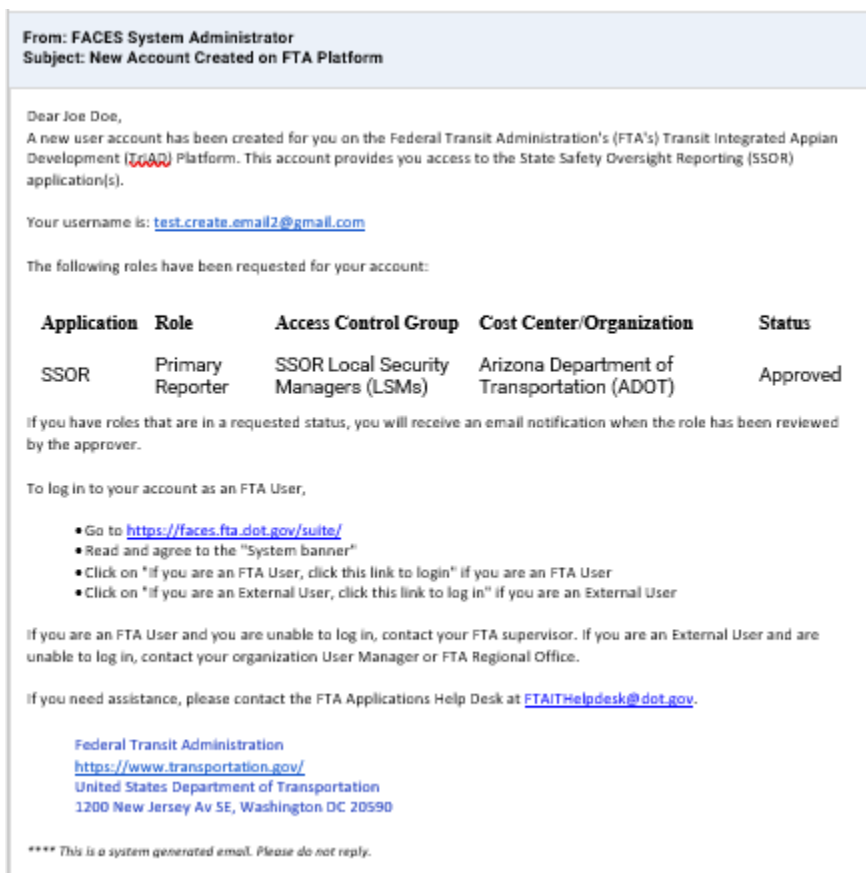
2.1 Account Setup

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

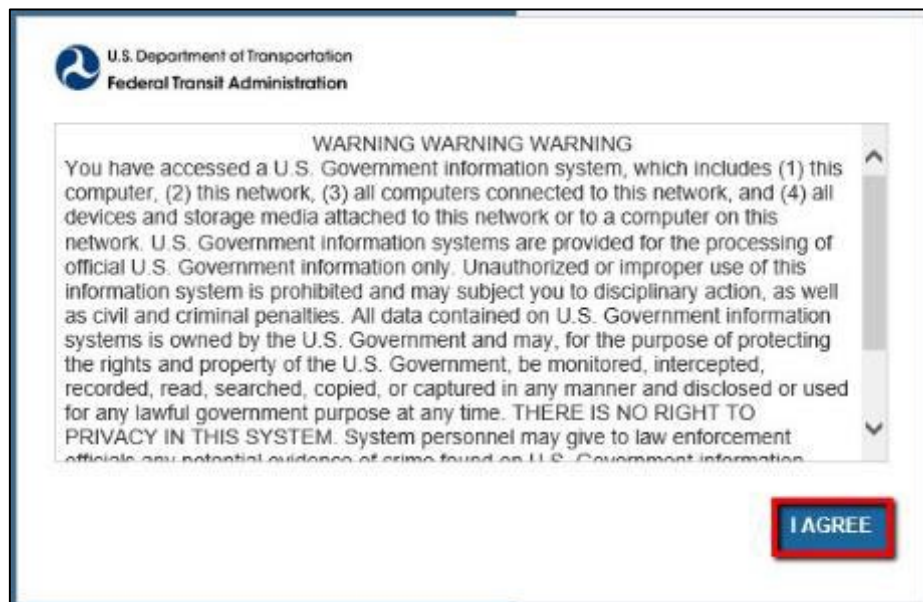
New non-FTA users will receive an automatic email notification from FACES once their account is created. It will look similar to the one below. If you need an account in the TriAD platform, then reach out to your User Manager or Local Security Manager.



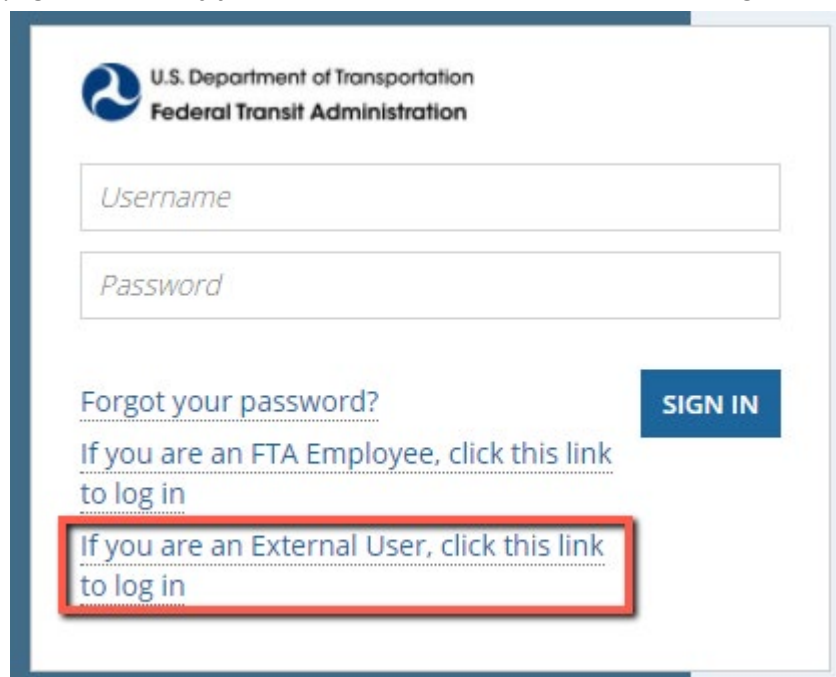
1) Using the email, select the URL (internet link) to access the site, <https://faces.fta.dot.gov/>



- 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) User 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 and account

A screenshot of the Login.gov interface for the U.S. Department of Transportation Federal Transit Administration. The header includes the LOGIN.GOV logo and the agency name. The main content area features a message from 'dev5' stating that Login.gov is used for safe and secure sign-in. Below this are input fields for 'Email address' and 'Password', with a 'Show password' toggle. Two buttons are present: a blue 'Sign in' button and a white 'Create an account' button with a red border. A link at the bottom reads 'Sign in with your government employee ID'.



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

LOGIN.GOV U.S. Department of Transportation
Federal Transit Administration

Create your account

Enter your email address

Select your email language preference

login.gov allows you to receive your email communication in English, Spanish or French.

☒ English (default)

☐ Español

☐ Français

☐ Check this box to accept the login.gov [Rules of Use](#)

Submit

[Cancel](#)

[Security Practices and Privacy Act Statement](#)

[Privacy Act Statement](#)

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

LOGIN.GOV

Confirm your email

Thanks for submitting your email address. Please click the link below or copy and paste the entire link into your browser. This link will expire in 24 hours.

Confirm email address

https://idp.int.identitysandbox.gov/sign_up/email/confirm?_request_id=152a7348-024b-4fb3-9751-8e83e10f6e70&confirmation_token=zyDhzaedCEX8lpRixRby

Please do not reply to this message. If you need help, visit www.login.gov/help

[About login.gov](#) | [Privacy policy](#)



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

A screenshot of the login.gov website's password creation page. At the top, there are logos for LOGIN.GOV and the U.S. Department of Transportation Federal Transit Administration. A green confirmation message states 'You have confirmed your email address'. The main heading is 'Create a strong password', followed by instructions: 'It must be at least 12 characters long and not be a commonly used password. That's it!'. There is a 'Password' input field with a 'Show password' toggle. Below the field is a green progress bar and the text 'Password strength: Great!'. A blue 'Continue' button is highlighted with a red border. At the bottom, there is a 'Password safety tips' link with a plus icon and a 'Cancel account creation' link.

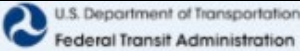

9) Select one of the five authentication method options and follow the setup instructions.

- **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](#).
- **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.
- **Authentication Application** - Authentication applications are downloaded to your device and generate secure, six-digit codes you use to sign into your accounts.
 - Google Authenticator
 - Authy
 - LastPass
 - 1Password
 - OTP Manager
 - Authenticator

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


- **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.
- **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.





Authentication method setup

Add a second layer of security so only you can sign in to your account.

 Keep this information safe. You will be locked out and have to create a new account if you lose your authentication method.

Select an option to secure your account:

☐ **Security key**

Use a security key that you have. It's a physical device that you plug in or that is built in to your computer or phone (it often looks like a USB flash drive). Recommended because it is more phishing resistant.

MORE SECURE

☐ **Government employee ID**

Insert your government or military PIV or CAC card and enter your PIN.

MORE SECURE

☐ **Authentication application**

Get codes from an app on your phone, computer, or tablet. Recommended because it is harder to intercept than texts or phone calls.

SECURE

☐ **Phone**

Get security codes by text message (SMS) or phone call. Please do not use web-based (VOIP) phone services.

LESS SECURE

☐ **Backup codes**

We'll give you 10 codes. You can use backup codes as your only authentication method, but it is the least recommended method since notes can get lost. Keep them in a safe place.

LEAST SECURE

Continue

[Cancel account creation](#)



- 10) Once the authentication method has been setup, the user will be redirected to sign in to Login.gov using the credentials just created.

LOGIN.GOV

Sign in

Email address
external.user@email.com

Password
..... ☐ Show password

Sign in

Create an account

[Sign in with your government employee ID](#)

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

Home

Federal Transit Administration

Welcome to the Transit Integrated Applan Platform!

Current user: Doe, Joe
Last Login Date:

TrAMS Transit Award Management System	NTD National Transit Database	SSOR State Safety Oversight Reporting
COVID-19 Form Transit COVID-19 Response Program	FACES User Management	

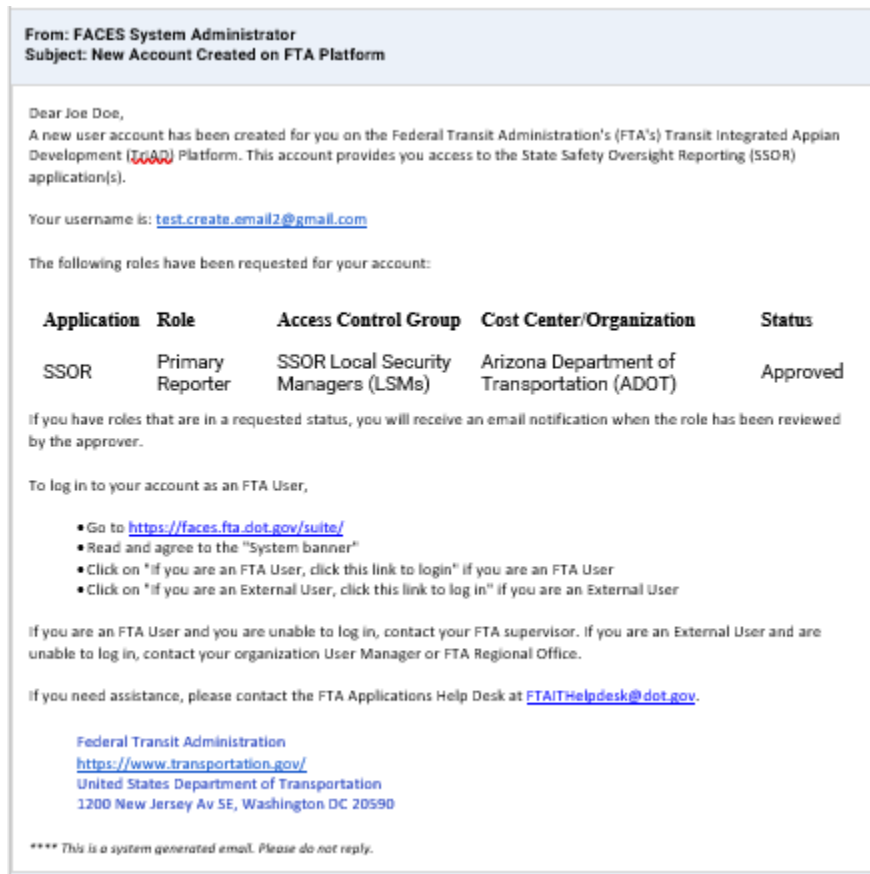
Please select a system above. To set a default system, click on the star next to desired system. For any questions, please contact the FTA Application Helpdesk at FTAITHelpdesk@dot.gov.

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 in the TriAD platform, then reach out to your User Manager or Local Security Manager.

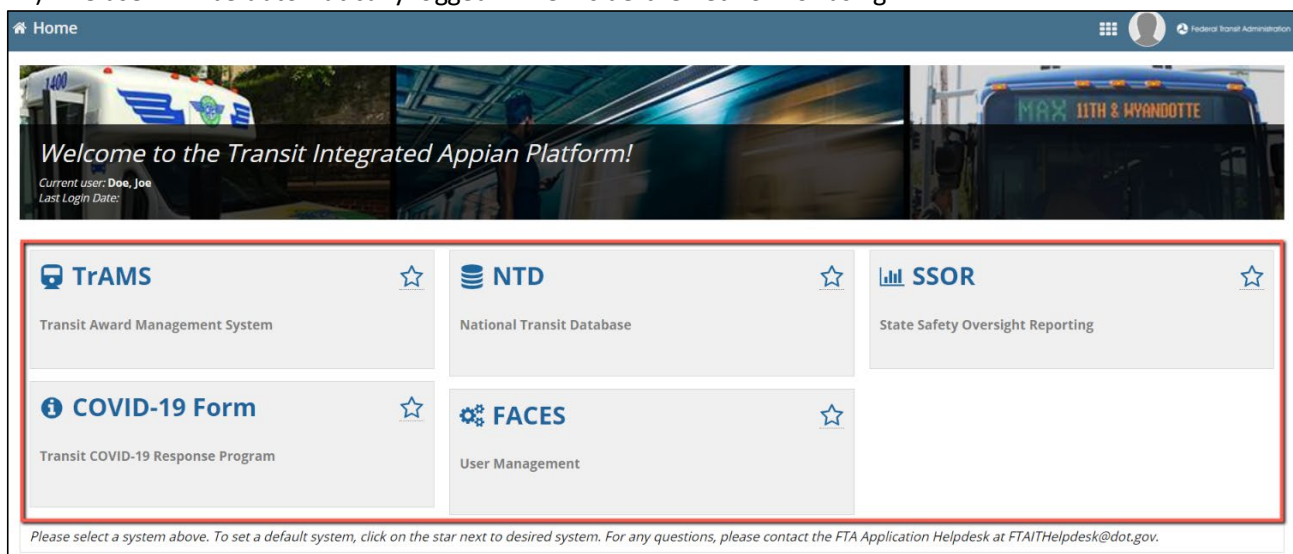


12) The email will be formatted much like the one below:



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

14) 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.

The screenshot shows the FACES user interface. At the top, there is a navigation bar with a 'Home' link, a user profile icon, and the text 'Federal Transit Administration'. Below the navigation bar is a large banner image with the text 'Welcome to the Transit Integrated Appian Platform!'. Underneath the banner, it says 'Current user: Palencia, Christina' and 'Last Login Date: 6/3/2021 9:20 AM EDT'. To the right of the banner, there is a red-bordered button that says 'Click here to finish setting up your Security Questions and Answers'. Below the banner, there are two main sections: 'OTrak' (Oversight Tracking System) and 'FACES' (User Management). Each section has a star icon next to it. At the bottom of the page, there is a small text line: 'Please select a system above. To set a default system, click on the star next to desired system. For any questions, please contact the FTA Application Helpdesk at FTAHelpdesk@dot.gov.'

- 15) 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.

- 16) Click **Submit**.

The screenshot shows the 'Manage Security Questions' form. It has a title 'Manage Security Questions' and a subtitle 'Select and answer three (3) security questions. These questions can be used for authentication to unlock your account. Please note that your answers are not case sensitive.' The form contains three sections, each for a question. Each section has a dropdown menu for 'Question', a text input for 'Answer', and a text input for 'Retype Answer'. At the bottom right of the form, there is a red-bordered button labeled 'SUBMIT'.

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



2.2 Logging In

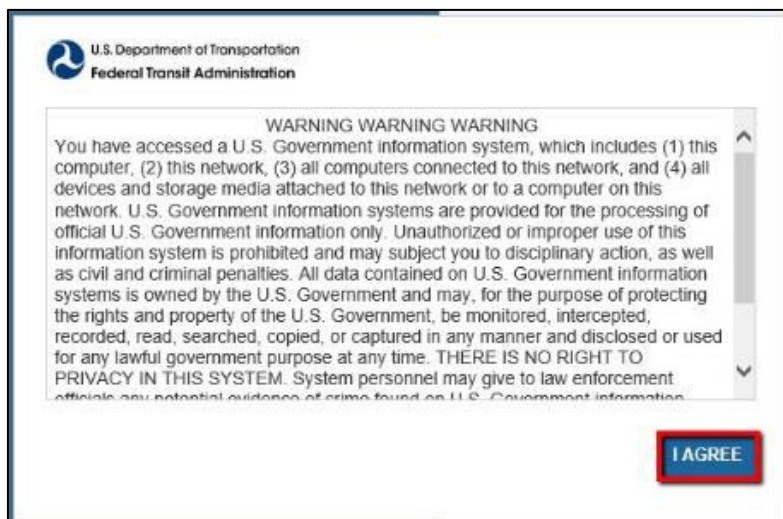
FACES manages user access to the FTA platforms via the FACES login page, accessed via a web browser. Two login methods are available, but one is only accessible to FTA employees using FTA's internal network. User access to software systems like TrAMS and NTD is based on the user's assigned **Roles**.

2.2.1 Standard Login (Non-FTA Employee)

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

To log in:

- 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***.

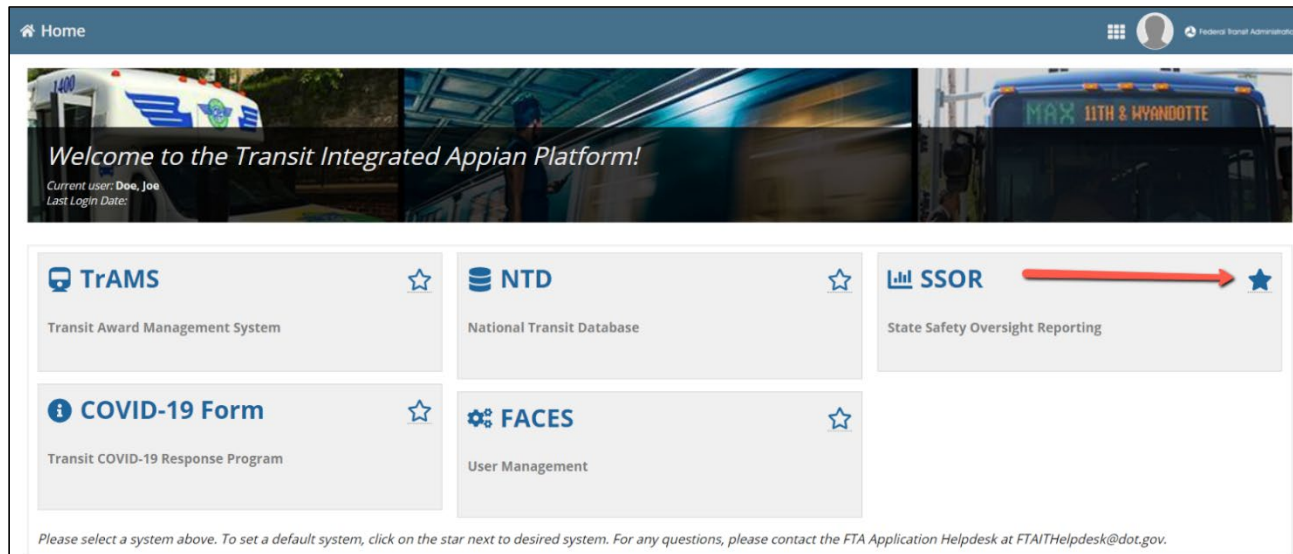


- 4) User will be redirected to Login.gov where all external users will need to sign in with the account that was created in section 2.1.1 and will need to be authenticated with the authentication method that was setup.

- 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.

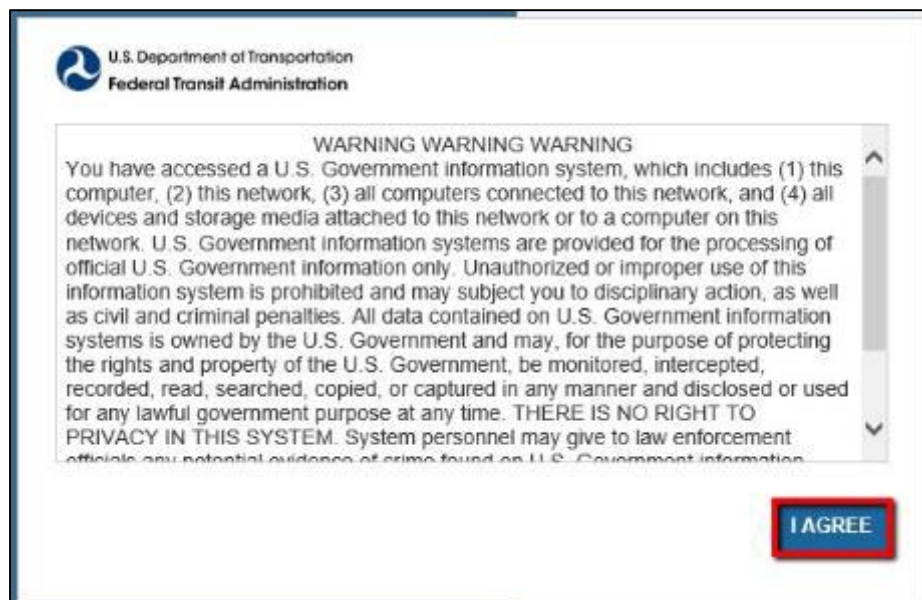


2.2.2 FTA Employee Login

FTA employees should access FACES via the FTA network. To log in:

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.

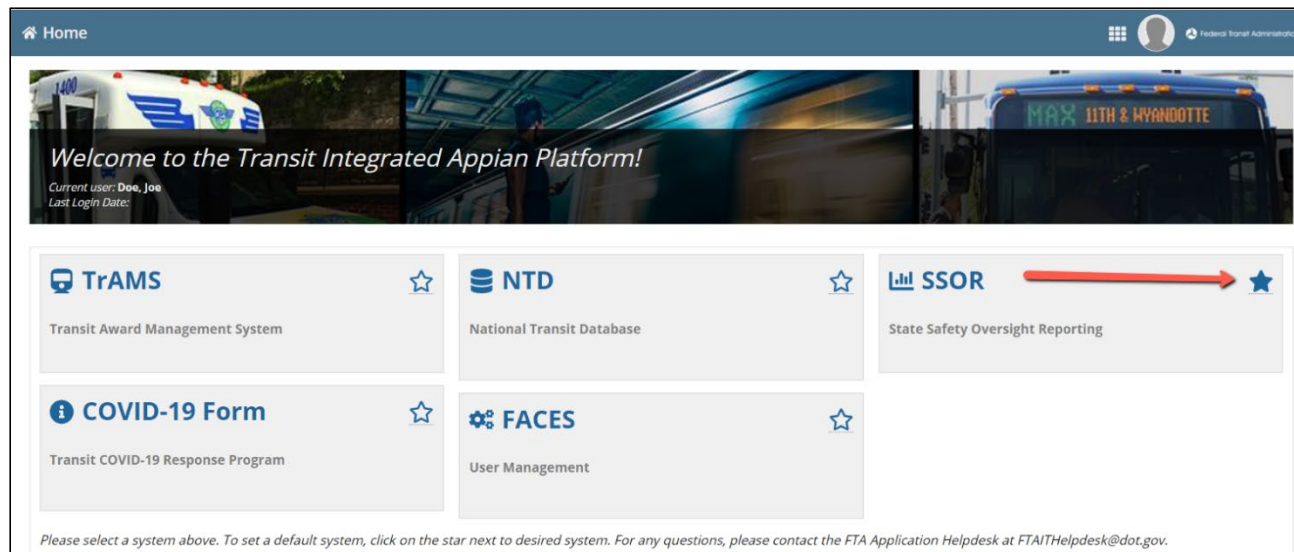
- 4) FTA Users will be automatically taken into the TrIAD Platform home page if they are in FTA network or logged into VPN.
- 5) On the Homepage, the user has the option to click the system they wish to use. If the user has access to more than one FTA platform (TrAMS, NTD, DGS, SSOR or FACES) all those options will be available as an option on the Home page.

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.



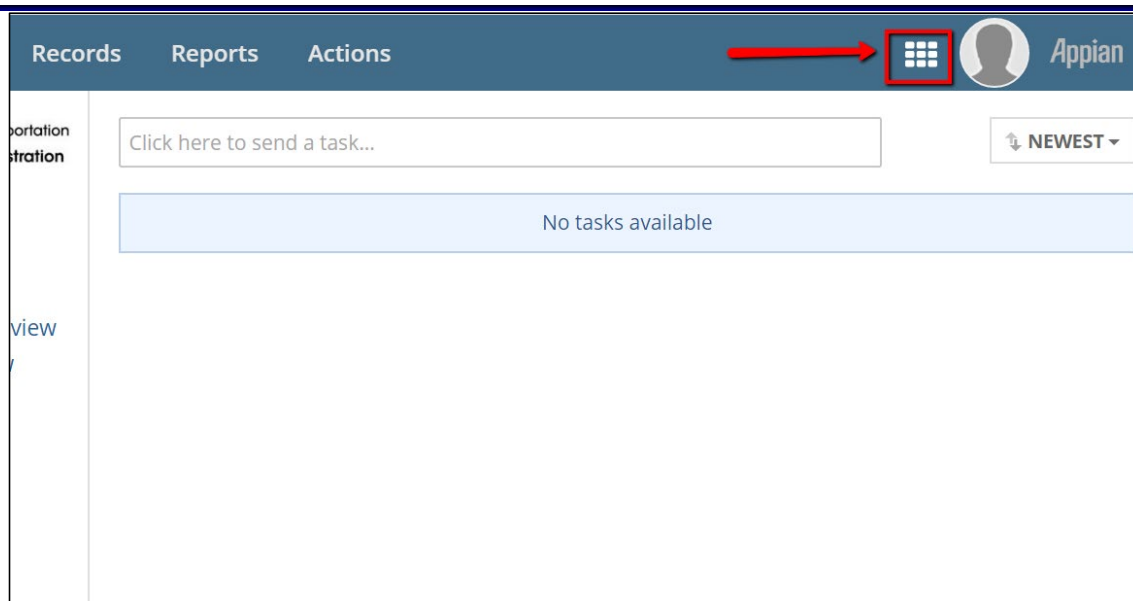
When a default system is selected, the next time a user logs in, they are taken to the default system and bypass the Sites Splash page.

2.2.3.1 Changing User Default System or Return to Homepage

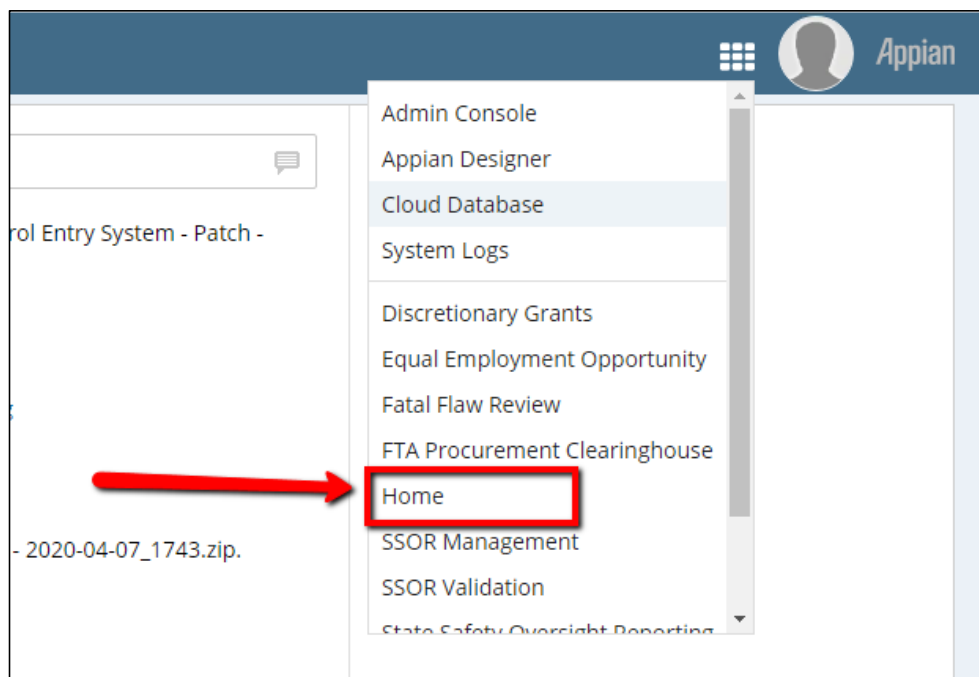
If a user wishes to change their default system to another system, they can do so by returning to the Homepage.

To return to the home page,

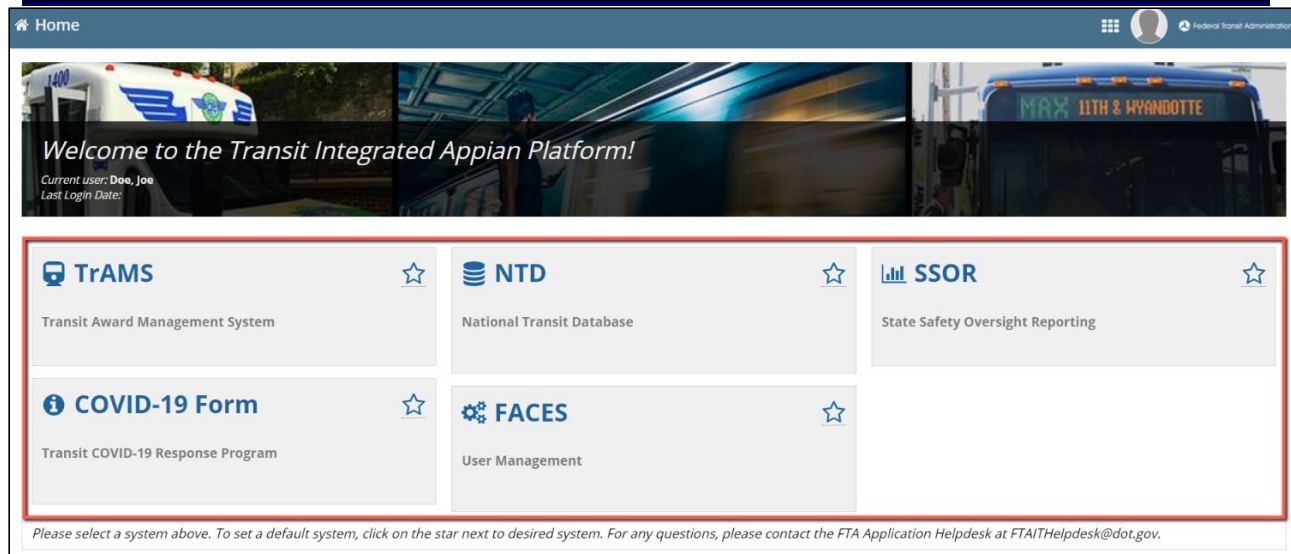
- 1) Click on the **NAVIGATION** button at the top right corner, next to the avatar.



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



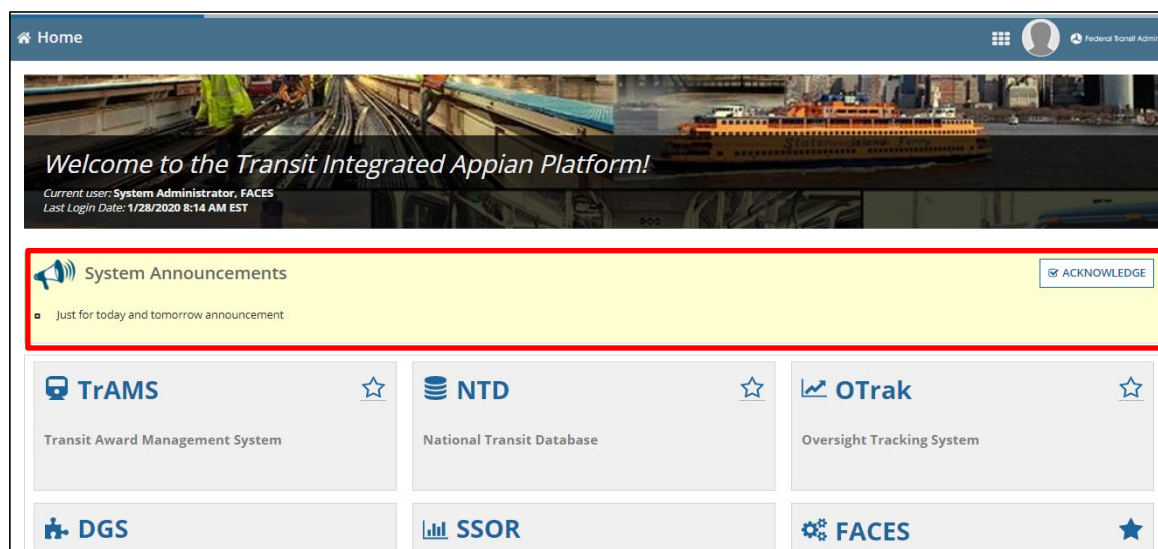
3) The user is taken back to the Homepage and can select another system to make a default system.



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

2.2.4 System Announcements

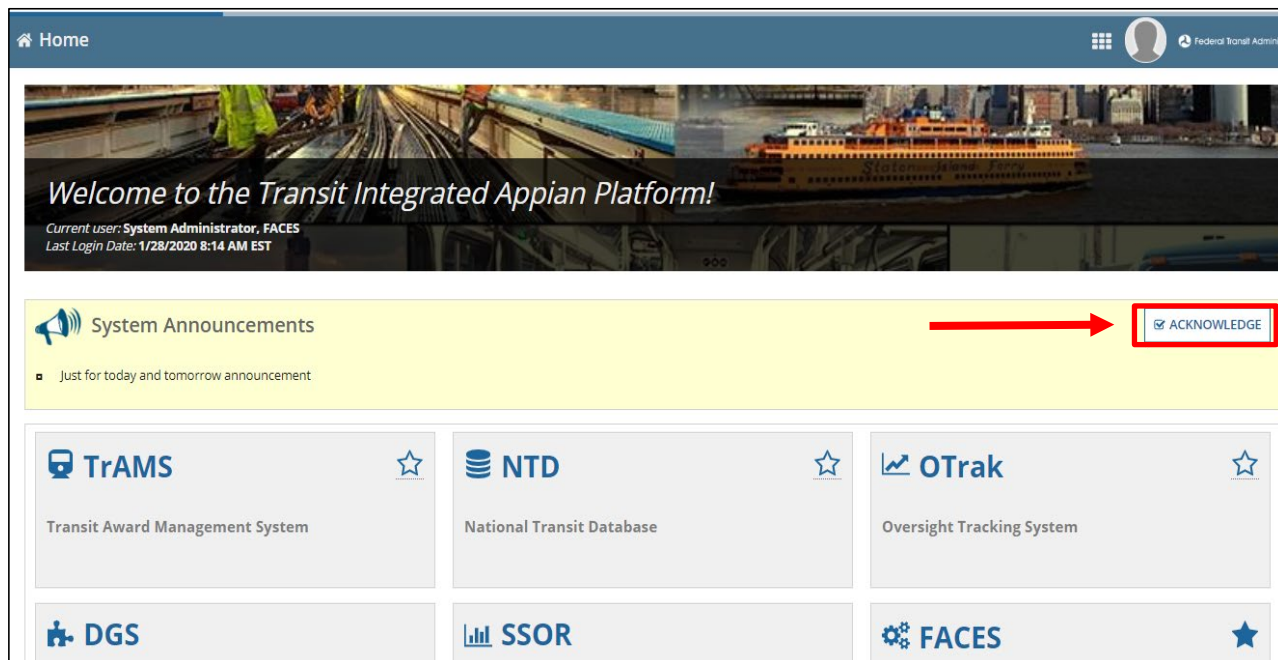
System Announcements are often needed to communicate to users about important information. When an announcement is created, it is posted in a yellow banner in the Homepage as shown below.



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.



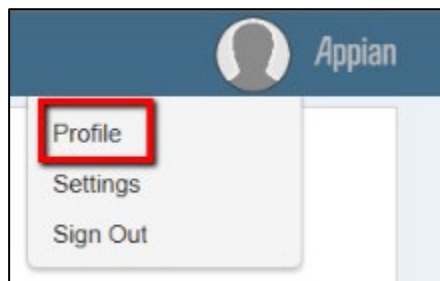
The next time the user logs in, they are directed to their default system if they elected one. However, anytime there is a new System Announcement, the user will always be directed to the FTA Home page when they login until they have acknowledged the announcement.

2.2.5 Accessing Your 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 record **Summary Page** displays.





2.3 Account Information

2.3.1 User Profile Contents

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 particular 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.

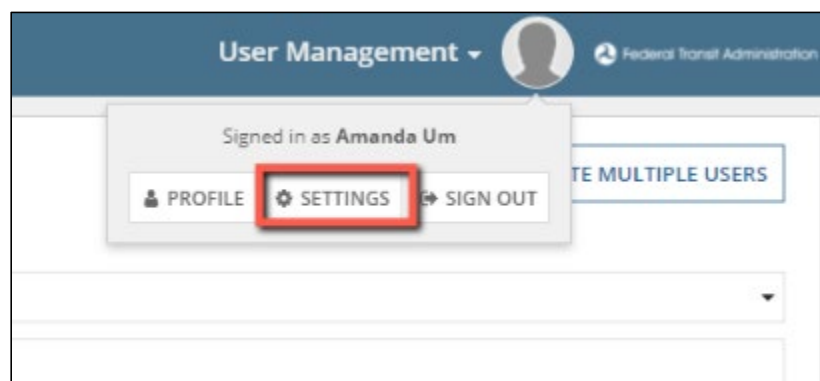
2.3.2 Account Settings

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.

Settings

General Password Third-Party Credentials Email Notifications Mobile Notifications Accessibility

Language

Use system default: English (United States)

Time Zone

Use system default: (UTC-05:00) Eastern Time (America/New_York); (UTC-05:00) Eastern Time (America/New_York)

Calendar Type

Use system default: Gregorian

CANCEL SAVE CHANGES

- 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 \(FTA Employees Only\)](#)
- [2.4.2 Forgot Login.gov Password \(Non-FTA Employees Only\)](#)
- [2.4.3 Reset Login.gov Account \(Non-FTA Employees Only\)](#)



2.4.1 Forgotten Passwords (FTA Employees Only)

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

dev5 is using login.gov to allow you to sign in to your account safely and securely.

Email address

Password ☐ Show password

[Sign in](#)

[Create an account](#)

[Sign in with your government employee ID](#)

[Back to dev5](#)

[Forgot your password?](#)

[Security Practices and Privacy Act Statement](#)

[Privacy Act Statement](#)



- 2) Enter the users email address and click Continue.

A screenshot of a web form titled "Forgot your password?". Below the title is a sub-header: "Don't know your password? Reset it after confirming your email address." There is a text input field labeled "Email". Below the input field is a blue button labeled "Continue". At the bottom left of the form is a blue link labeled "Cancel".

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

A screenshot of an email from LOGIN.GOV titled "Reset your password". The body text says: "To finish resetting your password, please click the link below or copy and paste the entire link into your browser." Below this is a blue button labeled "Reset your password" which is highlighted with a red rectangle. Under the button is a long URL: "https://idp.int.identitysandbox.gov/users/password/edit?reset_password_token=SZiXq-FmaLh61H-yK3u". Below the URL, it says "This link expires in 6 hours." At the bottom, it says "Please do not reply to this message. If you need help, visit www.login.gov/help" and includes links for "About login.gov" and "Privacy policy".

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

A screenshot of a web form titled "Change your password". It features a text input field for "New password" with a "Show password" checkbox to its right. Below the input field is a green progress bar and the text "Password strength: Great!". Below this is a blue button labeled "Change password" which is highlighted with a red rectangle. At the bottom is a box labeled "Password safety tips" with a blue plus icon to its right.



5) 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”

LOGIN.GOV

Present your PIV/CAC
Present the PIV/CAC that you associated with your account.

Present PIV/CAC card

Don't have your PIV or CAC available?
[Choose another authentication method](#)

[Cancel](#)

- 3) Scroll to the bottom and click on the “deleting your account” link

LOGIN.GOV

Select your authentication method
You set these up when you created your account

☒ **Text message**
Get security code via text/SMS or phone call to ***-4041.

☐ **Automated phone call**
Get security code via text/SMS or phone call to ***-4041.

☐ **Government employee ID**
Use your PIV/CAC card instead of a security code.

Continue

If you can't use any of the authentication methods above, you can reset your preferences by [deleting your account](#).

[Cancel](#)



- 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.

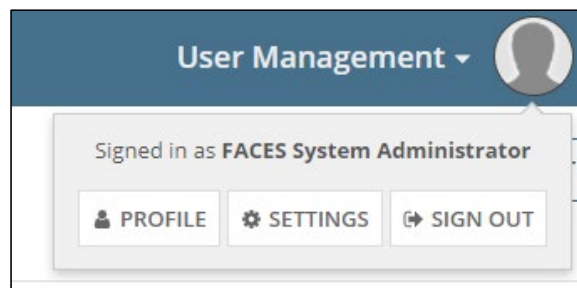
3 System Layout

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.



MANAGE USERS ACTIONS REPORTS HELP CENTER

User Management Federal Transit Administration

+ CREATE NEW USER + CREATE MULTIPLE USERS

Report Filter Criteria

System: TRAMS

Role Category: Select role category

Access Control Group: Select a group

Organization: Select an Organization

Role: Submitter

Cost Center: Select Cost Center

User: Select an active user

Name: Search on First or Last name (whole or part)

Status: ☒ Active ☒ Locked

CLEAR FILTER(S)

Users

Username	Name (Last, First)	System	Access Control Group	Cost Center	Organization	Role	Last Certified Date	Created Date	Modified Date	Last Login Date	Status
aiden.al@mailinator.com	Al, Aiden (Mr.)	TRAMS	Region 3	TRO-3	1396 - DELDOT	Submitter	11/25/2020 2:08 PM EST				
		TRAMS	Region 3	TRO-3	1398 - WMATA	Submitter	11/25/2020 2:08 PM EST				
		TRAMS	Region 3	TRO-3	1428 - HRA	Submitter	11/25/2020 2:08 PM EST	3/20/2019 10:44 AM EDT	9/2/2020 9:40 PM EDT	10/6/2020 9:56 AM EDT	Active
		TRAMS	Region 4	TRO-3	1448 - CHARLOTTESVILLE	Submitter	11/25/2020 2:08 PM EST				
		TRAMS	Region 1	TRO-4	1032 - COLLIER COUNTY	Submitter	11/25/2020 2:08 PM EST				
		TRAMS	Region 1	TRO-1	1334 - CONNDOT	Submitter	1/8/2021 10:33 AM EST				
assia.khadri@fake.com	khadri, assia (Mr.)	TRAMS	Region 1	TRO-1	1334 - CONNDOT	Submitter	11/30/2020 12:49 PM EST	9/6/2019 11:18 AM EDT	3/9/2020 2:54 PM EDT	10/6/2020 9:56 AM EDT	Active
bobthomas@mailinator.com	Thomas, Bob (Mr.)	TRAMS	Region 1	TRO-1	1330 - CRCOG	Submitter	12/30/2020 12:48 PM EST	12/30/2020 12:48 PM EST	12/30/2020 12:58 PM EST	12/30/2020 12:48 PM EST	Active
conndot.attorney1@dot.gov	Attorney, conndot	TRAMS	Region 1	TRO-1	1334 - CONNDOT	Submitter	11/16/2020 1:54 PM EST	1/11/2019 1:48 PM EST	11/16/2020 1:54 PM EST	10/6/2020 9:56 AM EDT	Active

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)**.

MANAGE USERS **ACTIONS** REPORTS HELP CENTER

User Management Federal Transit Administration

Assign Bulk Roles
Assign Bulk Roles to Multiple Users

Create and Manage Users
Create or Activate a New System User

Create Multiple Users
Upload information for Multiple New Users

Recertify Users
Recertify User Role(s) for Active Users

Remove Bulk Roles
Remove Roles in Bulk

Review Role Requests
Approve or Reject Role Requests

Review Unlock Requests
Approve or Reject Unlock Requests

Manage Access Control Groups
Create or Edit Access Control Groups and Manage Organizations

Manage Recertification
Manage User Role Certification Cycle

Manage Role Documentation
Add or Remove Role Justification Documentation

Manage System Announcements
Manage System Announcements

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

MANAGE USERS

ACTIONS

REPORTS

HELP CENTER

User Management

Assign Bulk Roles

Assign Bulk Roles to Multiple Users

Create and Manage Users

Create or Activate a New System User

Create Multiple Users

Upload Information for Multiple New Users

Recertify Users

Recertify User Role(s) for Active Users

Remove Bulk Roles

Remove Roles in Bulk

Review Role Requests

Approve or Reject Role Requests

Review Unlock Requests

Approve or Reject Unlock Requests

Manage Access Control Groups

Create or Edit Access Control Groups and Manage Organizations

Manage Recertification

Manage User Role Certification Cycle

Manage Role Documentation

Add or Remove Role Justification Documentation

Manage System Announcements

Manage System Announcements

Bulk Unlock Users

Unlock Users in Bulk

Send Ad-hoc Emails

Send Ad-hoc Emails to multiple users

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

April 11, 2022
FACES User Guide-6.3.7.doc



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

Send Ad-Hoc Email

▼ User Filters

System: --Select A Value--

Role Category: --Select A Value--

User Type: --Select A Value--

Role: --Select A Value--

Send To All Users? ☐ Yes
This will send to all Active and Locked users in the system across all applications.

Include Help Desk Information? ☐ Yes
This will include relevant Help Desk information in the footer of the email.

User Status: ☒ Active ☒ Locked

▼ Email Details

Subject *: [Text Field] 0/255

Body *: [Text Field] 0/8000

[+] Show formatting instructions

CANCEL NEXT

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

Send Ad-Hoc Email

▼ User Filters

System: --Select A Value--

Role Category: --Select A Value--

User Type: --Select A Value--

Role: --Select A Value--

Send To All Users? ☐ Yes
This will send to all Active and Locked users in the system across all applications.

Include Help Desk Information? ☐ Yes
This will include relevant Help Desk information in the footer of the email.

User Status: ☒ Active ☒ Locked

▼ Email Details

Subject *: [Text Field] 0/255

Body *: [Text Field] 0/8000

[+] Show formatting instructions

CANCEL NEXT

5. After completing the email, click Next to go to the next screen
6. On the confirmation screen, the GSM can review all of 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



Ad-hoc Email Confirmation

Selected Filters

System FACES

User Type FTA

Send To All Users? No
This will send to all Active and Locked users in the system across all applications.

Include Help Desk Information? No

Role Category Global Users

Role N/A

User Status Active, Locked

Basic Information

Subject Reminder

Body This is a friendly reminder that training certificate submissions are due at this time.

Recipient Type Bcc

Email Recipients

Username	System(s)	User Type	Email Address	Status
aaria.supervisor@dot.gov	FACES	FTA	example@example.com	Active
abby.administrator@dot.gov	FACES	FTA	sunjida.alam@hil.us	Locked
demo.dgs.gsm21@dot.gov	FACES	FTA	dgs.gsm@example.com	Active
demo.ntd.gsm21@dot.gov	FACES	FTA	brian.anderson@hil.us	Active
demo.ssr.gsm21@dot.gov	FACES	FTA	brian.anderson@hil.us	Active

1 - 5 of 15

Warning

Submitting this form will send an email to 15 user(s). To submit this form you will need to click the proceed and send test email button which will send a test email to your email address on record. Please validate all information before submitting. This action should not be run during peak business hours.

PROCEED AND SEND TEST EMAIL

CANCEL BACK

SEND TEST EMAIL SUBMIT

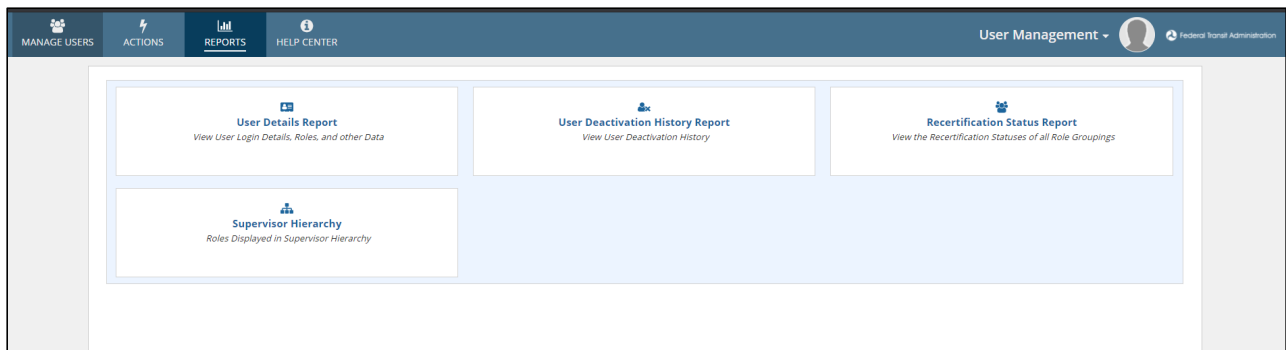
- Any changes can be made to the email by clicking on Back
- When ready to send the final email, click on Submit



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:

System

Select an Application

Role Category

Select role category

Access Control Group

Select a group

Organization

Role

Select a Role

Display individual Roles in Grid

☒

Cost Center

Select Cost Center

User

Select a user (including deactivated)

Name

Search on First or Last name (whole or part)

Status

☐ Active
☐ Locked
☐ Deactivated

CLEAR FILTER(S)

Users

Username	Name (Last, First)	System	Access Control Group	Cost Center	Organization	Role	Last Certified Date	Created Date	Modified Date	Last Login Date	Status
----------	--------------------	--------	----------------------	-------------	--------------	------	---------------------	--------------	---------------	-----------------	--------

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 User Name, or by partial name (first or last). The list can also be filtered by users who are **Active**, **Locked**, or **Deactivated**.



[+ CREATE NEW USER](#)
[+ CREATE MULTIPLE USERS](#)

Report Filter Criteria

System Select an Application

Role Category Select role category

Access Control Group Select a group

Organization Select an Organization

Role Read Only - (TrAMS), User Manager - (TrAMS)

☒ Display individual Roles in Grid

Cost Center Select Cost Center

User Select a user (including deactivated)

Name Search on First or Last name (whole or part)

Status ☒ Active
☐ Locked
☐ Deactivated

[CLEAR FILTER\(S\)](#)

Users

Username	Name (Last, First)	System	Access Control Group	Cost Center	Organization	Role	Last Certified Date	Created Date	Modified Date	Last Login Date	Status
aiden.al@mailinator.com	Al, Aiden (Mr.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	9/3/2020 9:18 PM GMT+00:00	3/20/2019 2:44 PM GMT+00:00	9/3/2020 1:40 AM GMT+00:00	9/2/2020 11:09 AM GMT+00:00	Active
alexa.hill@mailinator.com	Hill, Alexa (Mrs.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	7/15/2020 1:22 PM GMT+00:00	2/7/2019 9:17 PM GMT+00:00	8/17/2020 4:04 PM GMT+00:00	9/2/2020 11:09 AM GMT+00:00	Active

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

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

User Details Report

Report Filter Criteria

System TrAMS

Role Category Recipient

Access Control Group Select a group

Organization Select an Organization

Role Select a Role

☒ Display individual Roles in Grid

Cost Center TRAMS - Region 2 [TRD-2]

User Select a user (including deactivated)

Name Search on First or Last name (whole or part)

Status ☒ Active
☐ Locked
☐ Deactivated

[CLEAR FILTER\(S\)](#)

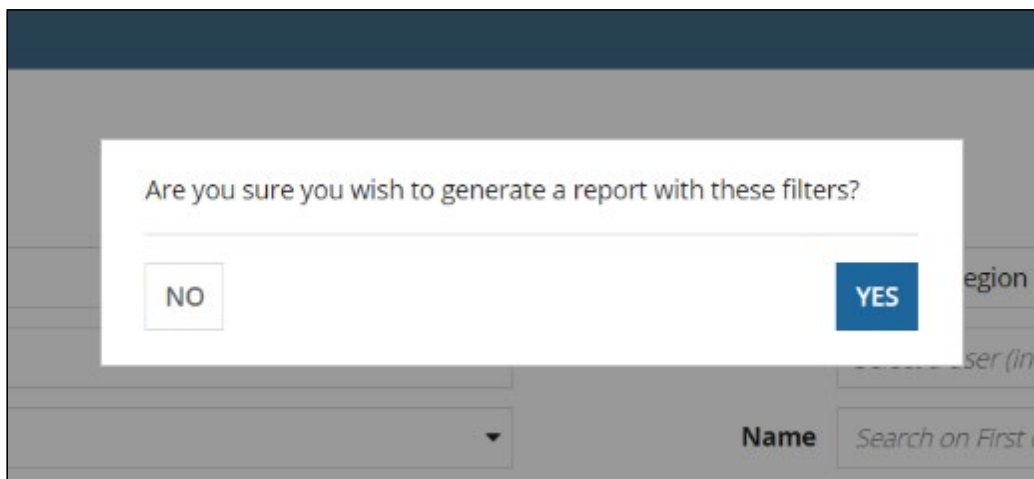
Users

Username	Name (Last, First)	System	Access Control Group	Cost Center	Organization	Role	Last Certified Date	Created Date	Modified Date	Last Login Date	Status
aryatunguser1@mailinator.com	Oruguer, Anya (Mrs.)	TrAMS	TrAMS Region 2	TRO-2	1414 - NJTC	Developer	11/14/2019 8:08 PM GMT+00:00	11/5/2019 10:07 PM GMT+00:00	11/5/2019 10:07 PM GMT+00:00	11/5/2019 10:07 PM GMT+00:00	Active
sunnie تراموس@mailinator.com	tramsum, Sunnie (Mrs.)	TrAMS	TrAMS Region 2	TRD-2	1414 - NJTC	User Manager	11/14/2019 9:19 PM GMT+00:00	11/4/2019 6:23 PM GMT+00:00	11/4/2019 6:23 PM GMT+00:00	11/4/2019 6:23 PM GMT+00:00	Active
testtramsales@mailinator.com	t. peter (Mr.)	TrAMS	TrAMS Region 2	TRO-2	1414 - NJTC	User Manager	11/5/2019 8:03 PM GMT+00:00	11/5/2019 8:02 PM GMT+00:00	11/5/2019 8:02 PM GMT+00:00	11/5/2019 8:02 PM GMT+00:00	Active

[GENERATE REPORT](#)



A prompt will pop 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.

adot.alternate.reporter@dot.gov	Alternate Reporter, adot	SSOR	SSOR Local Security Managers (LSMs)	TSD	1 - ADOT	Alternate Reporter	2/25/2020 10:44 AM EST	11/19/2019 10:57 AM EST	11/19/2019 10:57 AM EST	1/28/2020 8:14 AM EST	Active
adot.alternate.reporter-5@test.com	Alternate Reporter, adot	SSOR	SSOR Local Security Managers (LSMs)	TSD	1 - ADOT	User Manager	2/25/2020 10:44 AM EST	9/23/2019 4:15 PM EDT	9/23/2019 4:16 PM EDT	1/28/2020 8:14 AM EST	Active

1 - 10 of 337

Your document is being generated. You will receive a Task with a download link when it is ready. Please note that the process may take a while.

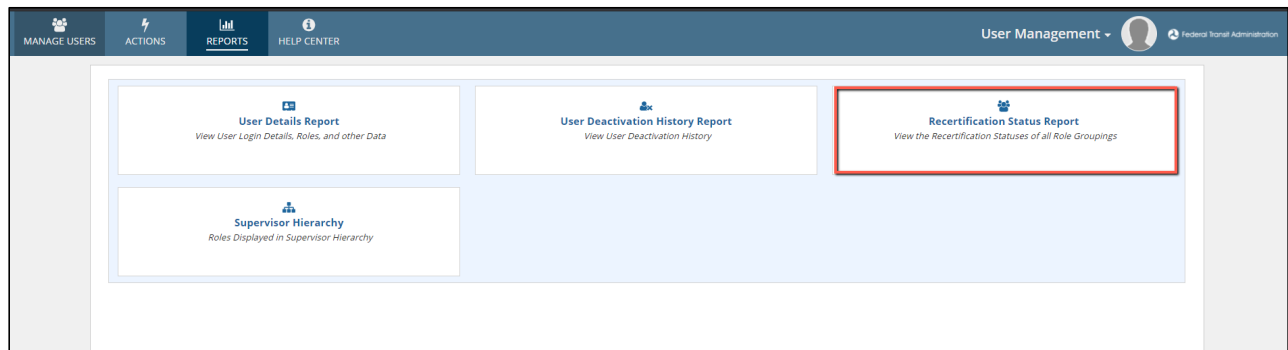
GENERATE REPORT

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) Clicks **Recertification Status Report**.



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

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

Filters

System

FACES

Recertification Group

Select Recertification Group

Access Control Group

Select a Group

Year

2020

Role

Select a Role

Organization

Select an Organization

CLEAR FILTER(S)

Recertification Status By Role Grouping

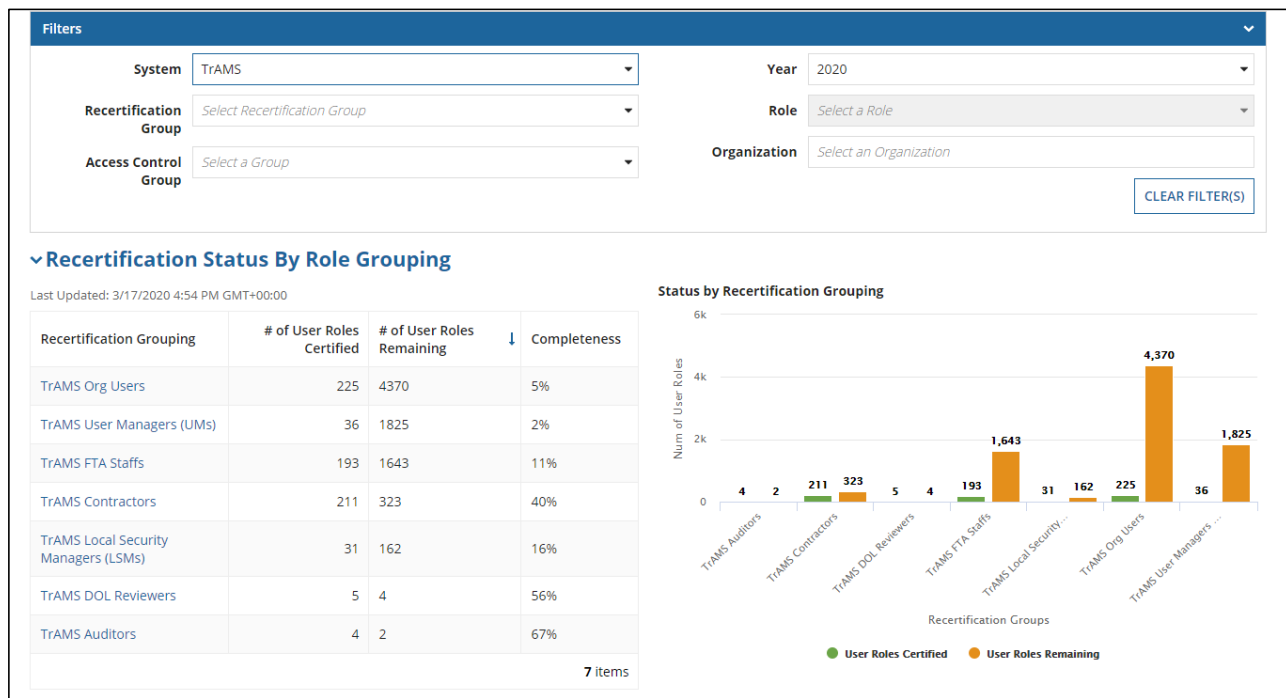
Last Updated: 3/17/2020 4:54 PM GMT+00:00

Recertification Grouping	# of User Roles Certified	# of User Roles Remaining	Completeness
No data available.			

Status by Recertification Grouping

No data available

5) **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.

MANAGE USERS ACTIONS REPORTS **HELP CENTER**
User Management Federal Transit Administration

Hello, Aiden.

Welcome to the FACES Help Center!

FACES User Manual

This easy-to-browse user manual will show you how to leverage FACES in a productive and efficient way to work for you!

Frequently Asked Questions

Answers to frequently asked questions about FACES, such as: how to perform basic functions and navigate the application.

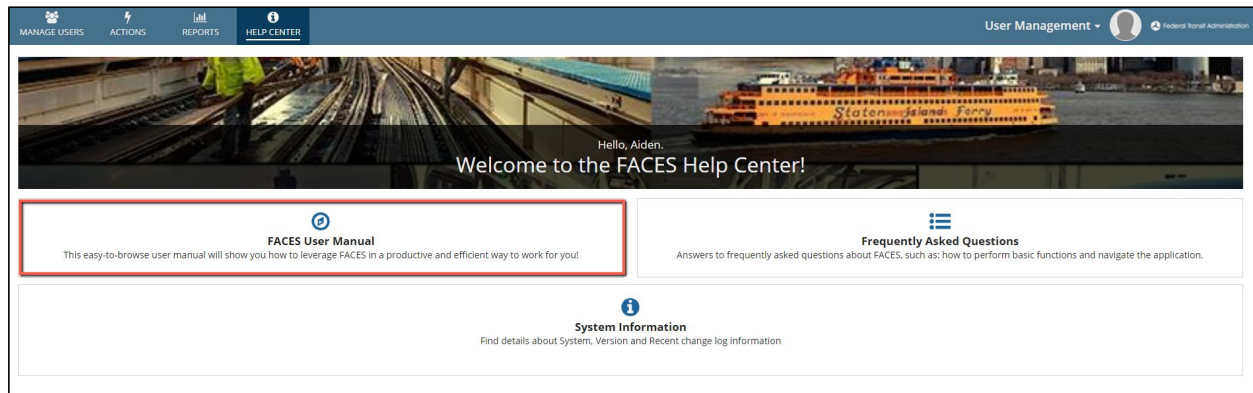
System Information

Find details about System, Version and Recent change log information

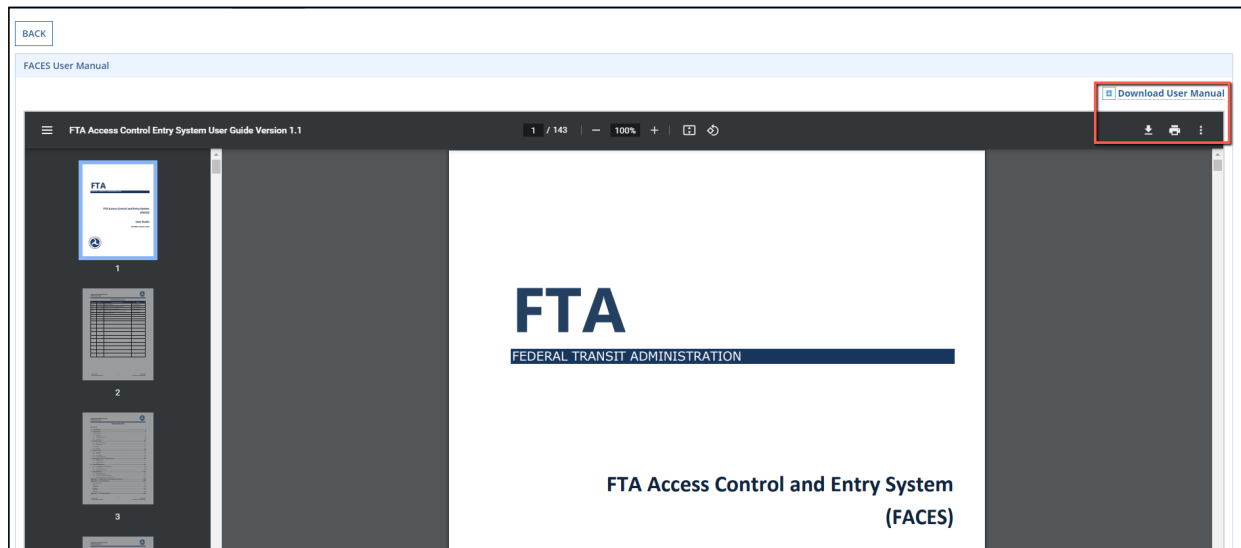


3.5.1 FACES User Manual

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

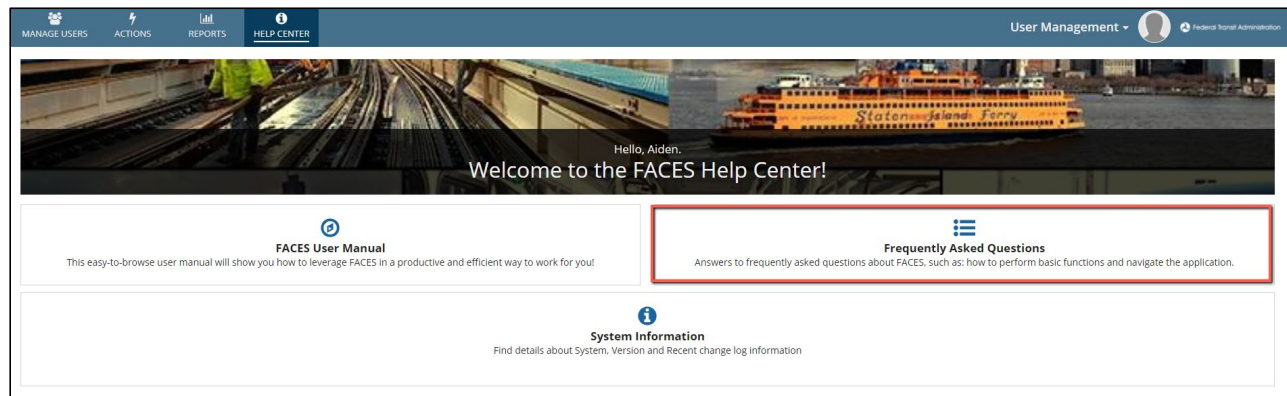


On this page the user can view it directly, download, or print it out.



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.

BACK

Frequently Asked Questions

Login.gov FAQs

Can I recover my account if I lose my MFA authentication method/password?

How can I use Login.gov for logging into the TriAD Platform?

How do I access my account if I don't have access to any of the multi-factor authentication (MFA) methods? For ex: I changed my mobile number (or) I have uninstalled Authenticator app

How do I reset my Login.gov password?

If a user already has a Login.gov account, will they be able to use it for this platform?

If a user has a Login.gov account with a different email address, how can they add additional emails to the account?

What happens if a user enters an incorrect password multiple times?

What happens if a user requests too many security codes?

What happens if a user submits an incorrect MFA authentication code multiple times?

What is the difference between External users and FTA users?

What should a user do if they get locked out of their account?

Where can I find training materials related to Login.gov?

FACES FAQs

Can I manage my own user role(s)?

How do I create a User Manager?

How do I create a new User?

How do I recertify a user?

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.

MANAGE USERS
ACTIONS
REPORTS
HELP CENTER

User Management - Federal Transit Administration

Hello, TrAMS.
Welcome to the FACES Help Center!

FACES User Manual
This easy-to-browse user manual will show you how to leverage FACES in a productive and efficient way to work for you!

Frequently Asked Questions
Answers to frequently asked questions about FACES, such as: how to perform basic functions and navigate the application.

System Information
Find details about System, Version and Recent change log information



System Information

FACES - System Information

System Details

Name

FACES

Description

User Management

Current Version

6.1.19

Release Date

May 12, 2021

System

FACES

Help Contacts

Description	Contact Information
FACES Help Desk Email	FTAITHelpdesk@dot.gov

Releases

System	Version	Description	Release Date
FACES	4.8.6	FTA Access Control Entry System	6/5/2019 12:00 AM EDT
FACES	6.1.10	Minor: TESS-6370: RESOLVED: Fixes filter population issues in Recertify users page TESS-6622: ENHANCED: Removes unnecessary reactivation/deactivation in LDAP nightly sync process TESS-6749: RESOLVED: Allows TrAMS user details report viewers to view TrAMS user profiles TESS-7168: RESOLVED: Allows hyphen in address line1 for User profiles TESS-7236: RESOLVED: Allows unchecking favorite option, if user would like to set Site splash page as a default page. TESS-7240: ENHANCED: Adds additional roles for OTrak system	11/12/2020 2:56 PM EST

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

System Information

FACES - System Information

System Details

Name

FACES

Description

User Management

Current Version

6.1.19

Release Date

May 12, 2021

System

FACES

Help Contacts

Description	Contact Information
FACES Help Desk Email	FTAITHelpdesk@dot.gov

Releases

System	Version	Description	Release Date
FACES	4.8.6	FTA Access Control Entry System	6/5/2019 12:00 AM EDT
FACES	6.1.10	Minor: TESS-6370: RESOLVED: Fixes filter population issues in Recertify users page TESS-6622: ENHANCED: Removes unnecessary reactivation/deactivation in LDAP nightly sync process TESS-6749: RESOLVED: Allows TrAMS user details report viewers to view TrAMS user profiles TESS-7168: RESOLVED: Allows hyphen in address line1 for User profiles TESS-7236: RESOLVED: Allows unchecking favorite option, if user would like to set Site splash page as a default page. TESS-7240: ENHANCED: Adds additional roles for OTrak system	11/12/2020 2:56 PM EST

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.

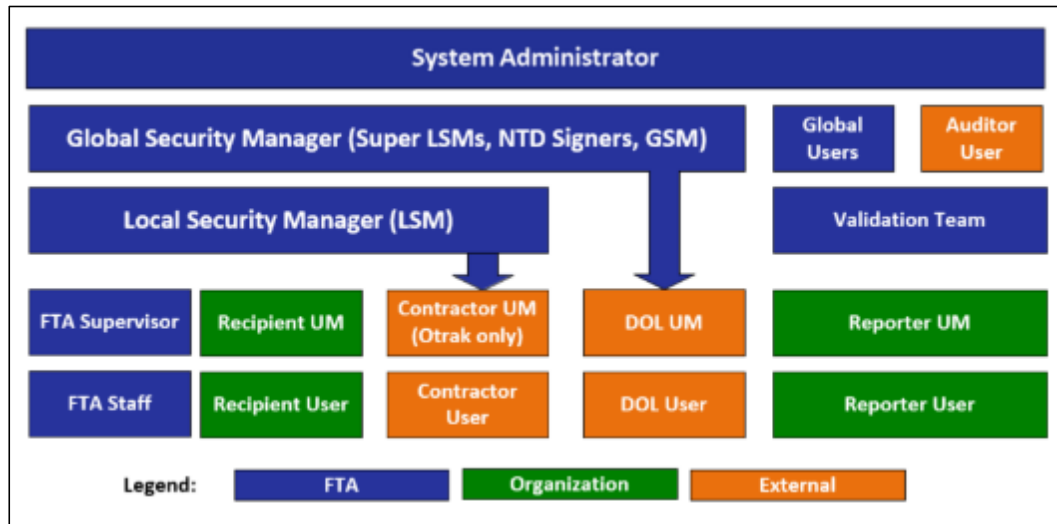
4.2 User Roles

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

Figure 2 – User Role Outline



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.

Table 1 – Organization User Roles
(continues to through page 20)

	Organization User Roles	FTA User Roles	External User Roles
NTD Reporters	<ol style="list-style-type: none"> 1) User Manager 2) CEO 3) NTD Contact 4) Editor 5) Viewer 6) Safety Contact 7) Safety Editor 8) Safety Viewer 9) CEO Delegate 	Global Roles <ol style="list-style-type: none"> 1) Global Security Manager (GSM) 2) Global Viewer 3) FTA Signers 4) FTA Viewer Validation Team <ol style="list-style-type: none"> 1) Validation Analyst 2) Validation Ops 3) Validation PM 4) Validation QA 	<ol style="list-style-type: none"> 1) Auditor

	Organization User Roles	FTA User Roles	External User Roles
TrAMS Recipients	1) Read Only 2) User Manager 3) Submitter 4) Developer 5) Official 6) Attorney 7) Civil Rights 8) FFR Reporter 9) MPR Reporter 10) JPC Procurement Officer	Global Roles Global Security Manager (GSM) Global Viewer Standard Regional Staff Roles 1) Supervisor 2) Local Security Manager (LSM) 3) Intake Manager 4) Pre-Award Manager 5) Post-Award Manager 6) Reservationist 7) Administrator 8) Director 9) Director of Operations 10) Initial Reviewer 11) Technical Reviewer 12) Environmental Reviewer 13) Civil Right Officer 14) Legal Counsel 15) Read-Only Specialized HQ Roles 1) Apportionment Manager 2) Budget Analyst 3) Budget Director 4) Dataset Administrator 5) DBE Approver 6) Discretionary Admin 7) Discretionary Manager 8) TCA Record 9) Transit Director 10) Vendor Setup	1) Auditor 2) DOL User 3) Contractor

	Organization User Roles	FTA User Roles	External User Roles
DGS		1) Program Manager 2) Team Lead 3) Reviewer 4) Global Security Manager 5) Local Security Manager 6) Administrator 7) Management	1) Auditor 2) FTA Contractor (DOT User)
SSOR	1) User Manager 2) Alternate Reporter 3) Primary Reporter 4) Viewer	Global Roles 1) Global Security Manager (GSM) 2) SSOR Viewer Standard Regional Staff Roles 3) Local Security Managers (LSM) 4) Validation Team Member 5) Validation Lead 6) Director 7) Regional Safety Officer	
CRM		Global Roles 1) Global Security Manager (GSM) 2) FTA Staff 3) CRM Global Viewer	

	Organization User Roles	FTA User Roles	External User Roles
OTRAK	Recipient 1) User 2) Approver 3) Manager 4) Submitter	1) Administrator 2) Program Administrator Global Users 3) Global Security Manager (GSM) 4) Global Viewer FTA Staff 5) Local Security Manager (LSM) HQ Staff 6) HQ User 7) Single Audit HQ Program Manager (PM) 8) TR PM 9) SMR PM 10) FMO PM 11) PSR PM 12) TCR PM 13) OAT PM 14) SSO Audit PM 15) Tribal Transit PM 16) Civil Rights Officer Region 17) Region User 18) Read-only 19) Regional Oversight Director 20) Single Audit Regional 21) Regional Tribal Liaison	1) OIG Auditor (Read-only) Contractor 2) Reviewer 3) PM 4) Delegate 5) User Manager 6) Regional Delegate
COVID-19	1) CEO 2) NTD Contact 3) Editor 4) Viewer 5) Safety Contact 6) Safety Editor 7) Safety Viewer 8) CEO Delegate		

4.3 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.

Table 2 summarizes these rules from the perspective of the logged-in users type:

Table 2 – User Record Viewing Privileges

My User Type	User Records I Can View		
	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).

4.4 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:

- 4.4.1 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).

Records / Users
Cook, Dale (dale.cook@dot.gov)

Summary **User Details** User Roles History News Related Actions

Account Information

User Type: FTA	Status: Active
Created On: 2/26/2018	Last Login Date:
Username: dale.cook@dot.gov	Title:
First Name: Dale	Honorific: Mr.
Middle Name:	Company Name:
Last Name: Cook	System: TrAMS, NTD

Contact Information

Email: sunnie162018@gmail.com	Fax Number:
Phone Number: (123) 123-1333	Phone Ext:
Address 1: 1372 East Main Street	Zip Code: 14609
Address 2:	Zip Ext:
City: Rochester	PO Box:
State: NY	

- 4.4.2 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**.

Records / Users
Global Security Manager GSM, TrAMS (sunnie.supergsmuser@mailinator.com)

Summary User Details **User Roles** History News Related Actions

Roles

Role	Role Category	System	Access Control Group	Cost Center	Organization	Document	Status
Global Security Manager (GSM)	Global Users	NTD	N/A	N/A	N/A	N/A	Approved
Global Security Manager (GSM)	Global Users	TrAMS	N/A	N/A	N/A	N/A	Approved
Global Security Manager (GSM)	Global Users	OTIS	N/A	N/A	N/A	N/A	Approved
Global Security Manager (GSM)	Global Users	DCS	N/A	N/A	N/A	N/A	Approved
Global Security Manager (GSM)	Global Users	SSOR	N/A	N/A	N/A	N/A	Approved

5 Items

- 4.4.3 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.



Summary User Details User Roles **History** News Related Actions

System *Select a System* Access Control Group *Select a Group*

Role Category *Select a Role Category* Cost Center *Select a Cost Center*

Role *Select a Role* Organization *Select an Organization*

Status *Select a Status* [CLEAR FILTER\(S\)](#)

Role History

Role	Role Category	System	Access Control Group	Organization	Status	Comments	Change By	Date
Recipient Submitter	Recipient	OTrak	OTrak Region 1	1330 - Capitol Region Council Of Governments (CRCOG)	Approved		arya.fosum@mailinator.com	1/13/2021
User Manager	Recipient	OTrak	OTrak Region 1	1330 - Capitol Region Council Of Governments (CRCOG)	Approved		fta.david.schilling@mailinator.com	1/12/2021
User Manager	Recipient	OTrak	OTrak Region 1	1330 - Capitol Region Council Of Governments (CRCOG)	Deleted		arya.fosum@mailinator.com	1/12/2021
Recipient Approver	Recipient	OTrak	OTrak Region 1	1330 - Capitol Region Council Of Governments (CRCOG)	Approved		arya.fosum@mailinator.com	1/12/2021
User Manager	Recipient	OTrak	OTrak Region 1	1330 - Capitol Region Council Of Governments (CRCOG)	Requested		arya.fosum@mailinator.com	1/12/2021

< 1 - 5 of 82 >

Certification History

Role	Role Category	System	Organization	Comments	Change By	Date	Projected Recertification Date
Recipient Submitter	Recipient	OTrak	1330 - Capitol Region Council Of Governments (CRCOG)		arya.fosum@mailinator.com	1/13/2021 7:29 AM EST	12/25/2021

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

Records / Users

Cook, Dale (dale.cook@dot.gov)

Summary User Details User Roles History **News** Related Actions

No entries available.

4.4.5 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**.

Records / Users

Attorney, Testing (testing.attorney@mailinator.com)

Summary User Details User Roles History News **Related Actions**

- Edit Profile**
Edit Profile
- Manage User Roles**
Add or Delete user roles
- Deactivate User**
Deactivate User Account
- Reset PIN**
This will reset the user's PIN

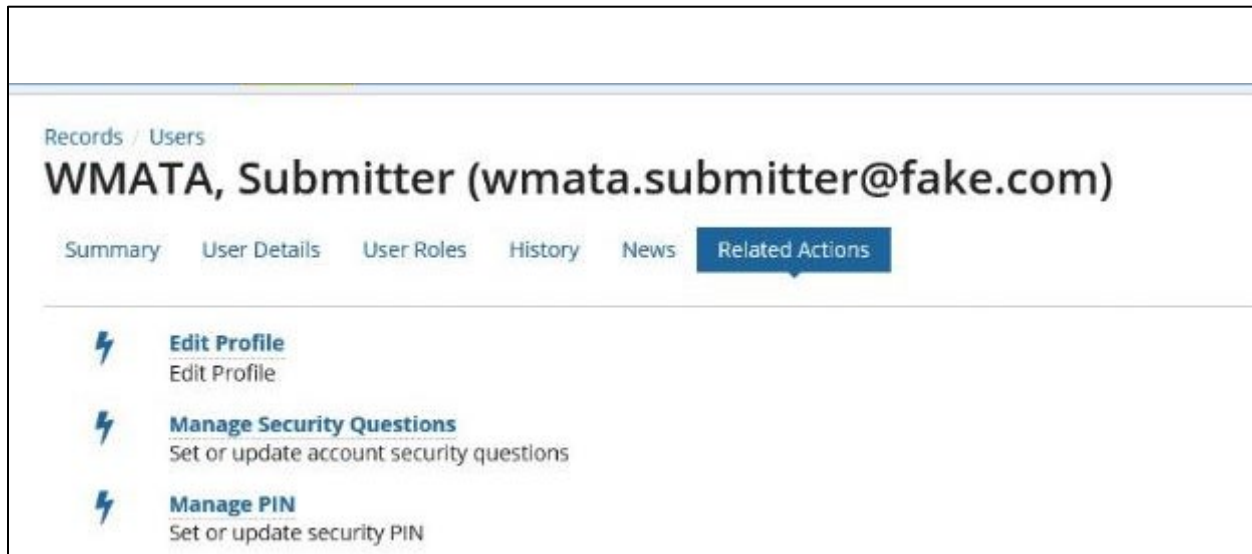
For detailed information about these user record pages, please reference [Section 6.4](#).



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**.

Records / Users
Transit-Rider, Sophia (transit.user@fake.com)

Summary User Details User Roles History News **Related Actions**

- Edit Profile**
Edit Profile
- Manage Security Questions
Set or update account security questions
- Manage PIN
Set or update security PIN

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

Records / Users
Transit-Rider, Sophia (transit.user@fake.com)

Summary User Details User Roles History News **Related Actions**

Edit User Profile

Basic Information

Username* transit.user@fake.com	Title* Analyst
First Name* Sophia	Honorific* Ms.
Middle Name A	Company Name Local Transit Agency
Last Name* Transit-Rider	Department FINANCES

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



First Name * <input type="text" value="Sophia"/>	Honorable * <input type="text" value="Ms."/>
Middle Name <input type="text" value="A"/>	Company Name <input type="text" value="Local Transit Agency"/>
Last Name * <input type="text" value="Transit Rider"/>	Department <input type="text" value="Finance"/>
Contact Information	
Email @ <input type="text" value="acs.usr.1@gmail.com"/>	Fax Number <input type="text"/>
Phone Number * <input type="text" value="(123) 123-1234"/>	Phone Ext <input type="text"/>
Address 1 * <input type="text" value="101 Transit Way"/>	Zip Code * <input type="text" value="12345"/>
Address 2 <input type="text"/>	Zip Ext <input type="text"/>
City * <input type="text" value="Transville"/>	PO Box <input type="text"/>
State * <input type="text" value="DC"/>	
<input type="button" value="CANCEL"/>	<input type="button" value="SAVE"/>

- 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 in order to save any other updates.

First Name * <input type="text" value="Sophia"/>	Honorable * <input type="text" value="Ms."/>
Middle Name <input type="text" value="A"/>	Company Name <input type="text" value="Local Transit Agency"/>
Last Name * <input type="text" value="Transit Rider"/>	Department <input type="text" value="Finance"/>
Contact Information	
Email @ <input type="text" value="acs.usr.1@gmail.com"/>	Fax Number <input type="text"/>
Phone Number * <input type="text" value="(123) 123-1234"/>	Phone Ext <input type="text"/>
Address 1 * <input type="text" value="101 Transit Way"/>	Zip Code * <input type="text" value="12345"/>
Address 2 <input type="text"/>	Zip Ext <input type="text"/>
City * <input type="text" value="Transville"/>	PO Box <input type="text"/>
State * <input type="text" value="DC"/>	
<input type="button" value="CANCEL"/>	<input type="button" value="SAVE"/>

- 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**:

- All users can set up and manage three (3) security questions through the **Manage Security Questions** page.
- Questions must be selected from an FTA approved list and 3 distinct questions must be selected.
- Answers must contain at least three (3) characters and cannot be used for more than one question.
- Users must correctly answer their existing questions to change them.
- Users have three (3) attempts within a calendar day to answer their security questions correctly before they are locked out of the action.
- Users cannot see the **Manage Security Questions** page on any other user's account.
- Users will receive an automated email notification any time their questions have been updated.

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

- Locate the **User Profile** through either the **User Settings** page or the **Manage Users** page.
- Select **Related Actions**
- Click **Manage Security Questions**
- 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 for 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.

Recent Users
Transit-Rider, Sophia (transit.user@fake.com)

Summary User Details User Roles History News **Related Actions**

- Edit Profile
Edit Profile
- Manage Security Questions**
Set or update account security questions
- Manage PIN
Set or update Security PIN

- 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.

Summary User Details User Roles History News **Related Actions**

Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24-hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What was the name of your first pet?
Answer *

Question 2
What was the make of your first car?
Answer *

Question 3
What is your favorite sports team?
Answer *

CANCEL **SUBMIT**

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



Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What was the name of your first pet?

Answer *

Fido

Question 2
What was the make of your first car?

Answer *

Chevy

Question 3
What is your favorite sports team?

Answer *

Red

[CANCEL](#) [SUBMIT](#)

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

[Summary](#) [User Details](#) [User Roles](#) [History](#) [News](#) [Related Actions](#)

Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What was the name of your first pet?

Answer *

Question 2
What was the make of your first car?

Answer *

Question 3
What is your favorite sports team?

Answer *

One or more of your security question answers is incorrect. You have 2 attempt(s) remaining.

[CANCEL](#) [SUBMIT](#)

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



Summary User Details User Roles History News **Related Actions**

Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24-hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What was the name of your first pet?

Answer *

Question 2
What was the make of your first car?

Answer *

Question 3
What is your favorite sports team?

Answer *

One or more of your security question answers is incorrect. You have 2 attempt(s) remaining.

CANCEL **SUBMIT**

- 8) The **Related Actions** page is again displayed.
- 9) If the information entered has been corrected for each question, click **Submit** once more.

Summary User Details User Roles History News **Related Actions**

Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24-hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What was the name of your first pet?

Answer *

Flido

Question 2
What was the make of your first car?

Answer *

Chrysler

Question 3
What is your favorite sports team?

Answer *

Red

CANCEL **SUBMIT**

- 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.



Summary User Details User Roles History News **Related Actions**

Manage Security Questions

Select and answer three (3) security questions. These questions can be used for authentication to unlock your account. Please note that your answers are not case sensitive.

Question 1 *
What was the name of your first pet? ▾

Answer * Retype Answer *

Question 2 *
What was the make of your first car? ▾

Answer * Retype Answer *

Question 3 *
What is your favorite sports team? ▾

Answer * Retype Answer *

CANCEL **SUBMIT**

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

Summary User Details User Roles History News **Related Actions**

Manage Security Questions

Select and answer three (3) security questions. These questions can be used for authentication to unlock your account. Please note that your answers are not case sensitive.

Question 1 *
What was the name of your first pet? ▾

Answer * Retype Answer *

Question 2 *
What was the make of your first car? ▾

Answer * Retype Answer *

Question 3 *
What is your favorite sports team? ▾

Answer * Retype Answer *

CANCEL **SUBMIT**



- 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.*

Summary User Details User Roles History News **Related Actions**

Manage Security Questions

Select and answer three(3) security questions. These questions can be used for authentic button to unlock your account. Please note that your answers are not case sensitive.

Question 1 *
What is your favorite sports team? ▼

Answer * **Retype Answer ***

Question 2 *
What was the make of your first car? ▼

Answer * **Retype Answer ***

Question 3 *
What is your favorite sports team? ▼

Answer * **Retype Answer ***

You can't pick the same question twice.

CANCEL **SUBMIT**



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

Note: *Only the first question was changed.*

Manage Security Questions

Select and answer three (3) security questions. These questions can be used for authentication to unlock your account. Please note that your answers are not case sensitive.

Question 1 *

---Please Select a Question---

Answer *

Retype Answer *

Question 2 *

---Please Select a Question---

Answer *

Retype Answer *

Question 3 *

---Please Select a Question---

Answer *

Retype Answer *

CANCEL

SUBMIT

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 are required to have 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:

- 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.
- No user can see the **Manage PIN** profile **Related Action** on any other user's account.
- PINs must be 4-digit numeric codes (e.g., "1234").
- To reset a PIN, a user must correctly enter their current PIN or correctly answer their Security Questions.
- 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**.

The screenshot shows the 'Related Actions' tab selected in the top navigation bar. Below the tab, there are three action items, each with a lightning bolt icon: 'Edit Profile' (Edit Profile), 'Manage Security Questions' (Set or update account security questions), and 'Manage PIN' (Set or update security PIN). The 'Manage PIN' item is highlighted with a red rectangular box.

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

The screenshot shows the 'Manage PIN' form. At the top, the 'Related Actions' tab is selected. The form has a title 'Manage PIN' and a section 'User Information' with fields for Full Name (Ms. Arya OrgUm), Username (arya.orgum@mailinator.com), Title (um), Status (Active), and User Type (Organization). Below this is a section 'My PIN Roles' with a single role: 'Official, 78100 - TRO-1 - Region 1, 1334 - Transportation, Connecticut Department Of (CONNDOT)'. The 'Set PIN' section is highlighted with a red rectangular box. It contains two required fields: 'Enter New PIN *' and 'Re-enter New PIN *', both with four asterisks indicating a four-digit PIN. At the bottom of the form are 'CANCEL' and 'SUBMIT' buttons.

- 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

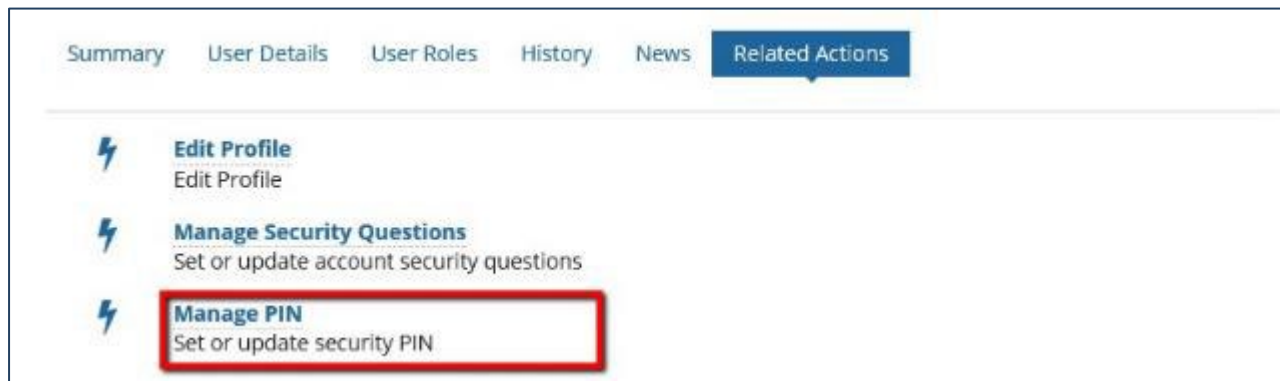
Once the PIN has been created, a user may again select the **Manage PIN** function from the **Related Action** page to change or re-set their personal four-digit PIN code.

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, containing **User Information** as well as the roles to which the PIN has been applied.



[Summary](#)
[User Details](#)
[User Roles](#)
[History](#)
[News](#)
[Related Actions](#)

Manage PIN

User Information

Full Name	Ms. Arya OrgUm	Username	arya.orgum@mailinator.com
Title	um	Status	Active
User Type	Organization		

My PIN Roles

Official, 78100 - TRO-1 - Region 1, 1334 - Transportation, Connecticut Department Of (CONNDOT)
--

Verify Identity

In order to set a new PIN, you must verify your identity by entering your current PIN or by correctly answering your security questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten your current PIN or the answers to your security questions, please contact the Help Desk.

☒ Enter Current PIN
☐ Answer Existing Security Questions

There are no security questions associated with your account.

Current PIN *

CANCEL

SUBMIT

- 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.

[Summary](#)
[User Details](#)
[User Roles](#)
[History](#)
[News](#)
[Related Actions](#)

Manage PIN

User Information

Full Name	Ms. Arya OrgUm	Username	arya.orgum@mailinator.com
Title	um	Status	Active
User Type	Organization		

My PIN Roles

Official, 78100 - TRO-1 - Region 1, 1334 - Transportation, Connecticut Department Of (CONNDOT)
--

Verify Identity

In order to set a new PIN, you must verify your identity by entering your current PIN or by correctly answering your security questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten your current PIN or the answers to your security questions, please contact the Help Desk.

☒ Enter Current PIN
☐ Answer Existing Security Questions

Current PIN *

CANCEL

SUBMIT

- 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.



Verify Identity

In order to set a new PIN, you must verify your identity by entering your current PIN or by correctly answering your security questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten your current PIN or the answers to your security questions, please contact the Help Desk.

☐ Enter Current PIN

☒ Answer Existing Security Questions

Question 1
What was the name of your first pet?

Answer *

Question 2
What was the color of your first car?

Answer *

Question 3
In what city did your parents meet?

Answer *

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

Verify Identity

In order to set a new PIN, you must verify your identity by entering your current PIN or by correctly answering your security questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten your current PIN or the answers to your security questions, please contact the Help Desk.

☐ Enter Current PIN

☒ Answer Existing Security Questions

Question 1
What was the name of your first pet?

Answer *

Cici

Question 2
What was the color of your first car?

Answer *

Blue

Question 3
In what city did your parents meet?

Answer *

New York

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



Verify Identity

In order to set a new PIN, you must verify your identity by entering your current PIN or by correctly answering your security questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten your current PIN or the answers to your security questions, please contact the Help Desk.

☐ Enter Current PIN
☒ Answer Existing Security Questions

Question 1
What was the name of your first pet?

Answer *

Question 2
What was the color of your first car?

Answer *

Question 3
In what city did your parents meet?

Answer *

- 7) After entering all of 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).

Summary User Details User Roles History News **Related Actions**

Manage PIN

User Information

Full Name	Ms. Arya OrgUm	Username	arya.orgum@mailinator.com
Title	um	Status	Active
User Type	Organization		

My PIN Roles

Official, 78100 - TRO-1 - Region 1, 1334 - Transportation, Connecticut Department Of (CONNDOT)

Update PIN

Enter New PIN *

Re-enter New PIN *

- 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*.



Summary User Details User Roles History News **Related Actions**

Manage PIN

User Information

Full Name	Ms. Arya OrgUm	Username	arya.orgum@mailinator.com
Title	um	Status	Active
User Type	Organization		

My PIN Roles

Official, 78100 - TRO-1 - Region 1, 1334 - Transportation, Connecticut Department Of (CONNDOT)

Update PIN

PIN must be a 4-digit numeric code.

Enter New PIN *

.....

Re-enter New PIN *

CANCEL

SUBMIT

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

Manage PIN

User Information

Full Name	Ms. Arya OrgUm	Username	arya.orgum@mailinator.com
Title	um	Status	Active
User Type	Organization		

My PIN Roles

Official, 78100 - TRO-1 - Region 1, 1334 - Transportation, Connecticut Department Of (CONNDOT)

Update PIN

Enter New PIN *

....

Re-enter New PIN *

....

CANCEL

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.*



5.2A 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 unlocking 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.

5.2.1 Answer Security Questions

If the account is locked and security questions were previously set up, the user can attempt to unlock the account by answer 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**.



Home

Welcome to the Transit Integrated Appian Platform!

Current user: Alam, Sunjida
Last Login Date: 10/6/2020 9:56 AM EDT

Unlock My Account
Unlock Account or Submit Unlock Request

Your Account has been locked. Please click on "Unlock My Account" to unlock your account.

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

Home

Unlock Account
Please select an available option to unlock account.

Options*

☐ Send a request to unlock your account

☒ Answer security questions

CANCEL SUBMIT

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

Note:	Answers are case insensitive.
--------------	-------------------------------

Home

Answer Existing Security Questions
You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What is your favorite sports team?
Answer *

Question 2
What was the color of your first car?
Answer *

Question 3
In what city did your parents meet?
Answer *

CANCEL SUBMIT

- 5) If incorrect information was entered, a validation error message will display that indicates the number of attempts remaining for the current calendar day. 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.



Home

Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What is your favorite sports team?

Answer *

Question 2
What was the color of your first car?

Answer *

Question 3
In what city did your parents meet?

Answer *

One or more of your security question answers is incorrect. You have 1 attempt(s) remaining.

CANCEL SUBMIT

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

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

Answer Existing Security Questions

You already have security questions set up. If you would like to change your questions or answers, you must first correctly answer your existing questions. You have 3 attempts within a 24 hour window to verify your identity. If you have forgotten the answers to your security questions, please contact the Help Desk.

Question 1
What is your favorite sports team?

Answer *

Question 2
What was the color of your first car?

Answer *

Question 3
In what city did your parents meet?

Answer *

CANCEL SUBMIT

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

9) Click **Refresh**.

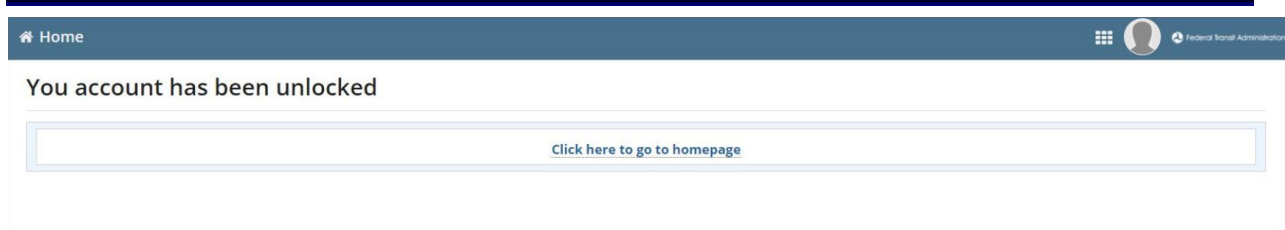
Home

Unlock In Progress

This may take a few minutes to complete. You may log out and return shortly, or click Refresh to check if the process is completed.

REFRESH

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



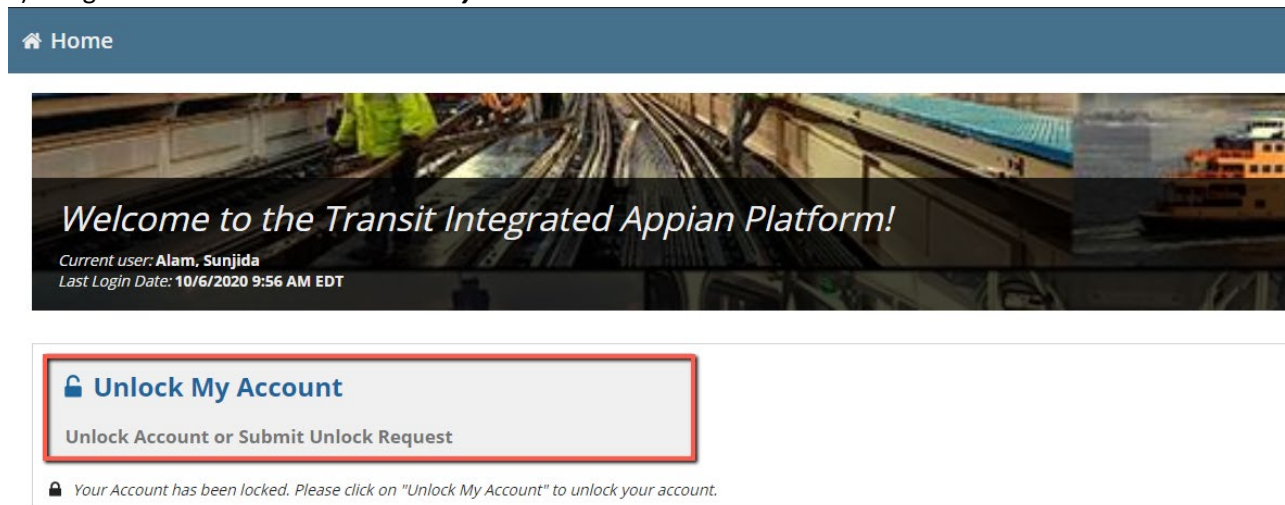
- 11) User can Click the link to return to Home page.
- 12) An email will be auto-generated and sent to the user.

5.2.2 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 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.



Home

Unlock Account

Please select an available option to unlock account.

Options *

☒ Send a request to unlock your account

☐ Answer security questions

Comment

Enter comment to unlock your account

CANCEL

SUBMIT

- 3) A message indicating **Unlock Request Successfully Submitted** will display.
- 4) Click **Close**.

Home

Unlock Request Successfully Submitted

A request to unlock your account was successfully submitted to your User Manager(s) or Local Security Manager(s).

CLOSE

- 5) The request for the account 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.

Action Cannot Be Completed

You cannot access this action at this time. You have already submitted an unlock request and have reached the maximum number of attempts to unlock your account using your security questions. If more than 48 hours has passed since your request was submitted, please reach out to one of your managers displayed below.

Click to Show Managers

CANCEL



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

Action Cannot Be Completed

You cannot access this action at this time. You have already submitted an unlock request and have reached the maximum number of attempts to unlock your account using your security questions. If more than 48 hours has passed since your request was submitted, please reach out to one of your managers displayed below.

Managers for Primary Reporter

Show all 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@mailinator.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.

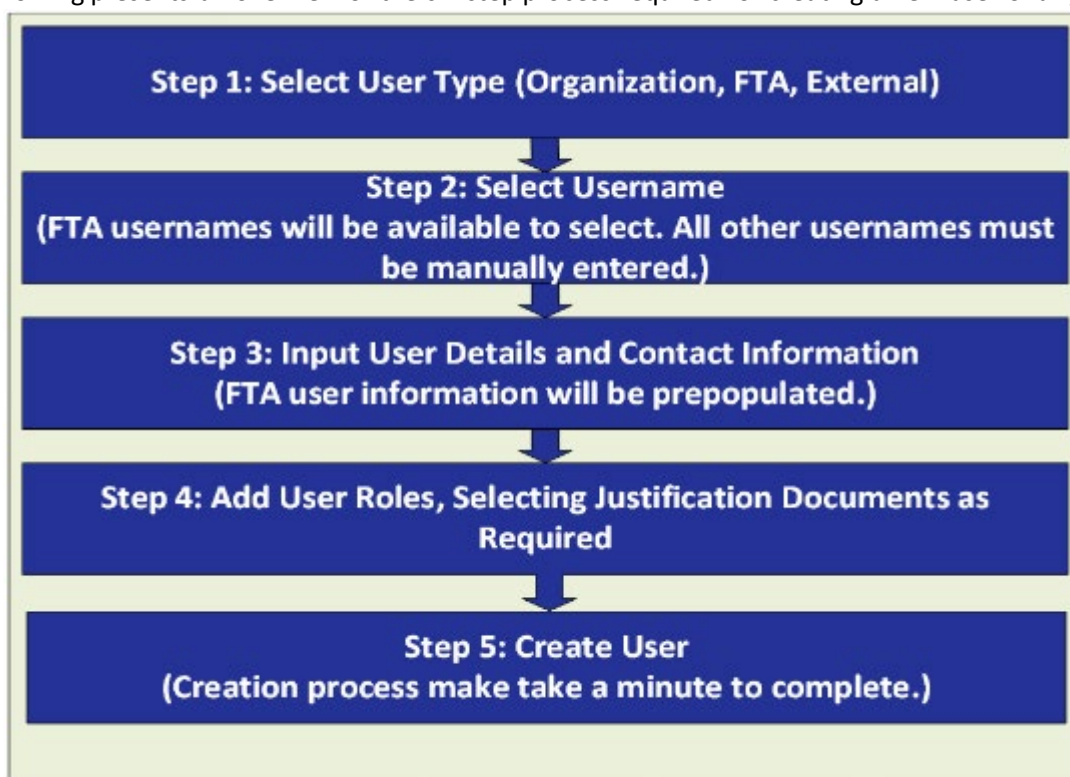


The remainder of this section presents an overview of each of the user management activities and responsibilities.

Note:	<i>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.</i>
--------------	--

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.



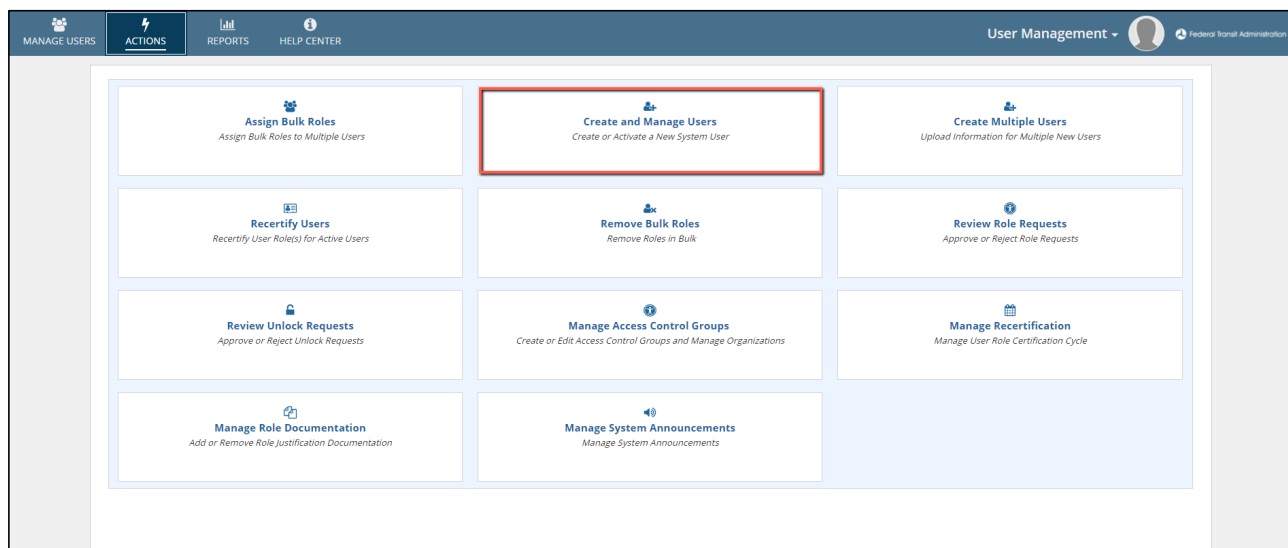
- 7) A user's username must be a valid email address.
- 8) Name, contact, and business address information is required when creating a new user.
- 9) A user cannot be created unless at least one role is assigned to the user.
- 10) Some roles require justification documents and/or approval by users with 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:

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



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

Create and Manage Users

User Type *

☐ FTA Staff
☐ Organization User (e.g. Recipient, Reporter)
☐ External User (e.g. DOL, DOT Reviewer, Auditor, Contractors)



- 5) The first information about a user required is their username, based on a valid email address. **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 cannot be changed after creation. Validation checks will confirm uniqueness before moving to the next step

Create and Manage Users

Username

The username must be an email address.

- 6) Enter an email address and tab forward.
7) If the email is rejected as invalid, the page will display an error message.

Create and Manage Users

Username

The username must be an email address.

Username must be a valid email address. Emails can contain only lowercase letters, numbers, and periods. Emails must contain an @ followed by at least one period (.).

- 8) 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.

Create and Manage Users

Username

The username must be an email address.

You are about to cancel the Create User process. No data will be saved. Are you sure you want to exit?

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



Create and Manage Users

Username

userx@mailinator.com

The username must be an email address.

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

Create and Manage Users

Basic Information

Username *
userx@mailinator.com ←

First Name *

Middle Name

Last Name *

Title *

Honorific *
Honorific ▼

Company Name

Department

Contact Information

Email *
userx@mailinator.com ←

Phone Number *
(555) 555-5555

Address 1 *

Address 2

Fax Number

Phone Ext

Zip Code *

Zip Ext

11) Enter the Basic Information for the following fields:

- The username just entered displays in the *Username* field but cannot be changed.
- Enter the user's first name in the *First Name* field (35-character limit). This is a required field.
- Enter the user's middle name in the *Middle Name* field (35-character limit).
- 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.

12) 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- c h a r a c t e r limit).
- c) Enter the user's business phone number extension in the *Phone Number Extension* field (10- c h a r a c t e r limit).
- d) Enter the user's business fax number in the *Fax Number* field (20-character limit).
- e) Enter the first line of the user's business address in the *Address 1* field (60-character limit).
- f) Enter the second line of the user's business address in the *Address 2* field (60-character limit).
- g) Enter the city for the user's business address in the *City* field (60-character limit; no numeric).
- h) Select the state for the user's business address from the dropdown menu provided under the *State* field.
- i) Enter the ZIP Code for the user's business address in the *ZIP Code* field (5-character limit).
- j) Enter the ZIP Code Extension for the user's business address in the *ZIP Code Extension* field (4- c h a r a c t e r limit).
- k) If necessary, enter the associated Post Office Box in the *PO Box* field (35-character limit).

Note:	<i>PO Box is limited to numeric values and cannot contain alphabetical characters.</i>
--------------	--

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



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

Manage User Roles

User Information

Full Name

 TrAMS Global Viewer

Username

 aana.globalviewer@dot.gov

Title

 Test User

Status

 Active

User Type

 FTA

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	OTrak	Region	Local Security Manager (LSM)	OTrak Region 2	-	78100 - Region 1 (TRO-1)	N/A	Approved				
2	TrAMS	FTA Staff	Local Security Manager (LSM)	Region 2	-	61000 - Office of the Administrator (TOA)	N/A	Approved				
3	TrAMS	FTA Staff	Director	Office of Administration	-	62000 - Office of Administration (TAD)	N/A	Approved	adding new role 8/16			

+ ADD NEW ROLE

CANCEL

VIEW HISTORY

SUBMIT

- 14) The role filters (System, Role Category, 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.
- 15) Click the checkbox next to the role to select a role for the user. Only one (1) role can be selected at a time. In the screenshot below, only roles available to TrAMS Recipients are listed. These roles will be granted only for the Organization that is listed. Once the role is selected, then click **Submit**.



Manage User Roles

User Information

Full Name TrAMS Global Viewer

Title Test User

User Type FTA

Username aana.globalviewer@dot.gov

Status Active

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	OTrak	Region	Local Security Manager (LSM)	OTrak Region 2	-	78100 - Region 1 (TRO-1)	N/A	Approved				
2	TrAMS	FTA Staff	Local Security Manager (LSM)	Region 2	-	61000 - Office of the Administrator (TOA)	N/A	Approved				
3	TrAMS	FTA Staff	Director	Office of Administration	-	62000 - Office of Administration (TAD)	N/A	Approved	adding new role 8/16			
4	FACES	Global Users	User Details Report Global Viewer				Select Existing Upload	Approved				

+ ADD NEW ROLE

CANCEL

VIEW HISTORY

SUBMIT



16) The **Manage Roles** page will display with the updated user role(s) assigned.

Manage Roles

User Information

Full Name: Ms. Sophia A. Transit-Rider
Username: transit.user@fake.com
Title: Analyst
Status: No Record
User Type: Organization

ADD DELETE DOCUMENTATION

User Roles

<input type="checkbox"/>	Role	Role Category	System	Cost Center	Organization	Document	Status
<input type="checkbox"/>	Developer	Recipient	TrAMS	78300 - Region 3	9123 - On Time Transit Company (OTTC)	N/A	Approved

BACK CREATE

17) If the role requires a justification or delegation of authority document, 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.

1	OTrak	FTA Staff	Local Security Manager (LSM)	OTrak Region 10	-	78900 - Region 9 (TRO-9)	N/A	Approved	test			
2	TrAMS	Global Users	Global Security Manager (GSM)				Select Existing Upload	Approved				

(#2) Add Document For Selected Role (Download the template)

System: TrAMS Cost Center: Organization: N/A

Document*

UPLOAD Drop file here

Description*

Document Name* 0/255

CANCEL **UPLOAD DOCUMENT** 0/4000



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

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	OTrak	Region	Local Security Manager (LSM)	OTrak Region 2	-	78100 - Region 1 (TRO-1)	N/A	Approved				
2	TrAMS	FTA Staff	Local Security Manager (LSM)	Region 2	-	61000 - Office of the Administrator (TOA)	N/A	Approved				
3	TrAMS	FTA Staff	Director	Office of Administration	-	62000 - Office of Administration (TAD)	N/A	Approved	adding new role 8/16			
4	FACES	Global Users	User Details Report Global Viewer				Justification	Approved				

+ ADD NEW ROLE

CANCEL

VIEW HISTORY **SUBMIT**

19) 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**.

User Creation In Progress

The user's data is being processed. It may take a few minutes for all changes to appear on the user's record. Click the 'Refresh' button after a minute to confirm that the user has been created. Click the 'Close' button to go back to the Actions tab.

CLOSE **REFRESH**

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

User Successfully Created

Login instructions have been sent to this user via email.

Username transit.user@fake.com	Title Analyst
First Name Sophia	Honorific MS.
Middle Name A	Company Name Local Transit Agency
Last Name Transit-Rider	System TrAMS

Click here to access the user's record.

CLOSE



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

User Successfully Created

Login instructions have been sent to this user via email.

Username	transit.user@fake.com	Title	Analyst
First Name	Sophia	Honorific	Ms.
Middle Name	A	Company Name	Local Transit Agency
Last Name	Transit-Rider	System	TRAMS

[Click here to access the user's record.](#)

CLOSE

22) The user will receive an automatic email alerting them of the account setup, similar to 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
<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.

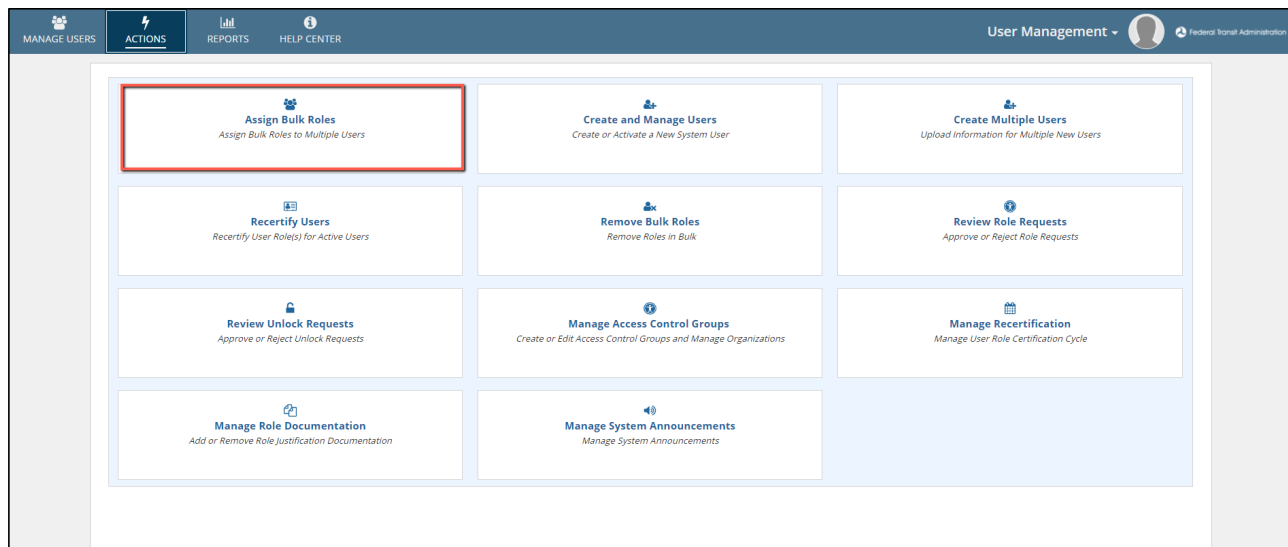


6.2.2 Action: Assign Bulk Roles

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 to 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 PROCEED.

Assign Bulk Roles

This action will affect System performance when submitted during business hours. Click proceed to continue.

PROCEED

* System TRAMS * Role Category Select a Role Category **RESET**

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of 300 roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
No items available									

+ ADD USER

CANCEL **NEXT**



- 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.

Assign Bulk Roles

* System
Select a System

* Role Category
Select a Role Category

RESET

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of 300 roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
No items available									

+ ADD USER

CANCEL

NEXT

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

Assign Bulk Roles

* System
TrAMS

* Role Category
Select a Role Category

RESET

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of 300 roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
<div> System Administrator Global Users FTA Staff Recipient OOL Contractors Auditors </div>									

+ ADD USER

CANCEL

NEXT

- 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.



Assign Bulk Roles

*System TrAMS *Role Category Recipient RESET

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of 300 roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
1	Select an active user	--- Select a Value ---	Select a Group			N/A			

+ ADD USER

CANCEL NEXT

- 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

Assign Bulk Roles

*System TrAMS *Role Category Recipient RESET

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of 300 roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
	Jon Test (test.user43@mailinator.c...)								
1	Jon Bon (test.filteruser1@mailinat...)	User Manager	Region 3	Select an Organization		N/A			

+ ADD USER

CANCEL NEXT

- 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.



Assign Bulk Roles

System TrAMS

Role Category Recipient

RESET

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of **300** roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
1	Jon Test (test.user43@mailinator.c...)								
	Jon Bon (test.filteruser1@mailinat...)	User Manager	Region 3	Select an Organization		N/A			

+ ADD USER

CANCEL

NEXT

- 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.

Assign Bulk Roles

System TrAMS

Role Category Recipient

RESET

Instructions: Users can be added by clicking on Add User below. Multiple users may be added as a group by typing the user name one after the other. To create another group, click on Add User again. When all users have been added to the grid, you may select a single role or multiple roles for each group of users. A maximum of **300** roles can be assigned.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
1	Jon Test (test.user43@mailinator.c...)								
	Jon Bon (test.filteruser1@mailinat...)	User Manager	Region 3	Select an Organization		N/A			

+ ADD USER

CANCEL

NEXT

- 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.

Confirm Bulk Role Assignment

System	Username	Role Category	Role	Access Control Group	Organization	Cost Center
TrAMS	for.contractor@dot.gov	Contractors	Contractor	Office of Budget and Policy	6031 - Quality Software Services, Inc.	62000 - Office of Administration
TrAMS	for.contractor@dot.gov	Contractors	Contractor	Region 7	1812 - Transportation, Iowa Dept Of	78700 - Region 7
TrAMS	adib.alam@mailinator.com	Contractors	Contractor	Office of Budget and Policy	6031 - Quality Software Services, Inc.	62000 - Office of Administration
TrAMS	adib.alam@mailinator.com	Contractors	Contractor	Region 7	1812 - Transportation, Iowa Dept Of	78700 - Region 7

BACK

SUBMIT



- 10) If necessary, 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.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
1	Analyst TestUser11 (state.analyst11) ✕	Global Security Manager (GSM) ▼	▼			Select Existing Upload			

(#1) Add Document For Selected Role (Download the template)

System: NTD Cost Center: Organization:

Document * Description *

Drop file here

Document Name * 0/255

- 11) If the role requires a justification or delegation of authority document, the **Add Document for Selected Role** 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.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
1	Analyst TestUser11 (state.analyst11) ✕	Global Security Manager (GSM) ▼	▼			Select Existing Upload			

(#1) Add Document For Selected Role (Download the template) ←

System: NTD Cost Center: Organization:

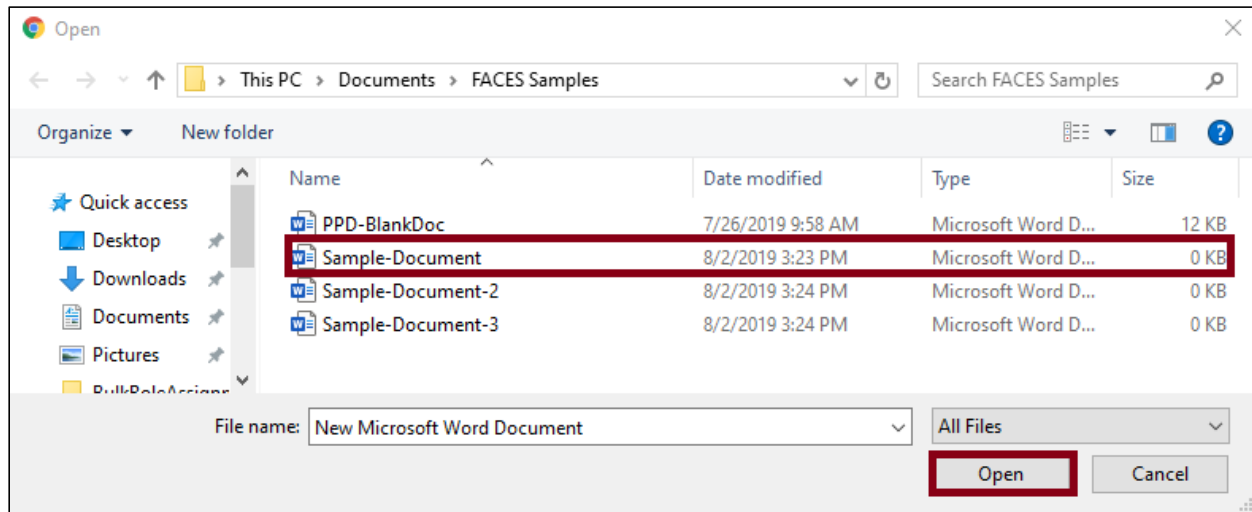
Document * Description *

Drop file here

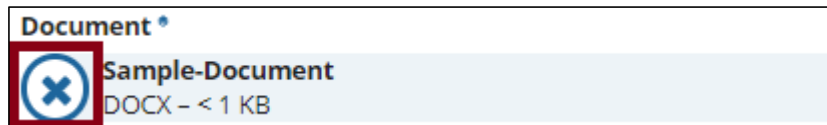
Document Name * 0/255



- 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.

#	User	Role	Access Control Group	Organization	Cost Center	Justification Document	Comments		
1	Analyst TestUser11 (state.analyst11) ✕	Global Security Manager (GSM) ▼	▼			Select Existing Upload			

(#1) Add Document For Selected Role (Download the template)

System: NTD Cost Center: Organization:

Document * Description *

UPLOAD Drop file here

Document Name * 0/255

CANCEL

0/4000

UPLOAD DOCUMENT

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

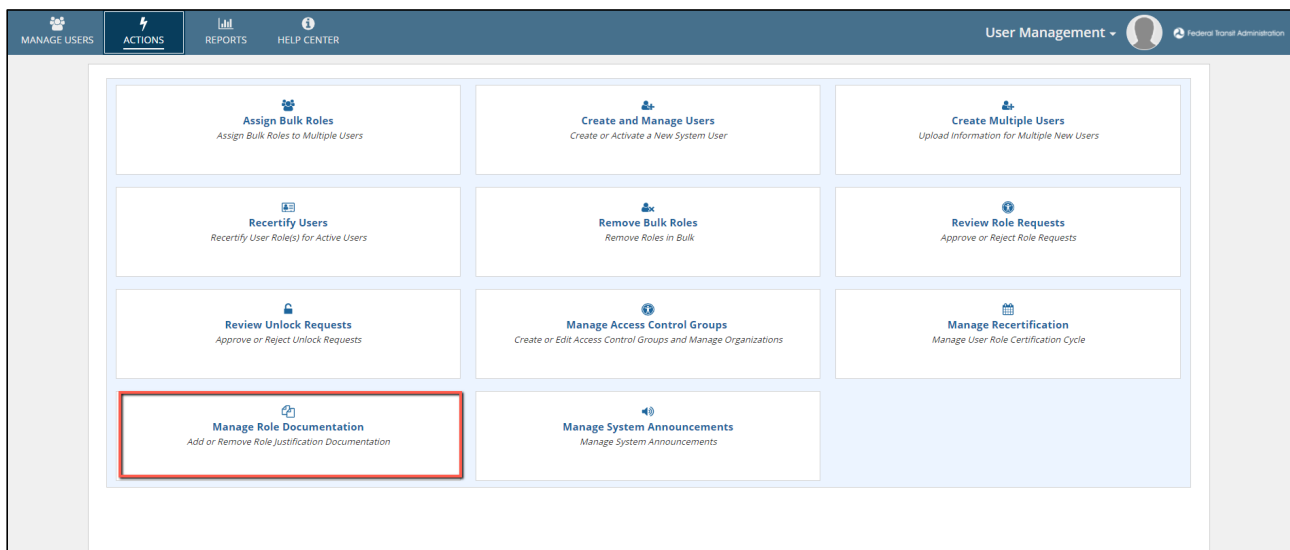


6.2.3 Action: Manage Role Documentation

Some roles require justification for their assignment to a specific user. The TrAMS **Submitter**, **Attorney**, and **Official** roles require a Delegation of Authority letter from the agency's CEO justifying the assignment of the role to the 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 showing 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).

Manage Role Documentation

System TrAMS

Access Control Group Region 3

Organization Select an Organization

Cost Center 78300 - Region 3

ADD DELETE

<input type="checkbox"/>	Document Name	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input type="checkbox"/>	Justification	Justification	Region 3	N/A	N/A	11/13/2020	faces.admin@test.com
<input type="checkbox"/>	Justification	Justification	Region 3	N/A	N/A	11/13/2020	faces.admin@test.com
<input type="checkbox"/>	Role Approval Doc	Test	Region 3	78300 - Region 3	1402 - Baltimore, City Of (BALTIMORE CITY)	5/1/2019	ahmed.khan
<input type="checkbox"/>	role change	doc	Region 3	78300 - Region 3	1396 - Transportation, Delaware Department Of (DELDOT)	2/4/2020	ahmed.khan
<input type="checkbox"/>	Sample	Sample	Region 3	78300 - Region 3	1401 - Transportation, Maryland Department Of (MTA)	1/8/2019	leslie.smith

CLOSE

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

Manage Role Documentation

System TrAMS

Access Control Group Region 3

Organization Select an Organization

Cost Center 78300 - Region 3

ADD DELETE

<input type="checkbox"/>	Document Name	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input type="checkbox"/>	Justification	Justification	Region 3	N/A	N/A	11/13/2020	faces.admin@test.com
<input type="checkbox"/>	Justification	Justification	Region 3	N/A	N/A	11/13/2020	faces.admin@test.com
<input type="checkbox"/>	Role Approval Doc	Test	Region 3	78300 - Region 3	1402 - Baltimore, City Of (BALTIMORE CITY)	5/1/2019	ahmed.khan
<input type="checkbox"/>	role change	doc	Region 3	78300 - Region 3	1396 - Transportation, Delaware Department Of (DELDOT)	2/4/2020	ahmed.khan
<input type="checkbox"/>	Sample	Sample	Region 3	78300 - Region 3	1401 - Transportation, Maryland Department Of (MTA)	1/8/2019	leslie.smith

CLOSE



- 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.

<input type="checkbox"/>	Document Name	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input checked="" type="checkbox"/>	Doc1	Fake Doc	TrAMS Region 2	78200 - Region 2	1414 - New Jersey Transit Corporation, The (NJTC)	11/5/2019	faces.sysadmin.bala@mailinator.com
<input type="checkbox"/>	test5	test5	TrAMS Region 2	78200 - Region 2	1924 - County Of Chemung (CHEMUNG CNT)	10/22/2019	Bruce.Hawkins12345
<input type="checkbox"/>	test6	test6	TrAMS Region 2	78200 - Region 2	1924 - County Of Chemung (CHEMUNG CNT)	10/22/2019	Bruce.Hawkins12345

<input checked="" type="checkbox"/>	Justified Roles	Justified Users
<input checked="" type="checkbox"/>	User Manager	peter t
		Sunnie tramsum

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

Manage Role Documentation

System: TrAMS Organization: Select an Organization

Access Control Group: TrAMS Region 2 Cost Center: 78200 - Region 2

ADD DELETE

<input type="checkbox"/>	Document Name	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input type="checkbox"/>	Doc1	Fake Doc	TrAMS Region 2	78200 - Region 2	1414 - New Jersey Transit Corporation, The (NJTC)	11/5/2019	faces.sysadmin.bala@mailinator.com
<input type="checkbox"/>	test5	test5	TrAMS Region 2	78200 - Region 2	1924 - County Of Chemung (CHEMUNG CNT)	10/22/2019	Bruce.Hawkins12345
<input type="checkbox"/>	test6	test6	TrAMS Region 2	78200 - Region 2	1924 - County Of Chemung (CHEMUNG CNT)	10/22/2019	Bruce.Hawkins12345

CLOSE



- 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.

<input type="checkbox"/>	1	1	Darlynn Smit (NTD Validation Analyst)	78100 - Region 1	10098 - Western Maine Transportation Services, Inc. (WMTS)	9/1/2020	faces.sysadmin.bala@mailinator.com
<input type="checkbox"/>	1	1	Office of the Administrator	62000 - Office of Administration	6522 - Personnel Management, U S Office Of (OPM)	3/23/2020	faces.sysadmin.bala@mailinator.com

« < 1 - 5 of 879 > »

Add Document (Download the template)

System *

Select a System

Access Control Group

Select a Group

Organization

Document *

Drop file here

Document Name *

0/255

Description *

0/4000

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

<input type="checkbox"/>	1	1	Darlynn Smit (NTD Validation Analyst)	78100 - Region 1	10098 - Western Maine Transportation Services, Inc. (WMTS)	9/1/2020	faces.sysadmin.bala@mailinator.com
<input type="checkbox"/>	1	1	Office of the Administrator	62000 - Office of Administration	6522 - Personnel Management, U S Office Of (OPM)	3/23/2020	faces.sysadmin.bala@mailinator.com

« < 1 - 5 of 879 > »

Add Document (Download the template)

System *

Select a System

Access Control Group

Select a Group

Organization

Document *

Drop file here

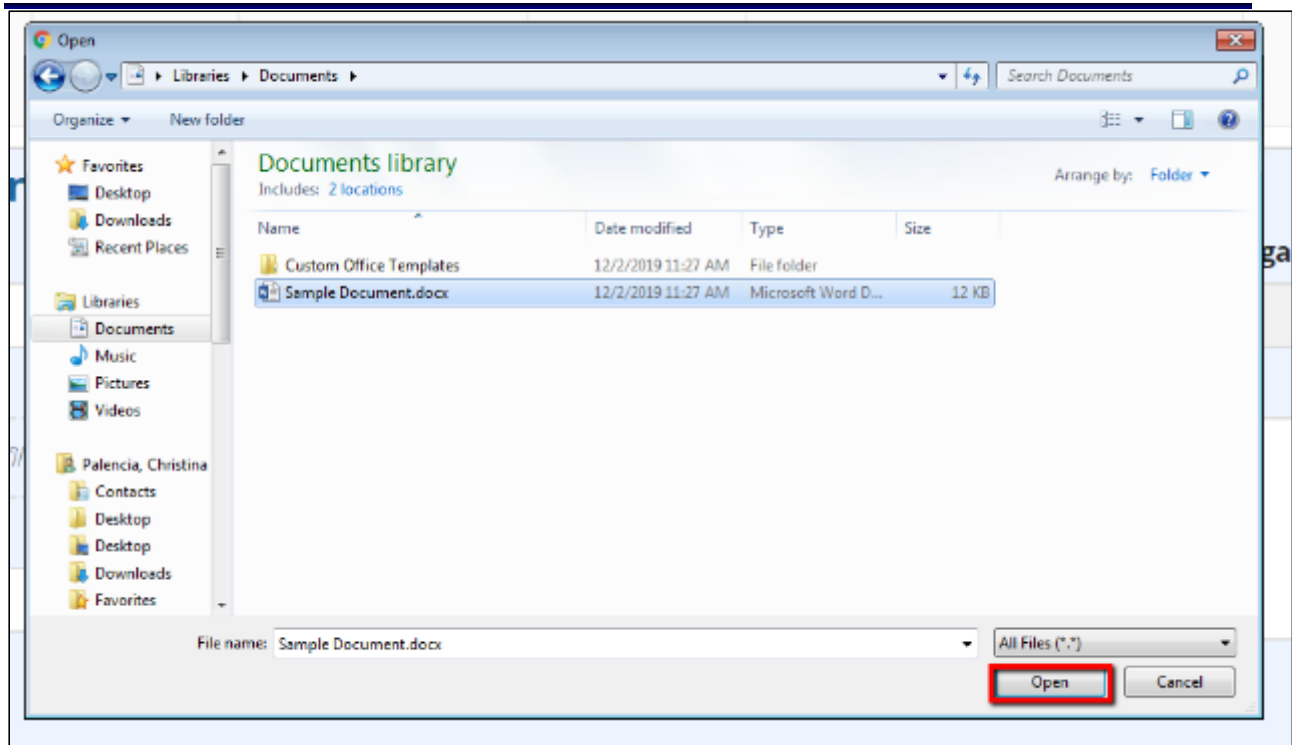
Document Name *

0/255

Description *

0/4000

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





- 7) The selected document will upload.
- 8) 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.



- 9) 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.

Add Document (Download the template)

System *	Access Control Group	Organization
SSOR	SSOR Local Security Managers (LSMs)	Select an Organization

Document

FACES Justification Document v1.0
PDF - 213.03 KB

Document Name *

0/255

Description

0/4000

CANCEL

UPLOAD DOCUMENT

CLOSE



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

- i) 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.
- ii) 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**.

11) 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.

Manage Role Documentation							
System		Access Control Group		Organization			
Select a System		Select a Group		Select an Organization			
ADD		DELETE					
<input type="checkbox"/>	Document Name ↑	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input type="checkbox"/>	1	123	Lillian (NTD Validation Analyst)	78100 - Region 1	10002 - Manchester Transit Authority (MTA)	10/18/2019	summie.ntdgsa@dot.gov
<input type="checkbox"/>	1001 role doc	1001 role doc	OTrak Region 4	78400 - Region 4	1001 - Transportation, Florida Department Of (FLORIDA DOT)	10/22/2019	faces.systemadministrator@dot.gov



- 12) 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.

Manage Role Documentation

System: Organization:

Access Control Group:

<input type="checkbox"/>	Document Name	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input type="checkbox"/>	1	123	Lillian (NTD Validation Analyst)	78100 - Region 1	10002 - Manchester Transit Authority (MTA)	10/18/2019	sunnie.ntdgsn@dot.gov
<input checked="" type="checkbox"/>	1001 role doc	1001 role doc	OTrak Region 4	78400 - Region 4	1001 - Transportation, Florida Department Of (FLORIDA DOT)	10/22/2019	faces.systemadministrator38@dot.gov
<input type="checkbox"/>	12	2	Bailey (NTD Validation Analyst)	78100 - Region 1	1R01 - Connecticut Department of Transportation (CDOT)	10/18/2019	sunnie.ntdgsn@dot.gov

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

Are you sure you want to delete the selected data?

- 14) Click **Yes** to delete the document. Click **No** to cancel.



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

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

Manage Role Documentation

System
TrAMS

Access Control Group
TrAMS Region 2

Organization
Select an Organization

Cost Center
78200 - Region 2

ADD
DELETE

<input type="checkbox"/>	Document Name	Description	Access Control Group	Cost Center	Organization	Uploaded Date	Uploaded By
<input type="checkbox"/>	Doc1	Fake Doc	TrAMS Region 2	78200 - Region 2	1414 - New Jersey Transit Corporation, The (NJTC)	11/5/2019	faces.sysadmin.bala@mailinator.com
<input type="checkbox"/>	test5	test5	TrAMS Region 2	78200 - Region 2	1924 - County Of Chemung (CHEMUNG CNT)	10/22/2019	Bruce.Hawkins12345
<input type="checkbox"/>	test6	test6	TrAMS Region 2	78200 - Region 2	1924 - County Of Chemung (CHEMUNG CNT)	10/22/2019	Bruce.Hawkins12345

CLOSE

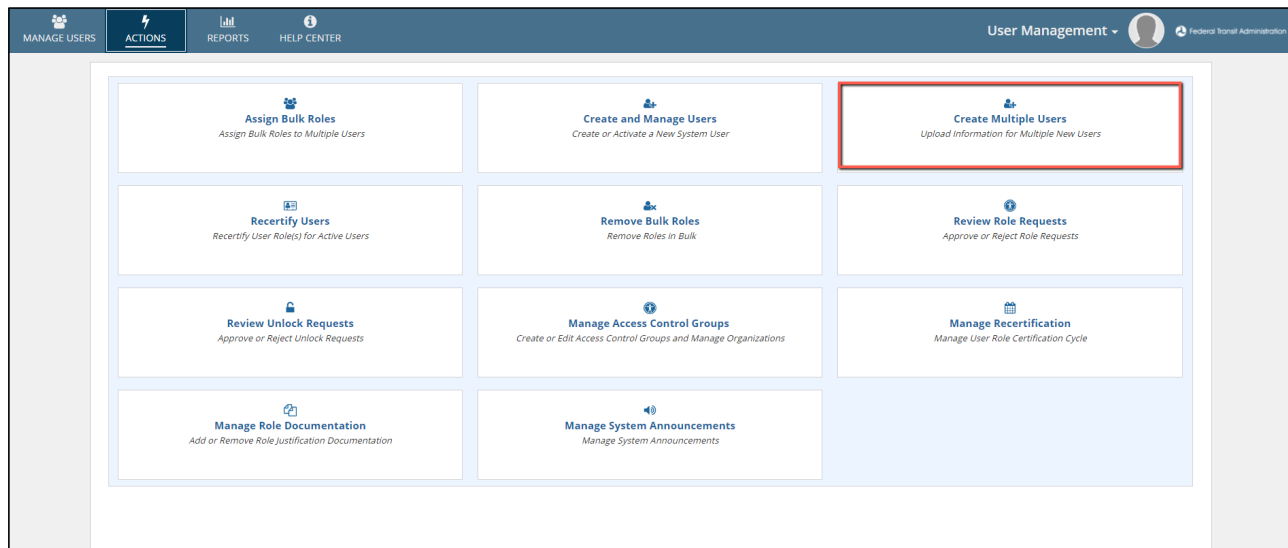
6.2.4 Action: Create Multiple Users

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 through the use of 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.

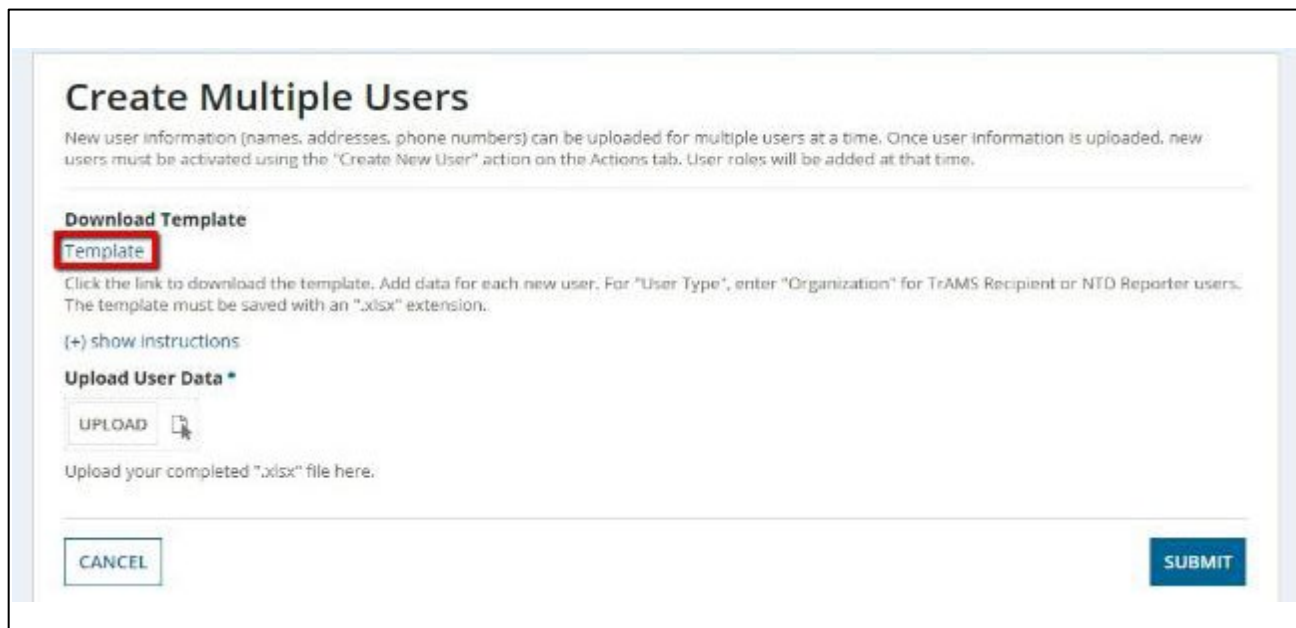


To upload multiple user information at once:

- 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 follow 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. (<i>periods required</i>).
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
	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.	(123)123-1234	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 ready to be uploaded, click **Upload** on the **Create Multiple Users** page to locate the Excel (.xlsx) file.

Create Multiple Users

New user information (names, addresses, phone numbers) can be uploaded for multiple users at a time. Once user information is uploaded, new users must be activated using the "Create New User" action on the Actions tab. User roles will be added at that time.

Download Template

Template

Click the link to download the template. Add data for each new user. For "User Type", enter "Organization" for TrAMS Recipient or NTD Reporter users. The template must be saved with an ".xlsx" extension.

(+) show instructions

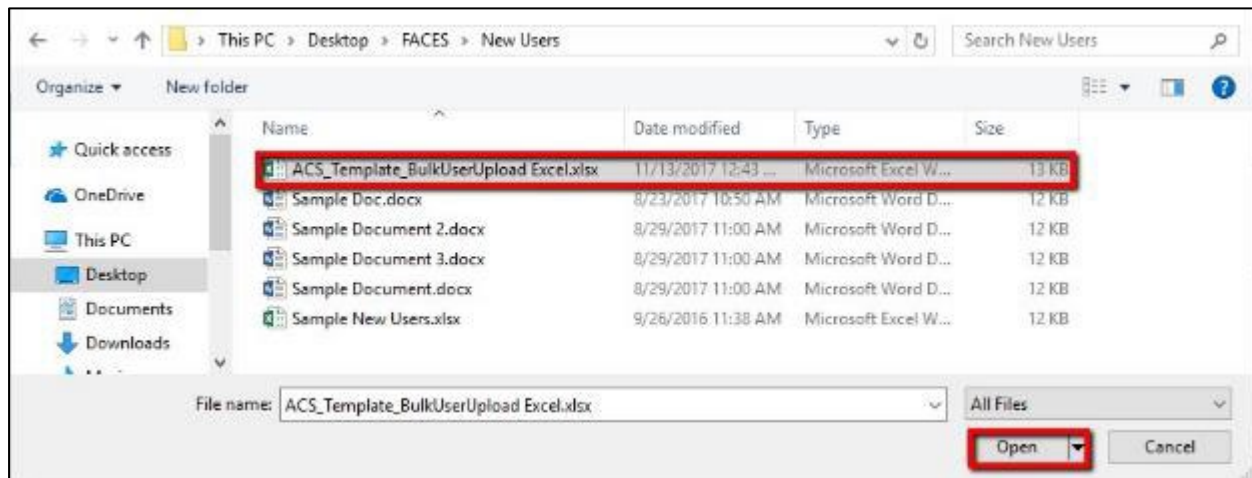
Upload User Data *

UPLOAD

Upload your completed ".xlsx" file here.

CANCEL **SUBMIT**

- 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.

Upload User Data *

ACS_Template_BulkUserUpload Excel
XLSX - 12.21 KB

Upload your completed ".xlsx" file here.

CANCEL **SUBMIT**



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

Create Multiple Users

New user information (names, addresses, phone numbers) can be uploaded for multiple users at a time. Once user information is uploaded, new users must be activated using the "Create New User" action on the Actions tab. User roles will be added at that time.

Download Template

Template

Click the link to download the template. Add data for each new user. For "User Type", enter "Organization" for TrAMS Recipient or NTD Reporter users. The template must be saved with an ".xlsx" extension.

(+) show instructions

Upload User Data *

ACS_Template_BulkUserUpload Excel
XLSX - 12.21 KB

Upload your completed ".xlsx" file here.

- 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.

Confirm Users

New Users

The information for the following users passed all validation checks. Click the "Submit" button to create these users.

Username	First Name	Last Name
jsmith1@fake.com	John	Smith
jsmith2@fake.com	Jessica	Smith

Users with Errors

The information for the following users contain one or more errors. These users cannot be created at this time. Click the "Back" button to upload a corrected file. Click "Cancel" to exit the form and try again later.

Username	Errors
jsmith3@fake.com	Office Phone: Input is Required
jsmith4@fake.com	City: Input is required



10) The user may:

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

You are about to exit this form. No users will be saved. Are you sure you want to continue?

NO YES

A confirmation dialog box with a light gray border. The text inside asks if the user is sure they want to continue exiting the form, noting that no users will be saved. There are two buttons at the bottom: a light gray 'NO' button on the left and a blue 'YES' button on the right. The 'YES' button is highlighted with a red rectangular border.

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

Changes will be lost, are you sure you want to go back?

NO YES

A confirmation dialog box with a light gray border. The text inside asks if the user is sure they want to go back, noting that changes will be lost. There are two buttons at the bottom: a light gray 'NO' button on the left and a blue 'YES' button on the right. The 'YES' button is highlighted with a red rectangular border.

- 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.

jsmith3@fake.com	Office Phone: Input is Required
jsmith4@fake.com	City: Input is required

CANCEL BACK SUBMIT

A summary screen for user upload. It features a table with two rows of user data and validation errors. Below the table are three buttons: 'CANCEL', 'BACK', and 'SUBMIT'. The 'SUBMIT' button is highlighted with a red rectangular border.

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

Creating Users

0 out of 2 users have been created. Please click refresh to see if the process is complete. This may take a few minutes.

REFRESH

A form titled 'Creating Users'. It displays a status message indicating that 0 out of 2 users have been created and advises the user to click refresh. A blue 'REFRESH' button is located at the bottom right of the form, highlighted with a red rectangular border.

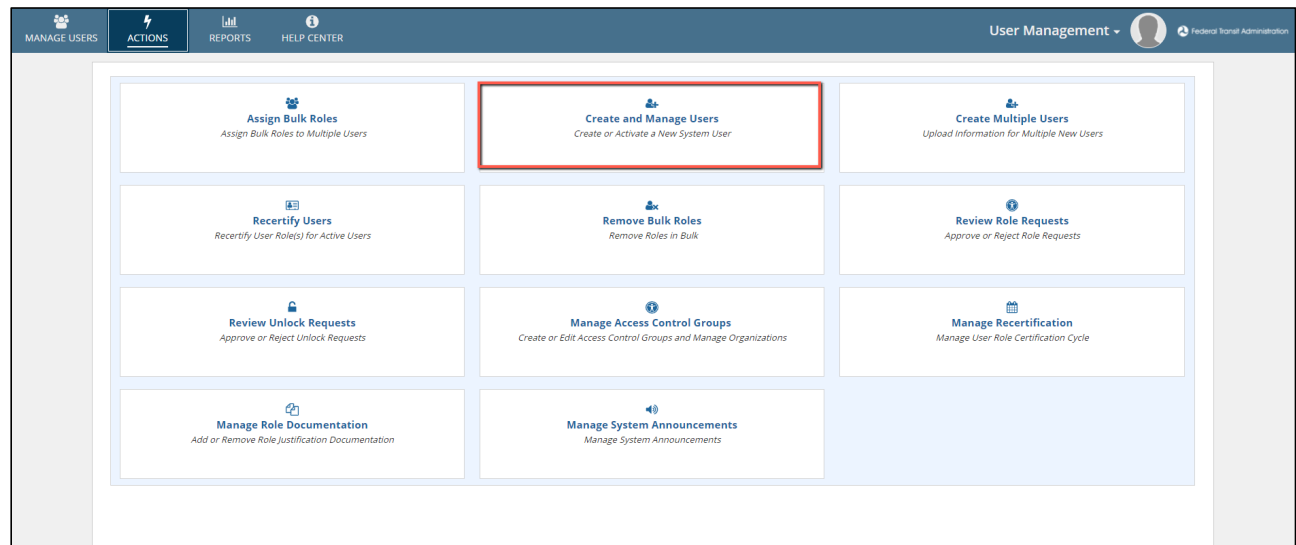


- 12) Once the users have been added to the system, clicking **Refresh** will display the **Users Created** screen. Click **Close** to return to the Actions tab.



- 13) To finalize user setup, **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**.



Create and Manage Users

User Type *

☐ FTA Staff

☐ Organization User (e.g. Recipient, Reporter)

☐ External User (e.g. DOL, DOT Reviewer, Auditor, Contractors)

Create and Manage Users

Username

The username must be an email address.

- 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**.

Create and Manage Users

User Information

Full Name	Ms. Jane Doe	Username	janedoe@fakeemail.com
Title	Analyst	Status	Deactivated
User Type	Organization		

The user needs to be activated. Would you like to manage this user's roles?



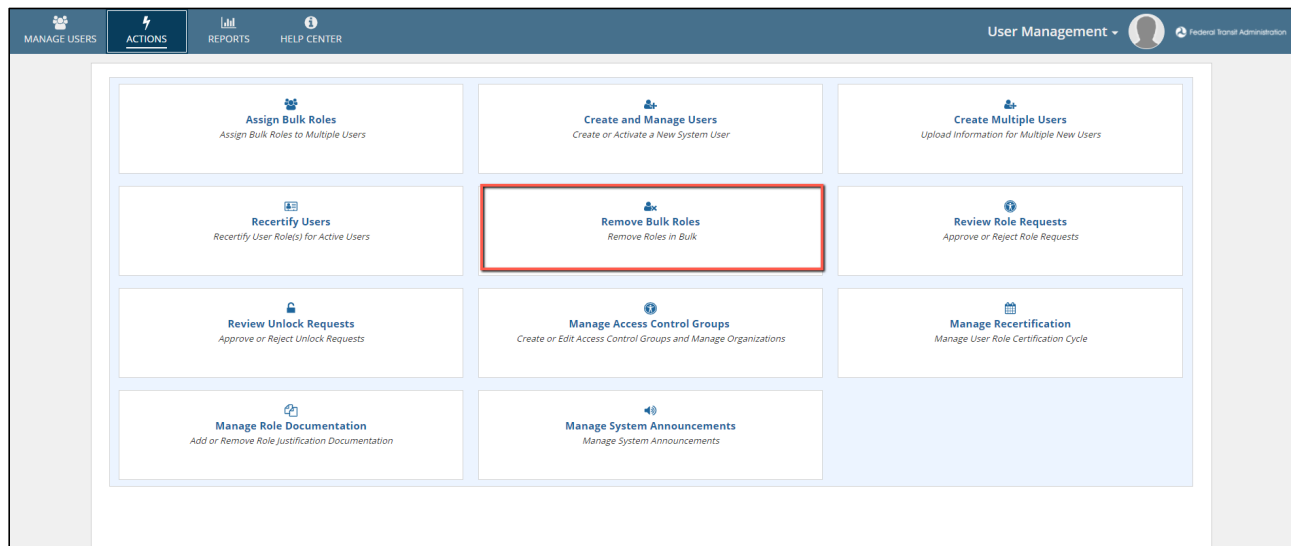
- 17) Follow the standard process for adding roles to the user and then click **Activate**. The user will be notified that their account has been established at this point.

6.2.5 Action: Remove Bulk Roles

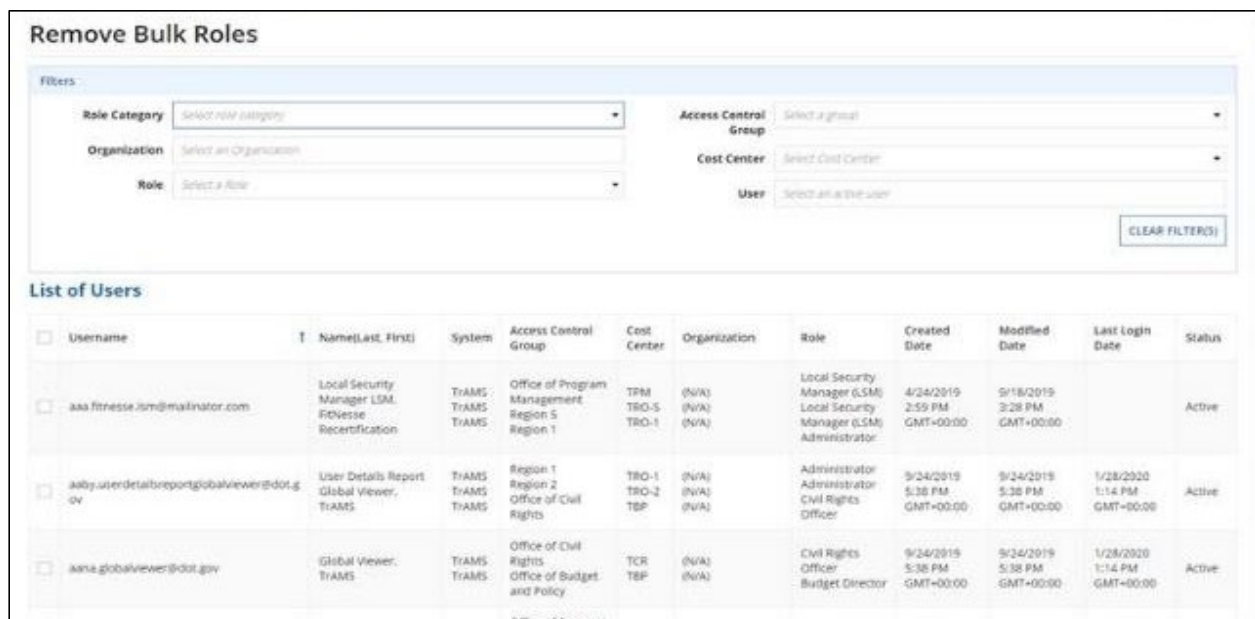
If more than one user or external user's user roles needs to be removed from the system, the **System Admin, Global Security Manager, Validation Analyst, LSM** may remove user roles through this action. The role removal process will provide validations and will only allow users to remove the user roles 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.

Remove Bulk Roles

Filters

Role Category

Recipient

Organization

1334 - Transportation, Connecticut Department Of (CONNDOT)

Role

Select a Role

Access Control Group

Region 1

Cost Center

TR100 - Region 1 (TRD-1)

User

Select an active user

CLEAR FILTER(S)

- 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.

Remove Bulk Roles

Filters

Role Category

Recipient

Organization

1334 - Transportation, Connecticut Department Of (CONNDOT)

Role

Select a Role

Access Control Group

Region 1

Cost Center

TR100 - Region 1 (TRD-1)

User

Select an active user

CLEAR FILTER(S)

List of Users

<input type="checkbox"/>	Username	Name (Last, First)	System	Access Control Group	Cost Center	Organization	Role	Created Date	Modified Date	Last Login Date	Status
<input checked="" type="checkbox"/>	aiden.al@mailinator.com	Al, Aiden (Mr.)	TrAMS	Region 1	TRD-1	1334 - CONNDOT	Submitter	3/20/2019 2:44 PM GMT+00:00	2/4/2020 4:36 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input checked="" type="checkbox"/>	aria.lee@mailinator.com	lee, aria (Ms.)	TrAMS	Region 1	TRD-1	1334 - CONNDOT	User Manager	5/1/2019 4:12 PM GMT+00:00	1/6/2020 8:32 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	arya.orguser@mailinator.com	Allen, Sunnie (Ms.)	TrAMS	Region 1	TRD-1	1334 - CONNDOT	Civil Rights Submitter	8/3/2019 5:58 PM GMT+00:00	8/29/2019 2:11 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	arya.sunnie@mailinator.com	sunnie, Arya (Ms.)	TrAMS	Region 1	TRD-1	1334 - CONNDOT	User Manager	1/6/2020 6:36 PM GMT+00:00	1/19/2020 6:39 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	assia.khadri@fate.com	Khadr, assia (Mr.)	TrAMS	Region 1	TRD-1	1334 - CONNDOT	Attorney Submitter	9/6/2019 3:18 PM GMT+00:00	3/9/2020 6:54 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active

<input type="checkbox"/>	essia.khadri@fake.com	Khadri, essia (Mr.)	TrAMS TrAMS TrAMS	Region 1 Region 1 Region 1	TRO-1 TRO-1 TRO-1	1334 - CONNDOT 1334 - CONNDOT 1334 - CONNDOT	Attorney Submitter FRR Reporter	9/9/2019 3:18 PM GMT+00:00	9/9/2020 6:54 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	brian.trams@mnoepry.com	Doe, Joe (Mr.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	11/12/2019 5:08 PM GMT+00:00	11/12/2019 5:08 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	christina.umtrams@mailinator.com	Pal, Christina (Mrs.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	5/16/2019 6:49 PM GMT+00:00	2/29/2020 10:09 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	conndot.civilrights2@dot.gov	Civil Rights, conndot	TrAMS	Region 1	TRO-1	1334 - CONNDOT	Civil Rights	9/10/2019 9:54 PM GMT+00:00	9/10/2019 9:55 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	conndot.developer1@dot.gov	Developer, conndot (Mrs.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	1/11/2019 6:47 PM GMT+00:00	9/24/2019 2:05 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	conndot.frrreporter2@dot.gov	FRR Reporter, conndot	TrAMS	Region 1	TRO-1	1334 - CONNDOT	FRR Reporter	9/10/2019 9:54 PM GMT+00:00	9/10/2019 9:55 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active

1 - 10 of 37 >

User Roles

<input checked="" type="checkbox"/>	Username	Role	Access Control Group	Cost Center	Organization	Document	Status
<input checked="" type="checkbox"/>	aster.al@mailinator.com	Submitter	Region 1	Region 1	Transportation, Connecticut Department Of	Test Doc	Approved
<input checked="" type="checkbox"/>	aria.lee@mailinator.com	User Manager	Region 1	Region 1	Transportation, Connecticut Department Of	Role Doc	Approved
<input checked="" type="checkbox"/>	aria.lee@mailinator.com	Submitter	Region 1	Region 1	Transportation, Connecticut Department Of	Role Doc	Approved

CANCEL

NEXT

<input type="checkbox"/>	essia.khadri@fakex.com	khadr, essia (MR.)	TrAMS TrAMS TrAMS	Region 1 Region 1 Region 1	TRO-1 TRO-1 TRO-1	1334 - CONNDOT 1334 - CONNDOT 1334 - CONNDOT	Attorney Submitter FR Reporter	9/6/2019 3:18 PM GMT+00:00	3/9/2020 6:54 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	brian.tramsu@noreply.com	Doe, Joe (MR.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	11/12/2019 5:08 PM GMT+00:00	11/12/2019 5:08 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	christina.untrams@mailinator.com	Pal, Christina (Mrs.)	TrAMS	Region 1	TRO-1	1234 - CONNDOT	User Manager	5/16/2019 6:49 PM GMT+00:00	2/29/2020 10:09 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	conndot.civilrights2@dot.gov	Civil Rights, conndot	TrAMS	Region 1	TRO-1	1334 - CONNDOT	Civil Rights	9/10/2019 9:54 PM GMT+00:00	9/19/2019 9:55 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	conndot.developer1@dot.gov	Developer, conndot (Mrs.)	TrAMS	Region 1	TRO-1	1334 - CONNDOT	User Manager	1/11/2019 6:47 PM GMT+00:00	1/24/2019 2:05 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active
<input type="checkbox"/>	conndot.frrreporter2@dot.gov	FR Reporter, conndot	TrAMS	Region 1	TRO-1	1334 - CONNDOT	FR Reporter	9/10/2019 9:54 PM GMT+00:00	9/19/2019 9:55 PM GMT+00:00	1/28/2020 1:14 PM GMT+00:00	Active

1 - 10 of 37 >

User Roles

<input checked="" type="checkbox"/>	Username	Role	Access Control Group	Cost Center	Organization	Document	Status
<input checked="" type="checkbox"/>	aiden.4@mailinator.com	Submitter	Region 1	Region 1	Transportation, Connecticut Department Of	Test Doc	Approved
<input checked="" type="checkbox"/>	aria.lee@mailinator.com	User Manager	Region 1	Region 1	Transportation, Connecticut Department Of	Role Doc	Approved
<input checked="" type="checkbox"/>	aria.lee@mailinator.com	Submitter	Region 1	Region 1	Transportation, Connecticut Department Of	Role Doc	Approved

CANCEL

NEXT

Version 6.3.7
Unclassified - For Official Use Only



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.

Confirm Role Removal

System	Username	Access Control Group	Role Category	Role	Organization	Cost Center
TRAMS	aiden.aj@mailinator.com	Region 1	Recipient	Submitter	1334 - Transportation, Connecticut Department Of	78100 - Region 1
TRAMS	aria.lee@mailinator.com	Region 1	Recipient	User Manager	1334 - Transportation, Connecticut Department Of	78100 - Region 1
TRAMS	aria.lee@mailinator.com	Region 1	Recipient	Submitter	1334 - Transportation, Connecticut Department Of	78100 - Region 1

BACK
CANCEL
CONFIRM

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 **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.

+ CREATE NEW USER
+ CREATE MULTIPLE USERS

Report Filter Criteria

System

Select an Application

Role Category

Select role category

Access Control Group

Select a group

Organization

Role

Select a Role

☒ Display individual Roles in Grid

Cost Center

Select Cost Center

User

Select a user (including deactivated)

Name

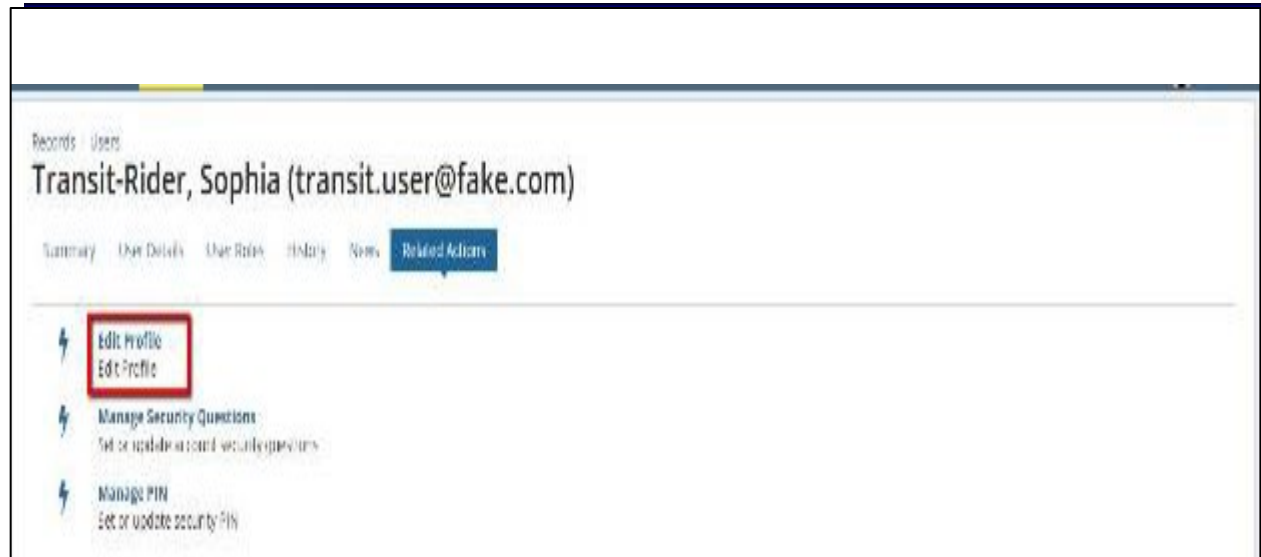
Search on First or Last name (whole or part)

Status

☐ Active
 ☐ Locked
 ☐ Deactivated

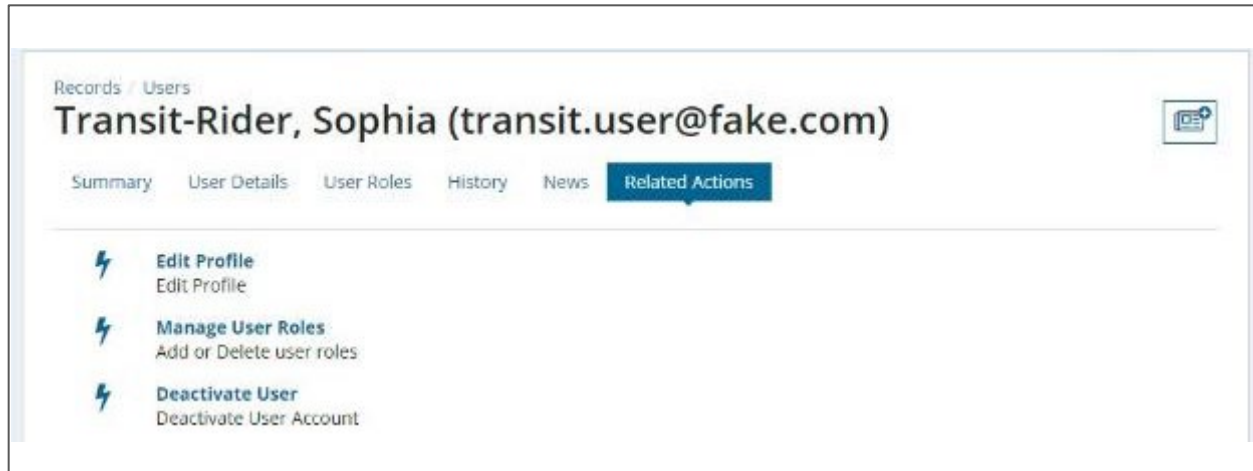
CLEAR FILTER(S)

- 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.



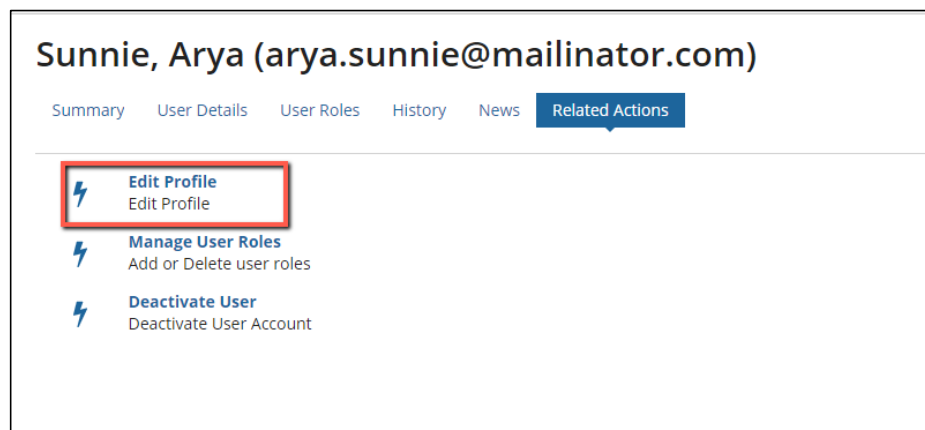
6.3.1 Related Action: Edit User Profile

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.



Edit User Profile

Basic Information

Username *

arya.sunnie@mailinator.com

Title *

um

First Name *

Arya

Honorific *

Ms.

Middle Name

Company Name

Last Name *

sunnie

Department

Contact Information

Email *

arya.orgum@mailinator.com

Fax Number

Phone Number *

(123) 454-5456

Phone Ext

Address 1 *

1330 summerfield dr

Zip Code *

20170

Address 2

Zip Ext

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

Edit User Profile

Basic Information

Username *

arya.sunnie@mailinator.com

Title *

um

First Name *

Arya

Honorific *

Ms.

Middle Name

Company Name

Last Name *

sunnie

Department

Contact Information

Email *

arya.orgum@mailinator.com

Fax Number

Phone Number *

(123) 454-5456

Phone Ext

Address 1 *

1330 summerfield dr

Zip Code *

20170

Address 2

Zip Ext

City *

Herndon

PO Box

State *

DC

CANCEL

SAVE

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

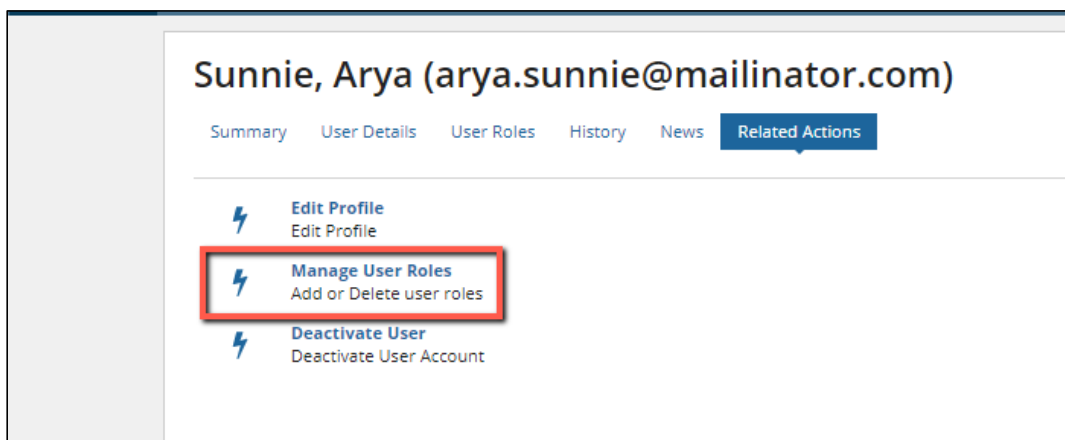
When adding/removing roles, note that users cannot have both Read Only and active roles in the same organization (or Cost Center for FTA users).

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

6.3.2.1 Add Role

To add roles to a user:

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



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



Manage User Roles

User Information

Full Name: Mrs. Joe Doe

Title: Tester

User Type: Organization

Username: briantramstestum@example.com

Status: Active

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	1439 - 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	FPR Reporter	Region 6	1206 - Central Arkansas Transit Authority	78600 - Region 6 (TRO 6)	N/A	Approved				
5	TrAMS	Recipient	Official	Region 7	1277 - Bistate Regional Commission	78700 - Region 7 (TRO 7)	Test1	Approved				

5 Items

- 4) Select **Cancel** at any point in this process to return to the previous page without saving any changes.
- 5) 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	1439 - 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	FPR Reporter	Region 6	1206 - Central Arkansas Transit Authority	78600 - Region 6 (TRO 6)	N/A	Approved				
5	TrAMS	Recipient	Official	Region 7	1277 - Bistate Regional Commission	78700 - Region 7 (TRO 7)	Test1	Approved				

5 Items

+ ADD NEW ROLE

CANCEL

VIEW HISTORY SUBMIT

- 6) 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	1439 - 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	78900 - 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

- 7) 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.

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	1439 - 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	... Select a Value ...	Select a Group	1618 - Association Of Monterey Bay Area Government	78900 - Region 9 (TRO-9)	testing doc	Approved				
4	TrAMS	Recipient	... Select a Value ...	Select a Group	1506 - Central Arkansas Transit Authority	78900 - Region 6 (TRO-6)	N/A	Approved				
5	TrAMS	Recipient	... Select a Value ...	Select a Group	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

- 8) Roles are further distinguished in terms of whether they require **Approval**, a justification **Document**, 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.

- 9) 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.

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	TrAMS	Recipient	User Manager	Office of Program Management	1439 - Philadelphia, City Of	65000 - Office of Program Management (TRM)	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	PRR 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	Attorney	Select a Group			N/A	Approved				

- 10) The user and the updated roles will display. In some cases, documentation is required before a role assignment can be submitted. In those cases, the Add Justification Document section will display. The TrAMS **Submitter**, **Attorney**, and **Official** roles all require a Delegation of Authority letter from the agency CEO to justify the role assignment. DGS and NTD **User Managers** require a letter as well. The Delegation of Authority letter template is available on the FTA public website.

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	TrAMS	Recipient	User Manager	Office of Program Management	1439 - Philadelphia, City Of	65000 - Office of Program Management (TRM)	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	PRR 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	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE...	78300 - Region 3 (TRO-3)	<div> Select Existing Upload </div>	Approved				



- 11) 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	62000 - Office of Program Management (TRM)	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	FIR Reporter	Region 6	1505 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved		
5	TrAMS	Recipient	Official	Region 7	1277 - U.S. State Regional Commission	78700 - Region 7 (TRO-7)	Test1	Approved		
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE ...	78300 - Region 3 (TRO-3)	Select Existing Upload	Approved		

- 12) 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	62000 - Office of Program Management (TRM)	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	FIR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved		
5	TrAMS	Recipient	Official	Region 7	1277 - U.S. State Regional Commission	78700 - Region 7 (TRO-7)	Test1	Approved		
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE ...	78300 - Region 3 (TRO-3)	Select Existing Upload	Approved		



- 13) The same upload section that is visible on the **Manage Role Documentation** [action](#) will display. The **Add Document for Selected Role** section will display beneath the list of available documents. You may download the available Justification Document template in the provided link displayed, if a justification document is not already available.

1	OTrak	FTA Staff	Local Security Manager (LSM)	OTrak Region 10	-	78900 - Region 9 (TRO-9)	N/A	Approved	test			
2	TrAMS	Global Users	Global Security Manager (GSM)				Select Existing Upload	Approved				

(#2) Add Document For Selected Role [Download the template](#)

System
TrAMS

Document*

UPLOAD
 Drop file here

Document Name*

0/255

Cost Center

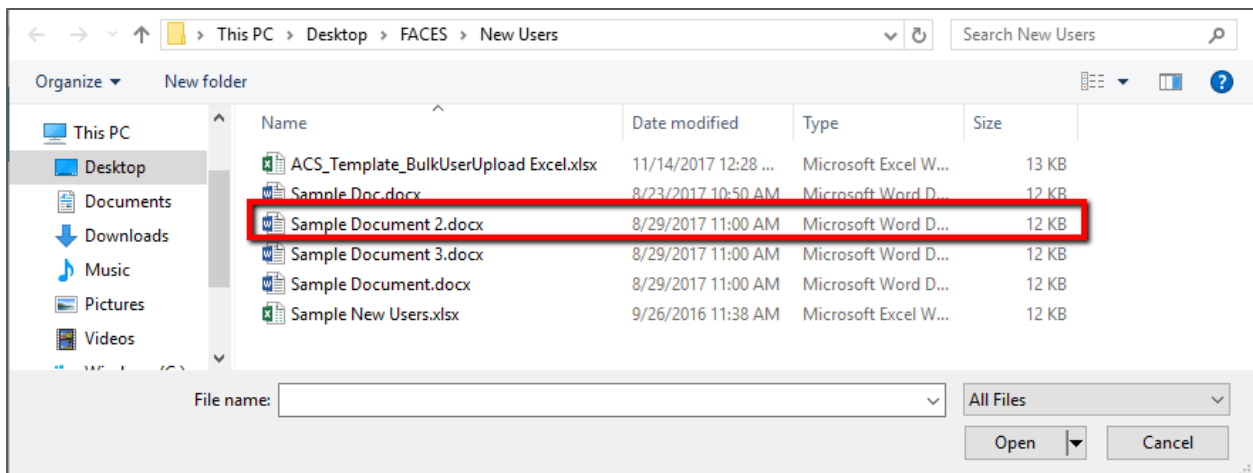
Organization
N/A

Description*

0/4000

CANCEL
UPLOAD DOCUMENT

- 14) 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**.



- 15) The appropriate document will upload.



- 16) 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. Maximum characters remaining will show beneath the document name and description fields.

1	OTrak	FTA Staff	Local Security Manager (LSM)	OTrak Region 10	-	78900 - Region 9 (TRO-9)	N/A	Approved	test			
2	TrAMS	Global Users	Global Security Manager (GSM)				Select Existing Upload	Approved				

(#2) Add Document For Selected Role [Download the template](#)

System: TrAMS Cost Center: Organization: N/A

Document *

UPLOAD Drop file here

Document Name *

CANCEL

Description *

UPLOAD DOCUMENT

- 17) Once the information for the document is finalized, click **Upload Document**.
- 18) 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.

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	1438 - Philadelphia, City Of	65000 - Office of Program Management (TPM)	Approval	Approved				
2	TrAMS	Recipient	User Manager	Office of Administration	2325 - 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 - Bistate Regional Commission	78700 - Region 7 (TRO-7)	Test1	Approved				
6	TrAMS	Recipient	Attorney	Region 1	1402 - Baltimore, City Of (IA) (MD) ...	78300 - Region 1 (TRO-1)	Role Approval Doc	Approved				

6 items



- 19) At this point, enter any comments into the **Comments** data entry box if there are any comments are necessary to complete the use of the document for that role, especially if the document is not obviously associated with the role. Then click **Save**.

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	TrAMS	Recipient	User Manager	Office of Program Management	1439 - Philadelphia, City Of	66000 - Office of Program Management (TPM)	Approval	Approved				
2	TrAMS	Recipient	User Manager	Office of Administration	2825 - National Science Foundation	67000 - 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	FTR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78600 - Region 6 (TRO-6)	N/A	Approved				
5	TrAMS	Recipient	Official	Region 7	1237 - Bistate Regional Commission	78700 - Region 7 (TRO-7)	Test1	Approved				
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of (BALTIMORE ...)	78300 - Region 3 (TRO-3)	Role Approval Doc	Approved				

6 items

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

CANCEL

VIEW HISTORY

SUBMIT

- 21) The **User Roles Updated** page displays with a message that the roles are being processed within the system.

User Roles Updated

The user's role changes are currently being processed. It may take a few minutes for all changes to appear on the user's record.

CLOSE

- 22) Click **Close**. The **Related Actions** page displays.

7.3.2.2 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**.



Records / Users

Doe, Joe (briantramstestum@example.com)

Summary User Details User Roles History News **Related Actions**

- Edit Profile**
Edit Profile
- Manage User Roles**
Add or Delete user roles
- Deactivate User**
Deactivate User Account
- Reset PIN**
This will reset the user's PIN

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

Doe, Joe (briantramstestum@example.com)

Summary User Details User Roles History News **Related Actions**

Manage User Roles

User Information

Full Name: Mrs. Joe Doe Username: briantramstestum@example.com
Title: Tester Status: Active
User Type: Organization

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	1439 - Philadelphia, City Of	62000 - 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				

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

Manage User Roles

User Information

Full Name: Mrs. Joe Doe Username: briantramstestum@example.com
Title: Tester Status: Active
User Type: Organization

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	1439 - Philadelphia, City Of	62000 - Office of Program Management (TPM)	Approval	Deleted				
2	TrAMS	Recipient	User Manager	Office of Administration	2355 - National Science Foundation	62000 - Office of Administration (TAD)	test	Approved				



- 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.

#	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	Deleted				
2	TrAMS	Recipient	User Manager	Office of Administration	2156 - National Science Foundation	60000 - 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	FTR Reporter	Region 6	1506 - Central Arkansas Transit Authority	78900 - Region 6 (TRO-6)	N/A	Approved				
5	TrAMS	Recipient	Official	Region 7	1277 - Bi-State Regional Commission	78900 - Region 7 (TRO-7)	Two 1	Approved				
6	TrAMS	Recipient	Attorney	Region 3	1402 - Baltimore, City Of	78900 - Region 3 (TRO-3)	Role Approval Doc	Apprent				

5 items

+ ADD NEW ROLE

CANCEL VIEW HISTORY SUBMIT

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

User Roles Updated

The user's role changes are currently being processed. It may take a few minutes for all changes to appear on the user's record.

CLOSE

6.3.2.2 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:

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



Primary Reporter, adot (aaria.primaryreporter@dot.gov)

Summary User Details User Roles History News **Related Actions**

- Edit Profile**
Edit Profile
- Manage User Roles**
Add or Delete user roles
- Deactivate User**
Deactivate User Account

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

Manage User Roles

User Information

Full Name: adot Primary Reporter Username: aaria.primaryreporter@dot.gov
Title: Test User Status: Active
User Type: Organization

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	1 - Arizona Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
2	SSOR	SSO	Viewer	SSOR Local Security Managers (LSMs)	2 - Arkansas State Highway and Transportation Department	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
3	SSOR	SSO	Viewer	SSOR Local Security Managers (LSMs)	1 - Arizona Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
4	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	15 - Missouri Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
5	SSOR	SSO	Alternate Reporter	SSOR Local Security Managers (LSMs)	15 - Missouri Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				

5 items

4) 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.

Manage User Roles

User Information

Full Name: adot Primary Reporter Username: aaria.primaryreporter@test.com
Title: Test User Status: Active
User Type: Organization

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	1 - Arizona Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
2	TRAMS	Recipient	Attorney	Office of Administration	7109 - Federal Aviation Administration	62000 - Office of Administration (TAD)	Dummy - Patch - 2019-06-10_1420	Approved				
3	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	10 - Louisiana Department of Transportation and Development	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
4	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	16 - New Jersey Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				



- 5) 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.

Manage User Roles

User Information

Full Name adot Primary Reporter

Title Test User

User Type Organization

Username arya.primaryreporter@test.com

Status Active

Add/Update User Roles

#	System	Role Category	Role	Access Control Group	Organization	Cost Center	Justification Document	Status	Comments			
1	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	1 - Arizona Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
2	TRAMS	Recipient	Attorney	Office of Administration	7109 - Federal Aviation Administration	62000 - Office of Administration (TAD)	Dummy - Patch - 2019-06-10_1420	Approved				
3	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	10 - Louisiana Department of Transportation and Development	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				
4	SSOR	SSO	Primary Reporter	SSOR Local Security Managers (LSMs)	16 - New Jersey Department of Transportation	74000 - Office of Transit Safety and Oversight (TSO)	N/A	Approved				

- 6) 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.
- 7) **Role Comments** can be directly added or edited. *Changes will overwrite the existing comment.*
- 8) Once all changes have been made, click **Submit**.
- 9) The **User Roles Updated** page will display. Click **Close** to return to the **Related Actions** page.

User Roles Updated

The user's role changes are currently being processed. It may take a few minutes for all changes to appear on the user's record.

CLOSE

6.3.3 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 of 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**.

Primary Reporter, adot (arya.primaryreporter@test.com)

[Summary](#)
[User Details](#)
[User Roles](#)
[History](#)
[News](#)
[Related Actions](#)

⚡ **Edit Profile**
Edit Profile

⚡ **Manage User Roles**
Add or Delete user roles

⚡ **Deactivate User**
Deactivate User Account

↺ **Reset PIN**
This will reset the user's PIN

- 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).

Primary Reporter, adot (aaria.primaryreporter@dot.gov)

[Summary](#)
[User Details](#)
[User Roles](#)
[History](#)
[News](#)
[Related Actions](#)

Deactivate User

User Information

Full Name

adot Primary Reporter

Username

aaria.primaryreporter@dot.gov

Title

Test User

Status

Active

User Type

Organization

This user has roles in other organizations. You do not have the authority to deactivate this user. To remove this user's access to your organization, go to 'Manage Roles' and remove all organization roles.

User's Roles You Can Manage

Role	System	Cost Center	Access Control Group	Organization
Alternate Reporter	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	15 - Missouri Department of Transportation (MoDOT)
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)	15 - Missouri Department of Transportation (MoDOT)
Viewer	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	2 - Arkansas State Highway and Transportation Department (ARDOT)
Viewer	SSOR	74000 - Office of Transit Safety and Oversight	SSOR Local Security Managers (LSMs)	1 - Arizona Department of Transportation (ADOT)

April 11, 2022
FACES_User_Guide-6.3.7.doc

125

Version 6.3.7
Unclassified - For Official Use Only



- 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.

Deactivate User

User Information

Full Name

adot Primary Reporter

Title

Test User

User Type

Organization

Username

arya.primaryreporter@test.com

Status

Active

User's Roles You Can Manage

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)

- 6) Click **Cancel** at the bottom of the page to return to the **Related Actions** page without saving any changes.
- 7) Enter any comments/justification for the deactivation and click **Deactivate** to proceed with the user deactivation. Comments are required.

Deactivation

Comments *

CANCEL

MANAGE ROLES

DEACTIVATE

- 8) 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.

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?

YES

NO

- 9) 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:



Are you sure you want to deactivate this user?

YES

NO

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

Deactivation In Progress

The user is being deactivated. It may take a few minutes for all changes to appear on the user's record. Click the 'Refresh' button after a minute to confirm that the user has been deactivated.

CLOSE

REFRESH

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

From: FACES System Administrator
Subject: ALERT: Account Deactivated

Dear fta.sungkyun.kim.ctr FACES - FTA,
Your account has been deactivated. You can no longer login to the following applications:

- FACES

Please contact your immediate user manager(s) if you need access reinstated.

If you need assistance please call your application help desk.
FACES 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.

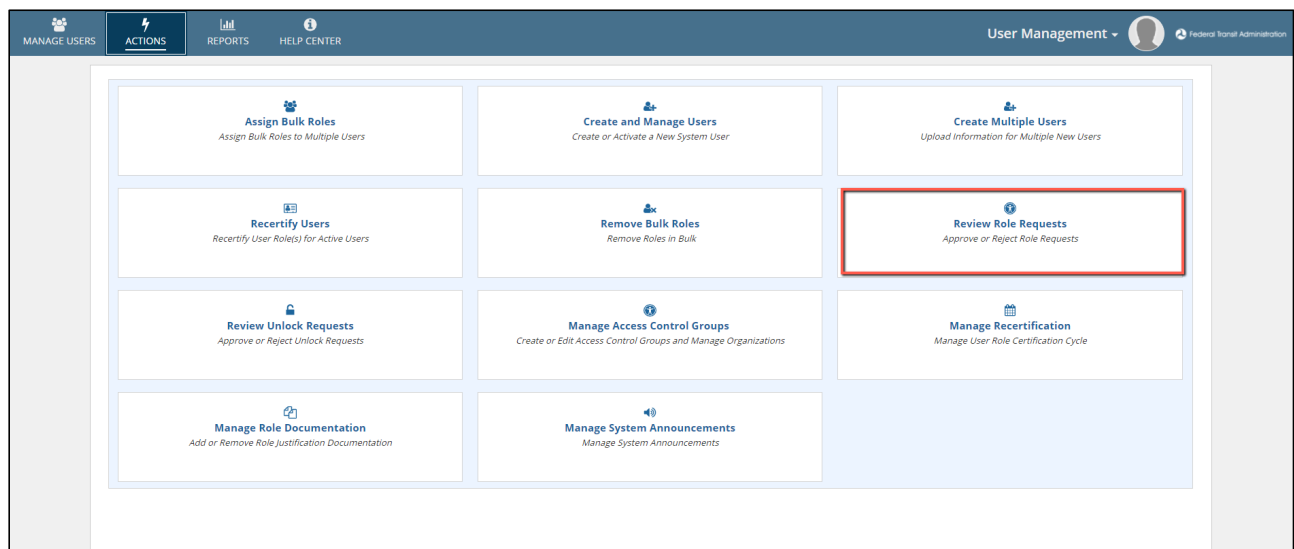


6.3.4 Action: Review Role Requests

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 at this time.* 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.

Approve Roles

System: NTD
Role Category: Reporter
User: *Select an active user*

Access Control Group: *Select a Group*
Cost Center: *Select a Cost Center*
Organization:
CLEAR FILTER(S)

<input type="checkbox"/>	User	Role	Role Category	System	Access Control Group	Cost Center	Organization	Document
<input type="checkbox"/>	ntd.njtransit.usermanager2@dot.gov (ntd.njtransit.usermanager2@dot.gov)	CEO Delegate	Reporter	NTD	Erik Chadwell (NTD Validation Analyst)	78100 - Region 1	1R06 - Vermont Agency of Transportation (VTrans)	Role Doc
<input type="checkbox"/>	ntd.userb.requestrole@fake.com (ntd.userb.requestrole@fake.com)	CEO Delegate	Reporter	NTD	Matt Bonzek (NTD Validation Analyst)	79000 - Region 10	00041 - Alaska Railroad Corporation (ARRC)	1
<input type="checkbox"/>	orguser.ntd@mailinator.com (orguser.ntd@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input type="checkbox"/>	seat.ceo1@dot.gov (seat.ceo1@dot.gov)	CEO Delegate	Reporter	NTD	Erik Chadwell (NTD Validation Analyst)	78100 - Region 1	1R06 - Vermont Agency of Transportation (VTrans)	Role Doc

CANCEL
APPROVE
REJECT

- 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.

<input type="checkbox"/>	User	Role	Role Category	System	Access Control Group	Cost Center	Organization	Document
<input type="checkbox"/>	Bala K (bala@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input checked="" type="checkbox"/>	njtransit User Manager (ntd.njtransit.usermanager2@dot.gov)	CEO Delegate	Reporter	NTD	Erik Chadwell (NTD Validation Analyst)	78100 - Region 1	1R06 - Vermont Agency of Transportation (VTrans)	Role Doc
<input type="checkbox"/>	d d (ntd.userb.requestrole@fake.com)	CEO Delegate	Reporter	NTD	Matt Bonzek (NTD Validation Analyst)	79000 - Region 10	00041 - Alaska Railroad Corporation (ARRC)	1
<input type="checkbox"/>	Orguser Ntd (orguser.ntd@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input type="checkbox"/>	pennsylvaniaiv Civil Rights (orgusers.tramsxyz@mailinator.com)	User Manager	Reporter	NTD	Courtney Springer (NTD Validation Analyst)	79000 - Region 10	0R01 - Idaho Transportation Department (ITD)	dummy doc
<input type="checkbox"/>	ram editor (ramesh.ntssafetyeditor@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input type="checkbox"/>	seat CEO (seat.ceo1@dot.gov)	CEO Delegate	Reporter	NTD	Erik Chadwell (NTD Validation Analyst)	78100 - Region 1	1R06 - Vermont Agency of Transportation (VTrans)	Role Doc

7 Items

Requester Comments
submitting a requested role

My Comments

CANCEL
APPROVE
REJECT

- 6) Additional details about the request will display 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 download.

<input type="checkbox"/>	User	Role	Role Category	System	Cost Center	Organization	Document
<input type="checkbox"/>	Administrator1 Region 3 (region3.administrator1)	Initial Reviewer	FTA Staff	TrAMS	78300 - Region 3	N/A	N/A
<input checked="" type="checkbox"/>	Submitter WMATA (wmata.submitter4@fake.com)	Submitter	Recipient	TrAMS	78300 - Region 3	1398 - WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY (WMATA)	Requested Document

- 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.

<input type="checkbox"/>	User	Role	Role Category	System	Access Control Group	Cost Center	Organization	Document
<input type="checkbox"/>	Bala K (bala@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input checked="" type="checkbox"/>	njtransit User Manager (ntd.njtransit.usermanager2@dot.gov)	CEO Delegate	Reporter	NTD	Erik Chadwell (NTD Validation Analyst)	78100 - Region 1	1R06 - Vermont Agency of Transportation (VTrans)	Role Doc
<input type="checkbox"/>	d d (ntd.userb.requestrole@fake.com)	CEO Delegate	Reporter	NTD	Matt Bonzek (NTD Validation Analyst)	79000 - Region 10	00041 - Alaska Railroad Corporation (ARRC)	1
<input type="checkbox"/>	Orguser Ntd (orguser.ntd@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input type="checkbox"/>	pennsylvania Civil Rights (orgusers.tramsxyz@mailinator.com)	User Manager	Reporter	NTD	Courtney Springer (NTD Validation Analyst)	79000 - Region 10	0R01 - Idaho Transportation Department (ITD)	dummy doc
<input type="checkbox"/>	ram editor (ramesh.ntssafetyeditor@mailinator.com)	User Manager	Reporter	NTD	Lillian Pecoraro (NTD Validation Analyst)	78100 - Region 1	10040 - Southeast Area Transit (SEAT)	doc
<input type="checkbox"/>	seat CEO (seat.ceo1@dot.gov)	CEO Delegate	Reporter	NTD	Erik Chadwell (NTD Validation Analyst)	78100 - Region 1	1R06 - Vermont Agency of Transportation (VTrans)	Role Doc

7 Items

Requester Comments
submitting a requested role

My Comments

- 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?”)

Are you sure you want to approve the selected role request?

YES

NO



- 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.

6.3.5 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 unlocking 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**.



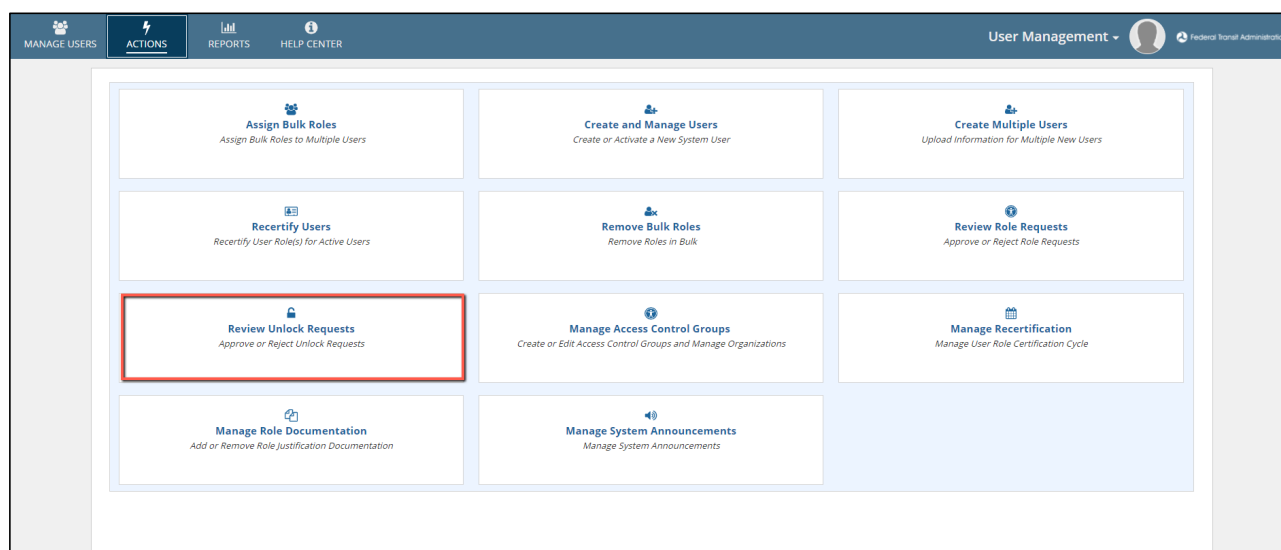
After submitting the **Unlock Request**, the **User Manager (UM)**, **Local Security Manager (LSM)** or **Validation Analyst** will receive an email notification of the unlock request with a hyperlink to review the request. Upon receiving the **Unlock Request**, the **UM, LSM or Validation Analyst** 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
User Type
User

Access Control Group
Cost Center
Organization

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.viewer8@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

- Click **Close** if no action is necessary to return to the **Actions** page. If not;
- Select the link representing the name of the user that needs to be unlocked.
- The **Review Unlock Request** page will display the user's detailed information
- Validate the **User Information** and review the **Request Comments** section.

User Information

Full Name TrAMS Global Viewer
Username demo.trams.tcrlsm@dot.gov

Title Test User
Status Active (Locked)

User Type FTA

Role	Role Category	System	Access Control Group	Cost Center	Organization	Document	Status
Local Security Manager (LSM)	FTA Staff	TrAMS	Office of Civil Rights	68000 - Office of Civil Rights	N/A	N/A	Approved
Budget Analyst	FTA Staff	TrAMS	Office of Budget and Policy	N/A	N/A	N/A	Approved

Request Comments
sunnie needs approval 7/13

Reviewer Comments

Comments entered will be visible on the user's profile in the 'History' dashboard.

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



Request Comments
I just returned from a 3 month leave of absence and now need access to my account.

Reviewer Comments

This unlock request has been verified and approved.

Comments entered will be visible on the user's profile in the 'History' dashboard.

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

Are you sure you want to approve the selected user's unlock request?

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

Unlock In Progress

The decision for the unlock request is being processed. It may take a few minutes for all changes to appear on the user's record. Click the 'Close' button to return to review unlock requests.

- 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.*



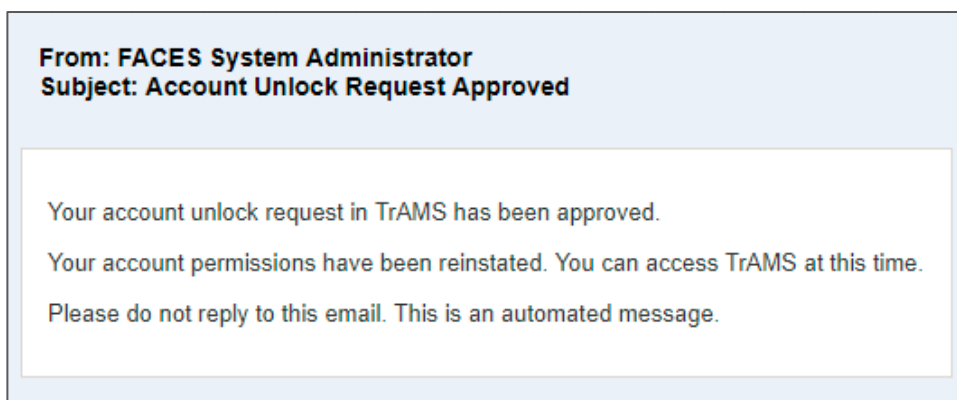
Review Unlock Request

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

Locked User	Username	Request On	Lock Date	Lock Reason
No Data Available				

[CLOSE](#)

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



6.3.6 Related Action: Unlock User

If any user is locked in 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 as long as 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 showing information about the user's account, the reason for the account lock, and the user's unlock request.

Unlock User

User Information

Full Name	Username
Title	Status No Record
User Type	

Lock Information

Lock Reason	Lock Date	Locked By	Comments
Inactivity Lock	10/17/2017 9:29 PM EDT	mpitluck	Inactive for 60+ days

Lock Information

Status	Request Date	User Comments	Reviewer	Reviewer Comments	Review Date
Rejected	10/17/2017 9:40 PM EDT	This is a sample request. Please unlock my account.	mpitluck	TEST	10/3/2017 3:26 PM EDT

Comments

CANCEL

SUBMIT

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

Comments

This unlock request is approved.

CANCEL

SUBMIT

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

Are you sure you want to unlock 10134.ceo1@test.com?

NO

YES



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

Unlock In Progress

The user is being unlocked. It may take a few minutes for all changes to appear on the user's record. Click the 'Refresh' button after a minute to confirm that the user has been unlocked.

CLOSE
REFRESH

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

6.3.7 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**.

Summary User Details User Roles History News Related Actions

⚡ **Edit Profile**
Edit Profile

⚡ **Manage User Roles**
Add or Delete user roles

⚡ **Deactivate User**
Deactivate User Account

Reset PIN
This will reset the user's 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.

Summary User Details User Roles History News **Related Actions**

Reset PIN for adot Primary Reporter

Warning

This will completely remove the user's original PIN, and allow them to enter a new PIN. Please verify that the request is authentic before proceeding.

- 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.

7 Recertification

Recertification is a process that requires 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 users' managers must review and re-certify all users that report to them.

7.1 Recertification Process

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 in order to reinstate their roles. The Certifiers (GSMs, LSMs, User Managers) are required to recertify users with a specific time period, depending on the system. This time period is called the recertification window.

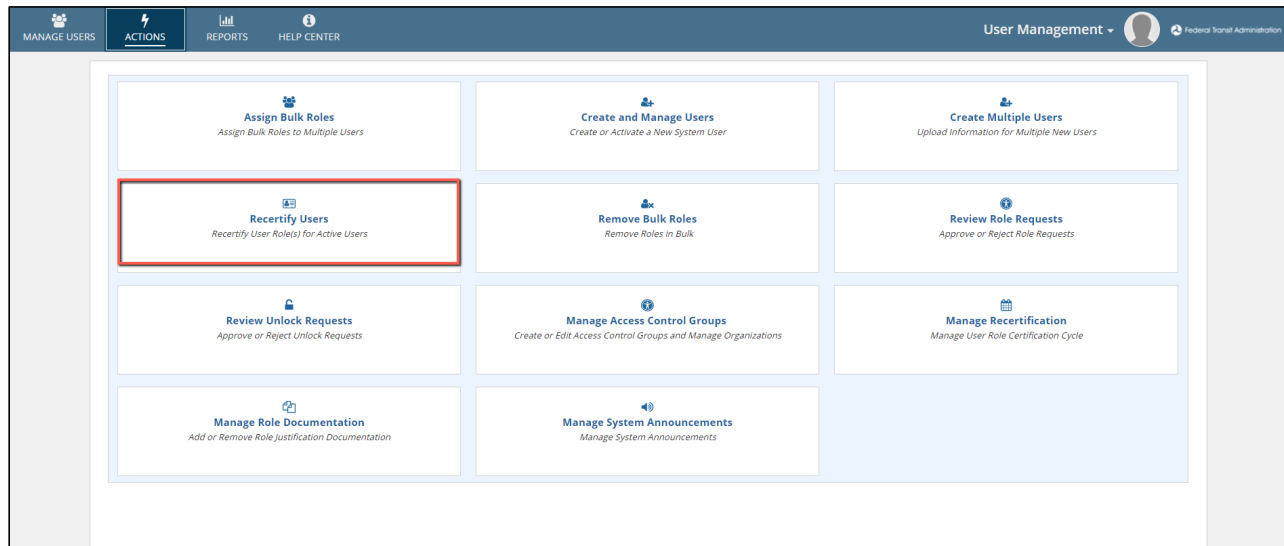
Note: If a user becomes locked, they can self-unlock themselves or submit unlock requests as detailed in Section [7.2](#).

How to recertify a user role:

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



2) Clicks **Recertify Users**.



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

Recertify Users

System Select a System
User Type Select a User Type
Locked ☒ All ☐ Yes ☐ No

Access Control Group Select a Group
Cost Center Select a Cost Center
Organization

Filter users with no User Managers? ☐
CLEAR FILTER(S)

Users Requiring Recertification

Select one or more users to re-certify. Select one user at a time to manage roles.

<input type="checkbox"/>	User	Username	Type	Organization	Locked	Last Login Date	Active?
<input type="checkbox"/>	User Man	azdotuserman@mailinator.com	Organization	1 - Arizona Department of Transportation (ADOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	Test Man	12345testman@mailinator.com	Organization	2 - Arkansas Department of Transportation (ArDOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	NTD UMSupervisor	ntd.umsupervisor	FTA	N/A	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	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	✓
<input type="checkbox"/>	Henry Cooper	henry.cooper	Organization	1334 - Transportation, Connecticut Department Of (CONNDOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	David Manager	david.manager	FTA	N/A	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	NTD Analyst2	ntd.Analyst2	FTA	N/A	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	NTD UMSAnalyst	ntd.UMSAnalyst	FTA	N/A	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	Derek Long	derek.long@mailinator.com	Organization	1353 - Barnstable, County Of (CAPE CODE COM.)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	Frankie Watson	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	✓

1 - 10 of 3,047

CLOSE
GENERATE REPORT



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

A. **System** displays a confirmation message.

Email	Role	Agency
com	NTD Reporter	Viewer
inator.com	NTD Reporter	Editor
inator.com	NTD Reporter	Safety Contact
inator.com	NTD Reporter	Safety Contact
inator.com	NTD Reporter	CEO
inator.com	NTD Reporter	Editor

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

Name	Email	Role	Agency	Status	Date
Sunnie DGSAdmin	sunnie.dgs@sysadmin.com	FTA	N/A	No	9/10/2020 5:00 PM EDT
ripta Viewer	ripta.viewer1@dot.gov	Organization	1R07 - Rhode Island Public Transit Authority (RIPTA)	No	10/6/2020 9:56 AM EDT
ripta Safety Editor	ripta.safetieditor1@dot.gov	Organization	1R07 - Rhode Island Public Transit Authority (RIPTA)	No	10/6/2020 9:56 AM EDT
tpm Local Security Manager LSM	tpm.lsm3@dot.gov	FTA	N/A	No	10/6/2020 9:56 AM EDT
toa Validation PM	toa.validationpm1@dot.gov	FTA	N/A	No	10/6/2020 9:56 AM EDT

Download Link(s)

- 12/28/2021 11:51:32 Recertify Users Export for sunnie.tramsgsm@dot.gov.xlsx
- 12/28/2021 11:25:06 Recertify Users Export for sunnie.tramsgsm@dot.gov.xlsx

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



Users Requiring Recertification

Select one or more users to re-certify. Select one user at a time to manage roles.

<input type="checkbox"/>	User	Username	Type	Organization	Locked	Last Login Date	Active?
<input checked="" type="checkbox"/>	User Man	azdotuserman@mailinator.com	Organization	1 - Arizona Department of Transportation (ADOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	Test Man	12345testman@mailinator.com	Organization	2 - Arkansas Department of Transportation (ArDOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	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	✓
<input type="checkbox"/>	massdot NTD Contact	massdot.ntdcontact1@dot.gov	Organization	12 - Massachusetts Department of Public Utilities (DPU)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	conndot Developer	conndot.developer1@dot.gov	Organization	1 - Arizona Department of Transportation (ADOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	massdot User Manager	massdot.usermanager2@dot.gov	Organization	12 - Massachusetts Department of Public Utilities (DPU)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	Aiden A. Al	aiden.al@mailinator.com	Organization	1 - Arizona Department of Transportation (ADOT) 12 - Massachusetts Department of Public Utilities (DPU)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	Cardamom Roundsworth	cpucPrimary@mailinator.com	Organization	3 - California Public Utilities Commission (CPUC)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	SSOR User Manager	ssor.um1@mailinator.com	Organization	31 - Wisconsin Department of Transportation (WisDOT)	No	10/6/2020 9:56 AM EDT	✓
<input type="checkbox"/>	dpu User Manager	dpu.usermanager1@dot.gov	Organization	12 - Massachusetts Department of Public Utilities (DPU)	No	10/6/2020 9:56 AM EDT	✓

« < 1 - 10 of 74 > »

User Roles

Username	System	Role Category	Role	Access Control Group	Cost Center	Organization	Last Certified Date	Certified?
azdotuserman@mailinator.com	SSOR	SSO	User Manager	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight	1 - Arizona Department of Transportation (ADOT)	12/22/2020	No

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

User Roles

Username	System	Role Category	Role	Access Control Group	Cost Center	Organization	Last Certified Date	Certified?
azdotuserman@mailinator.com	SSOR	SSO	User Manager	SSOR Local Security Managers (LSMs)	74000 - Office of Transit Safety and Oversight	1 - Arizona Department of Transportation (ADOT)	12/22/2020	No

Recertification Comments

Characters Remaining: 4000 / 4000

Document

UPLOAD
Drop file here

Document Name

Characters Remaining: 255 / 255

CLOSE
GENERATE REPORT
MANAGE ROLES
DE-CERTIFY
CERTIFY

- A. Username with user details is displayed on the table
- B. **Certifier** then enters Recertification Comments
- C. Can upload any supporting documentation
- D. Enters 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:



▼ User Roles

Username	System	Role Category	Role	Access Control Group	Cost Center	Organization	Last Certified Date	Certified?
wmata.readonly3@dot.gov	TrAMS	Recipient	Read Only	Region 3	78300 - Region 3	1398 - Washington Metropolitan Area Transit Authority (WMATA)	7/15/2020	No

Recertification Comments

Document

UPLOAD Drop file here

Document Name

Characters Remaining: 4000 / 4000

Characters Remaining: 255 / 255

You may not manage roles for locked users

Please unlock the user prior to managing user roles.

CLOSE

GENERATE REPORT MANAGE ROLES DE-CERTIFY CERTIFY

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

G. can click on the **De-Certify** button:

i. **System** displays a confirmation message.

Decertify Role(s)

Are you sure you want to decertify the roles for the selected users? If the user has no other roles, they will become deactivated.

NO YES

1 - 10 of 19

User Roles

Username	System	Role Category	Role	Access Control Group	Cost Center	Organization	Last Certified Date	Certified?
wmata.readonly3@dot.gov	TrAMS	Recipient	Read Only	Region 3	78300 - Region 3	1398 - Washington Metropolitan Area Transit Authority (WMATA)	7/15/2020	No

Recertification Comments

Document

UPLOAD Drop file here

Document Name

Characters Remaining: 4000 / 4000

Characters Remaining: 255 / 255

You may not manage roles for locked users

Please unlock the user prior to managing user roles.

SE

GENERATE REPORT MANAGE ROLES DE-CERTIFY CERTIFY

i. **Certifier** clicks on Yes button.

ii. 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. System displays a confirmation message.

The screenshot shows the 'User Roles' management interface. A modal dialog box titled 'Certify Role(s)' is displayed in the center, asking for confirmation to certify roles for selected users. The dialog has 'NO' and 'YES' buttons. In the background, a table lists user roles with columns for Username, System, Role Category, Organization, Last Certified Date, and Certified? status. Below the table, there are sections for 'Recertification Comments' and 'Document' upload. At the bottom, there are buttons for 'CLOSE', 'GENERATE REPORT', 'MANAGE ROLES', 'DE-CERTIFY', and 'CERTIFY' (which is highlighted with a red border).

Username	System	Role Category	Organization	Last Certified Date	Certified?
ssor.validationteammember1@dot.gov	SSOR	FTA Staff	Office of Transit Safety and Oversight	7/15/2020	No
ssor.validationteammember1@dot.gov	SSOR	FTA Staff	SSOR Local Security Managers (LSMs)	7/15/2020	No
ssor.validationteammember1@dot.gov	SSOR	FTA Staff	Regional Safety Officer	7/15/2020	No

- i. **Certifier** clicks on Yes button.
ii. 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 as a result 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 as a result 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**



The screenshot shows the FACES Home page. At the top is a blue header with a home icon and the text 'Home'. Below the header is a large banner image featuring a white bus and a person on a train platform. Overlaid on the banner is the text 'Welcome to the Transit Integrated Appian Platform!' followed by 'Current user: System Administrator, FACES' and 'Last Login Date: 10/5/2020 10:25 AM EDT'. Below the banner is a white box with a red border containing a blue padlock icon, the text 'Unlock My Account', and 'Unlock Account or Submit Unlock Request'. At the bottom of this box is a message: 'Your Account has been locked. Please click on "Unlock My Account" to unlock your account.'

- 3) The **System** displays Unlock Account page.
- 4) **User** enters comment and clicks Submit button.

The screenshot shows the 'Unlock Account' form. At the top is the title 'Unlock Account' and a sub-header 'Please select an available option to unlock account.'. Below this is a message: 'You have not set up account security questions. You are only allowed to send a request to your leadership (User Manager or Local Security Manager as appropriate).'. Under the heading 'Options *', there are two radio buttons: 'Send a request to unlock your account' (which is selected) and 'Answer security questions'. Below the options is a text area labeled 'Comment' with the placeholder text 'Enter comment to unlock your account.'. At the bottom of the form are two buttons: 'CANCEL' and 'SUBMIT'.

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.

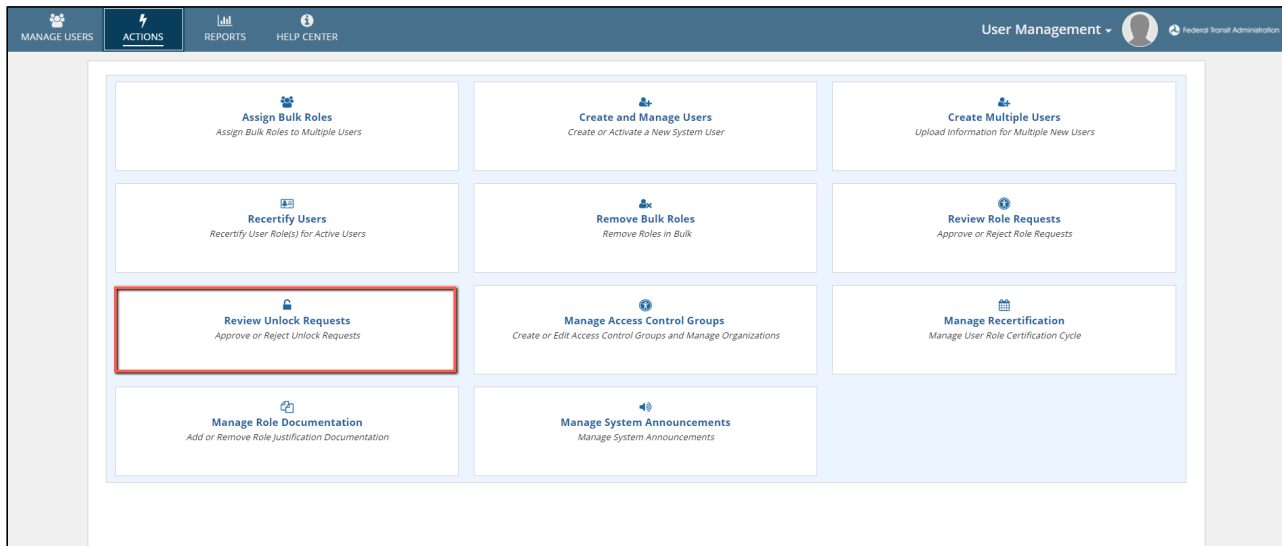
Hint: Alternatively, a certifier can use Unlock related action to unlock locked users. There is no mandate for user to submit unlock request in this case.

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

- 5) **Certifier** logs into System and clicks Actions.

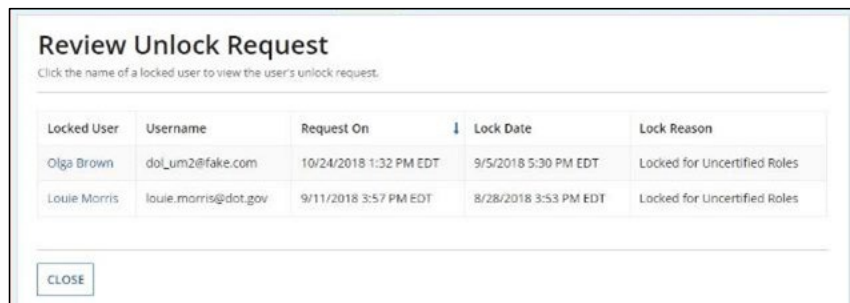


6) **Certifier** clicks **Review Unlock Request**.



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

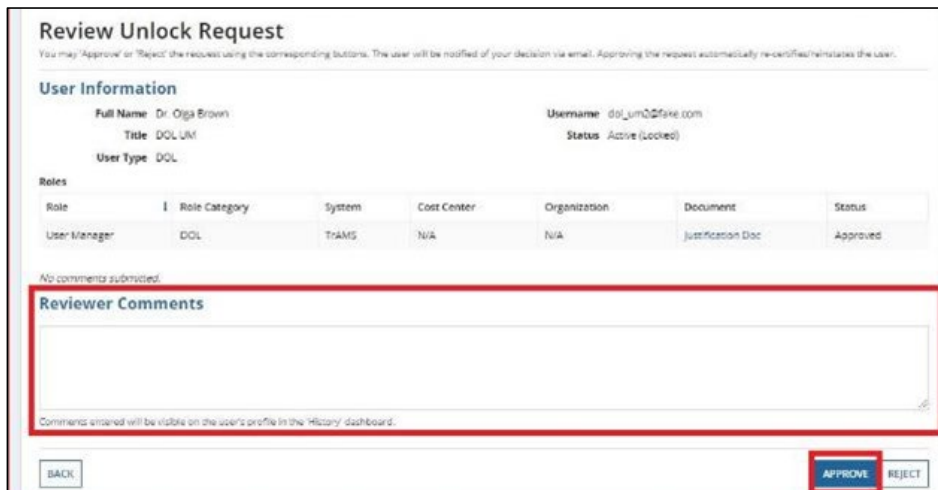
8) **Certifier** clicks on locked user name.



9) **System** displays User information page.

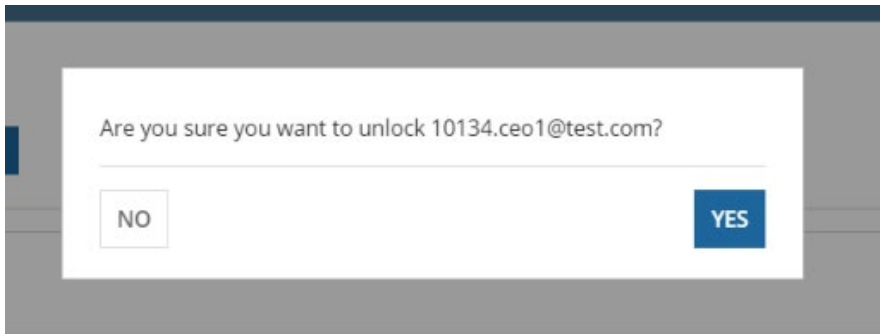
10) **Certifier** may enter text to explain the unlock action in the Reviewer Comments section.

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

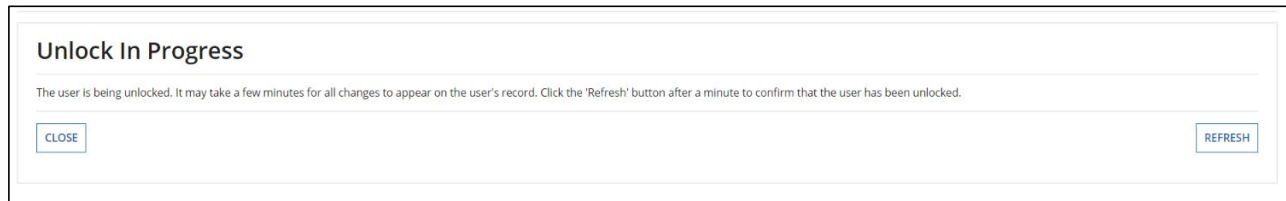




12) In the confirmation screen confirm you want to unlock user.



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



Note:	<i>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.</i>
--------------	---



Appendix A – Abbreviations, Acronyms, and Terms

Acronym	Definition
DOL	Department of Labor
DOT	Department of Transportation
FACES	FTA Access Control and Entry System
FTA	Federal Transit Administration
GSM	Global Security Manager
LSM	Local Security Manager
DGS	Discretionary Grant System
NTD	National Transit Database
TrAMS	Transit Award Management System
SSOR	State Safety Oversight Reporting
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.

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.
 - i) Auditors can only be assigned auditor roles.
 - ii) Contractors can only be assigned contractor roles.
 - iii) DOL Users can only be assigned DOL roles.

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The maximum number of NTD Contacts within a single Reporter organization is one (1).
Editor	<ul style="list-style-type: none"> Multiple users can be assigned the Editor role.
Viewer	<ul style="list-style-type: none"> Multiple users can be assigned the Viewer role. Viewers cannot also be assigned the User Manager role.
Safety Contact	<ul style="list-style-type: none"> The maximum number of Safety Contacts within a single Reporter organization is one (1).
Safety Editor	<ul style="list-style-type: none"> Multiple users can be assigned the Safety Editor role.
Safety Viewer	<ul style="list-style-type: none"> Multiple users can be assigned the Safety Viewer role.
CEO Delegate	<ul style="list-style-type: none"> Multiple users can be assigned the CEO Delegate role. Only CEOs and CEO delegates can assign the CEO delegate role.



TrAMS Rules

TrAMS Recipient Roles	Rules
Read Only	<ul style="list-style-type: none"> The Read Only role cannot be assigned at the same time as any other recipient roles within a single recipient organization.
User Manager	<ul style="list-style-type: none"> The User Manager assignment must be approved by an LSM or GSM.
Submitter	<ul style="list-style-type: none"> The Submitter assignment must be approved by an LSM or GSM. Role assignment requires attachment of Delegation of Authority letter.
Developer	<ul style="list-style-type: none"> No rules apply to this assignment
Official	<ul style="list-style-type: none"> The Official assignment must be approved by an LSM or GSM. Role assignment requires attachment of Delegation of Authority letter.
Attorney	<ul style="list-style-type: none"> The Attorney assignment must be approved by an LSM or GSM. Role assignment requires attachment of Delegation of Authority letter.
Civil Rights	<ul style="list-style-type: none"> No rules apply to this assignment
FFR Reporter	<ul style="list-style-type: none"> No rules apply to this assignment
MPR Reporter	<ul style="list-style-type: none"> No rules apply to this assignment
JPC Procurement Officer	<ul style="list-style-type: none"> 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	Office of Regional Services	Regional 1 Office	Regional 2 Office	Regional 3 Office	Regional 4 Office	Regional 5 Office	Regional 6 Office	Regional 7 Office	Regional 8 Office	Regional 9 Office	Regional 10 Office
	TOA	TAD	TCC	TCA	TPM	TBP	TRI	TCR	TPE	TRS	TRO-1	TRO-2	TRO-3	TRO-4	TRO-5	TRO-6	TRO-7	TRO-8	TRO-9	TRO-10
TrAMS Roles - FTA	61000	62000	63000	64000	65000	66000	67000	68000	71000	78000	78100	78200	78300	78400	78500	78600	78700	78800	78900	79000
Supervisor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local Security Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intake Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pre-Award Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Post-Award Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reservationist	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Director	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Director of Operations	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Initial Reviewer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Technical Reviewer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Environmental Reviewer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Civil Rights Officer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Legal Counsel	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Read Only	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Budget Director	No	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Budget Analyst	No	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Vendor Setup	No	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Apportionment Manager	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Transit Director	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Discretionary Admin	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
TCA Recorder	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
DBE Approver	No	No	No	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Dataset Administrator	No	No	Yes	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No



DGS Rules

DGS Recipient Roles	Rules
Program Admin/Manager	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The Program Admin/Manager with the GSM role must be assigned by an FTA user.
Team Lead	<ul style="list-style-type: none"> Multiple users can be assigned the Team Lead role.
Reviewer	<ul style="list-style-type: none"> Multiple users can be assigned the Reviewer role.

SSOR Rules

SSOR Roles	Rules
Program Management Lead	<ul style="list-style-type: none"> The Program Management Lead role can be held in combination with SSOR GSM role.
GSM	<ul style="list-style-type: none"> The Program Management Lead with the GSM role can create all other users within the SSOR system.
LSM	<ul style="list-style-type: none"> Any of the FTA SSOR role can be conjunction with LSM (example: Validation Lead)
Program Management Team Member	<ul style="list-style-type: none"> Multiple users can be assigned the Program Management Team Member
User Manager	<ul style="list-style-type: none"> User Manager role be held with Primary or Alternate Reporter.



CRM Rules

CRM Roles	Rules
GSM	<ul style="list-style-type: none"> Has access to all FACES functionality to manage, create and recertify global users.
Global Viewer	<ul style="list-style-type: none"> No rules apply to Global Viewer.
FTA User	<ul style="list-style-type: none"> Created by GSM and has only access to reports and view privilege of all the global users.

FACES Rules

CRM Roles	Rules
GSM	<ul style="list-style-type: none"> Has access to all FACES functionality to manage, create and recertify global users.
User Details Report Global Viewer	<ul style="list-style-type: none"> Only has access to User Details, User Deactivation History, and Supervisor Hierarchy reports
FACES Tier-1 Helpdesk Viewer	<ul style="list-style-type: none"> Only has access to User Details, User Deactivation History, Recertification Status, and Supervisor Hierarchy reports
FACES Tier-1 Helpdesk Lead	<ul style="list-style-type: none"> Has access to Manage System Announcements, Send ad-hoc emails, and reports

Appendix C – FTA Cost Centers



FTA is organized into 10 Regional FTA offices and 10 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:

Table 1: FTA Cost Centers

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