FTA

FEDERAL TRANSIT ADMINISTRATION

FTA Transit Award Management System (TrAMS) User Guide

Vol 02, User Access and Management Recipient User Guide

Version 1.0

APRIL 2018

U.S. Department of Transportation
Federal Transit Administration

Contents

1 User Access and Management

1.1 Accessing TrAMS

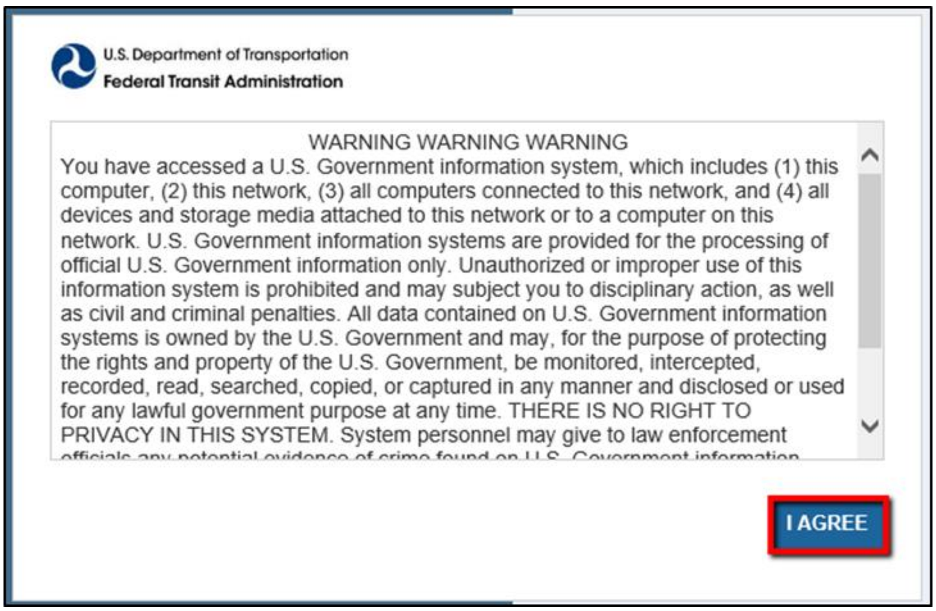
User access to each of the FTA software systems on the FTA platform, https://faces.fta.dot.gov/suite/, such as TrAMS and the NTD, is granted by either an organizational User Manager (UM), Local Security Manager (LSM), or Global Security Manager (GSM) within the appropriate system. An individual with 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, a temporary password, and access/login directions.

1.1.1 Logging into TrAMS

The TrAMS web system may be accessed through a web browser. The standard login method requires a Username and Password. Both are case sensitive.

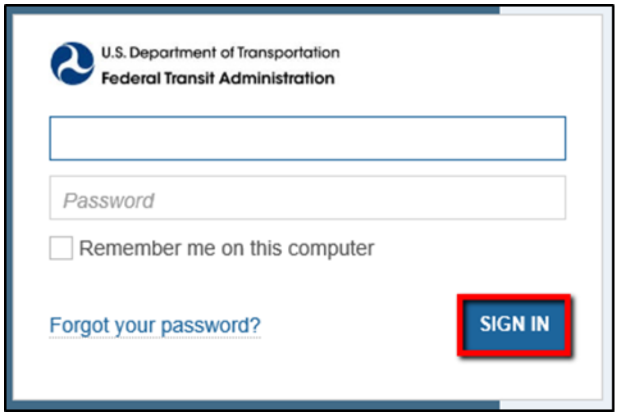
To access TrAMS:

1) Open a web browser and enter the TrAMS web address, https://faces.fta.dot.gov/suite/.



2) Read the security policy and select ‘I AGREE’

3) Enter the appropriate Username and Password



4. Click ‘Sign In’

For more detailed information on accessing TrAMS refer to Section 4 User Access, and Section 4.3.3 New User Login within the FACES User Guide located at http://www.transit.dot.gov/TrAMS.

1.1.1 User Name and Password

In order to log into TrAMS, users need a user name and password. A user’s email address is used in TrAMS as their user name. TrAMS user names and passwords are case sensitive.

New users should contact their organizations ‘User Manager’ in order to obtain access to TrAMS. After the User Manager has added the users contact information into TrAMS the user will receive an email from TrAMS indicating that the account has been created. Users will need to use the ‘Forget Your Password?’ option to initially set their password.

For more detailed step-by-step instructions on the login process (including screenshots) refer to Section 4.3 Logging In within the FACES User Guide.

1.1.2 Passwords

TrAMS will allow you to update or change your password or request a password reset from the login screen. Both new users and users that have forgotten their password should use this option.

For more detailed step-by-step instructions on the login process (including screenshots) refer to Section 4.5 Passwords within the FACES User Guide.

1.2 User Records

1.2.1 Introduction

A User Record includes all information directly related to the user’s Profile (e.g., name, address, title, role(s), and 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 and some user information must be managed by a user’s User Manager(s), Supervisor(s), Local Security Manager(s) (LSMs), and Global Security Manager(s) (GSMs).

For more information on the User Record, refer to Section 3 User Records within the FACES User Guide.

1.2.2 TrAMS User Roles

Each recipient organization will have a User Manager assigned to them and it will be the User Manager's responsibility to assign roles to each user within their organization. Recipient users will be assigned one or multiple roles. The roles assigned to a user control the 'Actions' that a user will have access to and the 'Tasks' that the system assigns to the user. Recipient users are limited to viewing the data for the recipient organizations that the user belongs to.

The following table lists the available user roles that may be assigned to recipient users and the system actions that these roles provide access to.

User Role & Description	Available Actions	Tasks Assigned
Read Only - View only *Note: • The Read Only role cannot be assigned at the same time as any other recipient roles within a single recipient organization.*	• Search Applications/Awards • Search Recipient Organizations • Search FFR and MPR for Review • Search DBE Reports • Application Budget by ALI Report • Application by Status Report • Application Budget Report • Application Discretionary Allocation Detail Report • TrAMS User Detail Report • FFR Detail Report • Recipient POC Detail Report • MPR Detail Report • Project Scope Budget Report • Project Budget Report	N/A
User Manager - Adds, edits, or removes roles and privileges for organization's users; edits agency point of contact (POC) and profile information; deactivates and reactivates users	• ALL Read-Only role actions • Create New User • Create Multiple Users • Recertify User Roles • Review Unlock Requests • Manage Role Documentation	N/A
Submitter - Creates and edits applications and their details; creates, edits, and deletes applications' projects and their details; validates and transmits initial draft applications for FTA review; formally submits applications to FTA for award consideration; implements post-award activities (amendments, budget revisions, and closeouts); adds, edits, and deletes direct recipients and formula	• ALL Read-Only role actions • Create Application	• Submit and Transmit Application • Re-Submit Application • Complete Sub-Allocations

User Role & Description	Available Actions	Tasks Assigned
program sub-allocations (if designated recipient)		
Developer - Creates and edits applications and their details; creates, edits, and deletes applications' projects and their details; validates draft applications (but CANNOT transmit or submit); creates and edits post-award activities (amendments, budget revisions, and closeouts)	• ALL Read-Only role actions • Create Application	
Official - Executes grant/cooperative agreements; certifies (PINs) the annual Certifications & Assurances; adds, edits, and deletes direct recipients and formula program sub-allocations (if designated recipient)	ALL Read-Only role actions	• Execute Application
Attorney - Prepares and submits/uploads recipient legal documents; certifies (PINs) the annual Certifications & Assurances	ALL Read-Only role actions	N/A
Civil Rights - Updates civil rights program compliance and documents; completes and submits DBE reports	ALL Read-Only role actions	• Submit DBE Report • Update DBE Report
FFR Reporter - Prepares and submits Federal Financial Reports	ALL Read-Only role actions	• Complete FFR • Update FFR
MPR Reporter - Prepares and submits Milestone Progress Reports	ALL Read-Only role actions	• Complete MPR • Update MPR

1.2.3 Searching for User Records

Users may view and edit their own profile information and view other users within their organization. You may access your own user record by selecting the 'Profile' option from the silhouette or profile picture at the top right hand corner or by searching within the 'Users' from the 'Records' tab.

1.2.3.1 Profile access from Your User Record

You can access your profile information by clicking on the silhouette or profile picture.

For more detailed step-by-step instructions on accessing your profile information (including screenshots) refer to Section 4.3.4 Accessing Your Record within the FACES User Guide.

1.2.3.2 Searching from the Records Tab

You may find your own or to find other users profile(s) from within your organization from the 'Records' tab in TrAMS.

For more detailed step-by-step instructions on finding other user profiles (including screenshots) refer to Section 6.1 Locating a User Profile from the Record Tab within the FACES User Guide.

1.3 Working with your own Record

1.3.1 Users Summary Page

The Users summary page is the landing page when a user either selects the 'Profile' option at the top right hand corner or they choose themselves or another user from the' Records' tab. This page consists of the users' business card and news items related to the user.

When viewing others users summary pages, users will have the option to select to follow them or to provide them with kudos.

1.3.1.1 Customize Summary Page

Users may customize their page by uploading a background, adding a profile picture, or adding some brief text such as their business title. For more detailed step-by-step instructions on customizing your summary page (including screenshots) refer to Section 5.1 Customizing the User Summary Page within the FACES User Guide.

1.3.1.2 Adding/Changing Profile Picture

Users may select to add or update their profile picture. This profile picture will be associated with the user and will be displayed alongside any posts attributed to them.

For more detailed step-by-step instructions on adding/changing your profile picture (including screenshots) refer to Section 5.1.1 Adding/Changing Profile Picture within the FACES User Guide.

1.3.1.3 Adding/Changing Background

Users may modify the background of their business card. This image will be seen when other users view your summary page.

For more detailed step-by-step instructions on adding/changing the background of their business card (including screenshots) refer to Section 5.1.2 Adding/Changing Profile Background within the FACES User Guide.

1.3.1.4 Follow Users

To automatically see posts attributed to other users, a user may choose to follow others. By following a user their posts will automatically appear in their News feeds. Users may select to follow users from the News tab (Refer to **Error! Reference source not found.**) or from selecting their Profiles.

For more detailed step-by-step instructions on following a user (including screenshots) refer to Section 6.2 Following Another User within the FACES User Guide.

1.3.1.5 Provide Kudos

Kudos is a way to praise another user's work. Kudos will display for a user under their business card on the Users Summary page. Kudos may be provided from the News tab (Refer to Kudos) or by locating the users profile from the 'Records' tab. Kudos will be visible to all users that visit the user's profile page.

For more detailed step-by-step instructions on following a user (including screenshots) refer to Section 6.3 Provide Kudos to Another User within the FACES User Guide.

1.3.2 Viewing User Details

This is a ‘view only’ page; users are able to see their own profiles and the profiles of other users within their organization. User Details are split between multiple pages for legibility: the User Details page, the User Roles page, and the History page.

1.3.2.1 User Details Page

The User Details page consists of two groups of essential information about the user: account information and contact information.

For more detailed step-by-step instructions on viewing the User Details page (including screenshots) refer to Section 6.4.1 User Details Page within the FACES User Guide.

1.3.2.2 User Roles Page

The User Roles page consists of two main parts: a Roles section, and, if applicable, a section listing User Managers for the selected user.

For more detailed step-by-step instructions on viewing the User Roles page (including screenshots) refer to Section 6.4.2 User Roles Page within the FACES User Guide.

1.3.2.3 History Page

The History page contains user audit information. It consists of three sections: Role History, Account History, and Profile History.

For more detailed step-by-step instructions on viewing user’s audit history (including screenshots) refer to Section 6.4.3 History Page within the FACES User Guide.

1.3.3 Related Actions

By selecting ‘Related Actions’ users will be provided with additional options that can be performed on their User Record.

For more detailed step-by-step instructions on viewing a user’s Related Actions (including screenshots) refer to Section 5.2 Related Actions within the FACES User Guide.

1.3.3.1 Related Actions: Edit User Profile

All recipient users can edit their own user profile (name, contact information, and business address) using a profile related action.

For more detailed step-by-step instructions on editing a user profile (including screenshots) refer to Section 5.2.1 Related Action: Edit Profile within the FACES User Guide.

1.3.3.2 Manage User PIN

TrAMS employs a PIN-based system to add security to some of its functions. A four-digit numeric Personal Identification Number (PIN) code, as set by the users themselves, will be required to complete specialized actions only available to specific user roles (Submitter, Attorney, and Official). For a recipient organization, these actions include formally submitting an application to FTA for review as the Submitter, executing an application as the Official, and signing off on Certifications and Assurances as either the Official or Attorney.

1.3.3.3 Create/Update PIN

If the User Manager for your organization elects to add one or more of the PIN-based roles (Submitter, Attorney, and/or Official) to your user record, you will gain access to a new Related Action to set your personal four-digit PIN code.

For more detailed step-by-step instructions on creating or updating your PIN (including screenshots) refer to Section 5.2.4 Related Action: Creating a PIN and Section 5.2.5 Related Action: Changing the PIN within the FACES User Guide.

1.3.3.4 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.

For more detailed step-by-step instructions on setting up security questions and answers (including screenshots) refer to Section 5.2.2 Related Action: Set Security Questions/Answers within the FACES User Guide.

1.3.3.5 Related Action: Manage Security Questions/Answers

Users can update or change their security questions/answers from the Related Action: Manage Security Questions/Answers.

For more detailed step-by-step instructions on changing security questions and answers (including screenshots) refer to Section 5.2.3 Related Action: Manage Security Questions/Answers within the FACES User Guide.

1.3.4 A Locked Account

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 (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 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. Once an account is unlocked, the user's access privileges will be fully restored.

1.3.4.1 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.

For more detailed step-by-step instructions on unlocking your account by answering your security questions (including screenshots) refer to Section 5.3.1 Answer Security Questions within the FACES User Guide.

1.3.4.2 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.

For more detailed step-by-step instructions on unlocking your account by submitting an unlock request (including screenshots) refer to Section 5.3.2 Submit Unlock Request within the FACES User Guide.

1.4 User Manager Responsibilities

Each organization will have one or more users that have been assigned the 'User Manager' role. As a User Manager for an organization a user is able to:

- Create new users
    - Assign user roles
- Create multiple users
- Review user role request
- Manage role documentation
- Review unlock requests
- Update existing user records
    - Edit user profile information
    - Deactivate users
    - Reactivate users
    - Manage user roles
    - Unlock users
- Recertify user roles

For more detailed information about user management responsibilities refer to Section 7.1 User Management Responsibilities within the FACES User Guide.

1.4.1 Action: Create New User

User Managers have access to the Action 'Create New User'. This action allows the User Manager to add new users for their recipient organization(s).

For more detailed step-by-step instructions on creating a new user (including screenshots) refer to Section 7.2.1.1 Organization and External Users within the FACES User Guide.

1.4.1.1 Assigning User Roles

Users are assigned roles during the user creation process. The User Manager adds roles based on a user's access and permissions. Security rules govern which types of roles can be added or removed from a user.

For more detailed step-by-step instructions on assigning and managing user roles (including screenshots) refer to Section 7.3.2. Related Action: Manage User Roles within the FACES User Guide.

1.4.2 Action: Create Multiple Users

If more than one user needs to be created for a recipient organization the User Manager may "bulk load" users into the system through the use of a CSV (Comma Separated Values) file.

For more detailed step-by-step instructions on the bulk upload process (including screenshots) refer to Section 7.2.3 Create Multiple Users within the FACES User Guide.

1.4.3 Role Requests

Some roles added by User Managers require elevated approvals (Submitter, Official, and Attorney). When these roles are added, a role request is generated and a request to review the role is sent to the user's LSM.

For more information on how role requests are reviewed (including screenshots) refer to Section 7.3.5 Action: Review Role Requests within the FACES User Guide.

1.4.4 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. 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.

For more detailed step-by-step instructions on uploading role documentation (including screenshots) refer to Section 7.2.2 Action: Manage Role Documentation within the FACES User Guide.

1.4.5 Action: Review Unlock Requests

User accounts are automatically locked after 60 days of user inactivity. Users who are locked out will still be able to log into TrAMS but their access will be severely restricted. User Managers may review unlock requests for users in their organization.

For more detailed step-by-step instructions on reviewing unlock requests (including screenshots) refer to Section 7.3.6 Action: Review Unlock Request s within the FACES User Guide.

1.4.6 Updating Existing User Records

Once a user has been created, users with the User Manager role are able to manage details for existing users in their organization including: managing the users' profiles, updating their user roles/privileges, and assigning User Manager privileges. Users may be deactivated from the Users Record, and deactivated users may be reactivated as well.

For more information on managing user records refer to Section 7.3 Managing User Records within the FACES User Guide.

1.4.6.1 Related Action: Edit User Profile

User Managers may edit the user profile using the Related Action: Edit User Profile.

For more detailed step-by-step instructions on editing the user profile (including screenshots) refer to Section 7.3.1 Related Action: Edit User Profile within the FACES User Guide.

1.4.6.2 Related Action: Deactivate User

User Managers may deactivate a user using the Related Action: Deactivate Users.

For more detailed step-by-step instructions on deactivating users (including screenshots) refer to Section 7.3.3 Related Action: Deactivate Users within the FACES User Guide.

1.4.6.3 Related Action: Reactivate User

User Managers may reactivate users using the Related Action: Reactivate Users.

For more detailed step-by-step instructions on reactivating users (including screenshots) refer to Section 7.3.4 Related Action: Reactivate Users within the FACES User Guide.

1.4.6.4 Related Action: Manage User Roles

User roles must be assigned at the time of user creation and may be updated at any time by selecting the 'Manage User Roles' related action. Each user may be assigned multiple roles.

For more detailed step-by-step instructions on managing user roles (including screenshots) refer to Section 7.3.2 Related Action: Manage User Roles within the FACES User Guide.

1.4.6.5 Related Action: Unlock User

If a locked user has submitted an unlock request, an additional related action will become available on the user's record, Unlock Account. This related action allows a User Manager to unlock a user directly from the user's profile. It is intended as a backup method of unlocking an account.

For more detailed step-by-step instructions on unlocking a user (including screenshots) refer to Section 7.3.7 Related Action: Unlock User within the FACES User Guide.