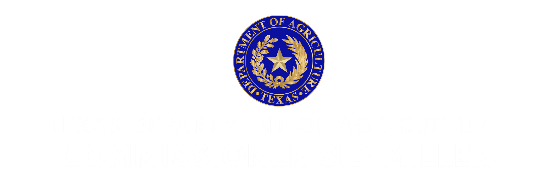
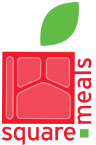
A picture containing icon

Description automatically generated

**TX-UNPS**

**USER ACCESS MANAGER**

**HANDBOOK GUIDE**



Updated 3/21/2024

www.SquareMeals.org

Food and Nutrition Division

Nutrition Assistance Programs

Fraud Hotline: 1-866-5-FRAUD-4 or 1-866-537-2834 | P.O. Box 12847 | Austin, TX 78711

Toll Free: (877) TEX-MEAL | For the hearing impaired: (800) 735-2989 (TTY)

This product was funded by USDA.

This institution is an equal opportunity provider.

Table of Contents

[Introduction iii](#_Toc85178488)

[User Access Manager Expectations iii](#_Toc85178489)

[Covered in this Guide iv](#_Toc85178490)

[Security Request Forms vi](#_Toc85178491)

[1.0 Logging into TX-UNPS 8](#_Toc85178492)

[1.1 Viewing the Training Video Link 8](#_Toc85178493)

[1.2 Logging In 8](#_Toc85178494)

[1.3 User Main Screen 9](#_Toc85178495)

[2.0 Adding a New User 10](#_Toc85178496)

[2.1 Viewing the Training Video Link 10](#_Toc85178497)

[2.2. Adding a User 10](#_Toc85178498)

[3.0 Modifying/Updating a User 15](#_Toc85178499)

[3.1 Viewing the Training Video Link 15](#_Toc85178500)

[3.2 Modifying/Updating a User 15](#_Toc85178501)

[4.0 Resetting User Password 18](#_Toc85178502)

[4.1 Viewing the Training Video Link 18](#_Toc85178503)

[4.2 Resetting User Password 18](#_Toc85178504)

[5.0 Deactivating/Activating Users 21](#_Toc85178505)

[5.1 Viewing the Training Video Link 21](#_Toc85178506)

[5.2 Deactivating User 21](#_Toc85178507)

[5.3 Viewing the Training Video Link 24](#_Toc85178508)

[5.4 Activating a User 24](#_Toc85178509)

[6.0 Unlock User Accounts 29](#_Toc85178510)

[6.1 Viewing the Training Video Link 29](#_Toc85178511)

[6.2 Unlock User Accounts 29](#_Toc85178512)

[7.0 Using the Search and Filter 32](#_Toc85178513)

[7.1 Viewing the Training Video Link 32](#_Toc85178514)

[7.2 Filtering User Status 32](#_Toc85178515)

[FAQs and Troubleshooting 35](#_Toc85178516)

[Security Groups 36](#_Toc85178517)

[School Nutrition Programs (SNP) Groups 36](#_Toc85178518)

[Child and Adult Care Food Program (CACFP) Groups 37](#_Toc85178519)

[Summer Food Service (SFSP) Groups 37](#_Toc85178520)

[Food Distribution Program (FDP) Groups 38](#_Toc85178521)

[Appendix Page 39](#_Toc85178522)

[Resources 39](#_Toc85178523)

[Abbreviations and Acronyms (Most Commonly Used) 39](#_Toc85178524)

[Definitions 40](#_Toc85178525)

[Food Distribution Program Users 40](#_Toc85178526)

[Helpful Information 41](#_Toc85178527)

[Recommended Internet Browsers 41](#_Toc85178528)

[Sharing of Login Information 41](#_Toc85178529)

[Avoiding/Resolving TX-UNPS Session Conflicts 41](#_Toc85178530)

[TX-UNPS Password Lockout 41](#_Toc85178531)

[Resetting Your Password 41](#_Toc85178532)

# Introduction

Texas Department of Agriculture (TDA) implemented the User Access Manager (UAM) to streamline the processing of the Texas Unified Nutrition Program System (TX-UNPS) security access for each Contracting Entity (CE) user.

Implementing a UAM means a quicker turnaround time for adding new users or modifying existing user access within TX-UNPS. This would greatly reduce the downtime for staff waiting for the appropriate access to be completed. It will also reduce the risk for inappropriate user access as the UAM should know when staff are no longer working for the entity or have changed job duties. It may also assist with managing separation of duties between staff and being able to identify a user to serve as a backup to critical TX-UNPS roles.

The UAM will be responsible for the following tasks within TX-UNPS:

* Adding new user access
* Modifying existing user access
* Resetting user passwords
* Deactivating/Reactivating user accounts
* Unlocking user accounts after too many password attempts

This handbook will cover each task with a step-by-step instruction and a training video link. The UAM is responsible for all security access provided and managed for each user associated to your CE. Therefore, it is important to be familiar with the tasks and security groups covered in this handbook.

*This Standard Operating Procedure (SOP) will be the same for all School Nutrition Programs.*

## User Access Manager Expectations

Part of the UAM responsibility is to understand the different security groups as they pertain to the roles within your entity. The security groups are based on the type of role – Application, Claims, Compliance, and Read-Only.

NOTE: If your CE has an agreement with a Food Service Management Company or participates in the Food Distribution Program, the UAM may also be responsible for users within these groups.

* Application allows a user to create, modify, and submit applications for a particular program.
* Claims allows a user to create, modify, and submit claims for a particular program.
* Compliance allows a user to view and submit a Corrective Action Documents response for a particular program.
* Read-Only allows a user to view all screens as it related to application, claims, and compliance for a particular program.

The security groups are explained in more detail in the [Security Groups section](#_Security_Groups) of this manual. It is important to understand what type of access/data you will be providing to users especially data that may include personal identifiable information. Security access is based on the program(s) for which your CE participates and what access is provided to you as the UAM by TDA.

It is expected that you will not disclose information that is considered confidential under TDA policy and understand that User IDs and passwords are specific to the user and should not be shared. **Each user accessing TX-UNPS should have their own User ID/password.** Sharing login information is considered a security violation and improper use of TX-UNPS which may result in the CE being disqualified from program participation and all user rights revoked.

Even though notification to TDA is not needed when adding or modifying a user, it is suggested that you keep a record of the action. You may create a “form” to be used in-house that will assist in your record keeping. TDA has included an example template in the [Appendix section](#Updates) of this manual which can be used, if desired. Please keep in mind that all records and information resources are the responsibility of the CE and may be subject to audit review.

## Covered in this Guide

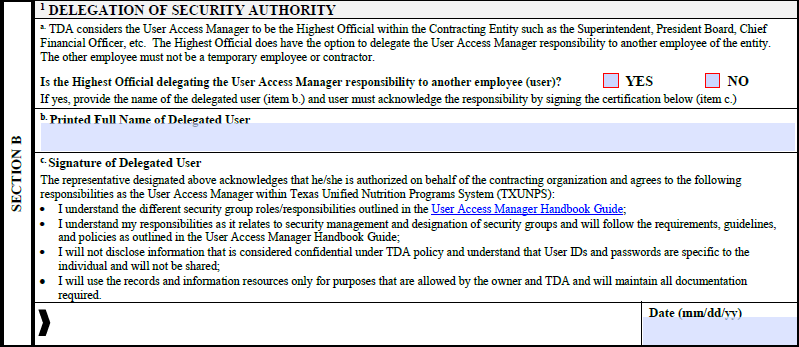
* A step-by-step process for each of the six tasks listed.
* Screen shots of the process taken straight from TX-UNPS.
* A link to training videos showing each task being completed using the steps provided in this manual.
* Complete description list of all security group types.
* Troubleshooting questions and some quick fixes to common issues encountered.
* Helpful TX-UNPS information.

# Security Request Forms

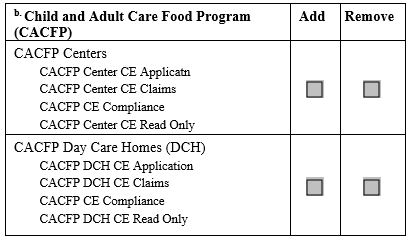
TDA considers the User Access Manager (UAM) to be the Highest Official within the Contracting Entity such as the Superintendent, President Board, Chief Financial Officer, etc. **Only two UAMs will be established at a time within each CE.**

The Security Authority for User Access Manager (FND-135) form must be completed and submitted to TDA. The FND-135 form will provide information on the UAM and indicate the security groups that pertain to the program the CE is participating. The form will be provided to the CE upon approval of participating within a program or can be requested from (877) TEX-MEAL.

The Highest Official does have the option to delegate the security responsibility to another user within the CE. The delegated user must be an employee of the CE and not a temporary employee or contractor. To delegate the security authority to another user, Section B of the FND-135 form must be completed by selecting “Yes” and completing the employee’s name and signature.



When selecting the security groups on the FND-135 form, only select the programs that are applicable to your CE. For example, if you participate in the CACFP Day Care Homes (DCH) program, you will only select that section. All security groups within that program (those listed under the type) will be included. The UAM will have all the security groups to allow for the groups to be assigned to users as needed.



If your CE elects to participate in a new program, the FND-135 form must be completed again to have the new program security groups added to the UAM account. For example, your CE participates in CACFP Day Care Homes (DCH) and wishes to participate in SFSP as well. Once TDA has approved the pre-eligibility for SFSP, a new FND-135 form must be submitted for the SFSP security groups to be added to the UAM.

The following items require additional handling:

* If your CE decides to no longer participate in a particular program, security access for the users and UAM must be completed in a certain order. Contact TDA at (877) TEX-MEAL for further directions.
* If your CE participates in the Food Distribution Program and has an agreement with an external entity, additional forms must be submitted to TDA for processing. Refer to [Food Distribution Program Users](#_Food_Distribution_Program) of this manual for further information.

Every CE is allowed to have two UAM. If any UAM is no longer employed with the CE, a new FND-135 form must be submitted to remove security access of the previous UAM and appoint a new UAM. The Highest Official can delegate a different user to act as the UAM, as desired. ***Access for the other users at the CE will not be terminated but CE cannot continue to update security rights for existing users or add new users without removing access for previous UAM.***

As a reminder, users (including the UAM) MUST log into TX-UNPS once every 120-days or their access may be deactivated for lack of activity. If the user’s account is deactivated, the UAM will have to reactivate the account. If the UAM’s account is deactivated, a new FND-135 form will be required in order to establish a new account for the UAM. This is especially important for Texas Eligibility List Management System (TX ELMS) users as they can sign in directly to TX ELMS. If the user does not sign into TX-UNPS every 120-days, their access to TX ELMS may be deactivated.

# 1.0 Logging into TX-UNPS

## 1.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TX-UNPS_LoggingOn/story.html) to view the training video on Logging into TX-UNPS.

## 1.2 Logging In

Follow the steps listed below to get to the login screen for TX-UNPS:

* Search for [Squaremeals.org](http://www.squaremeals.org/) in your URL or click the link
* Once the page has opened, scroll down until you find the **Quick Links** section
* Click on the **Accessing TX-UNPS** hyperlink
* Add the log on page to your Favorites list for future use

|  |  |
| --- | --- |
| **Steps** | **Here’s How** |
| 1. Log in to ***TX-UNPS.*** | NOTE: If you have not received your User ID and Password, contact TDA at (877) TEX\_MEAL.   * Enter your User ID and your Password. * Click the “Log On” button. |
| 1. Navigate to **CE Systems Logins** screen | * Click the “Security” link on the top menu bar. * Click the “CE System Logins” link under the Item list.     To access the UAM screen, log in through the CE Systems Logins on SNP, CACFP, or SFSP modules. |

## 1.3 User Main Screen

This is the UAM’s main page. From here you can make all the modifications needed for any user’s account within the TX-UNPS.

Here is a list and explanation of some of the areas that we will be talking about today.

1. Security Groups – a list of the security groups assigned to the UAM and can be given to users.
2. The search field— ability to filter or narrow down a search by a user’s name or status (Pending, Active, or Inactive)
3. Details link— this link will take you to the user’s detail page. You can make your updates or changes to the user’s status, name, security group, etc.
4. UAM Key– this key will only be present next to a person who is delegated as the User Access Manager.
5. Lock Symbol– this symbol identifies all the users who have user account locked. This happens when the user has entered the incorrect password more than 5 times.
6. User ID– the User ID will be established when the user account is created. This ID is system generated and unique for every person.
7. Status– this identifies the current status of each user (Active, inactive, or pending).

|  |  |
| --- | --- |
| UAM Main Page consists of the following:   1. Security Groups 2. Search Field 3. Details Link 4. UAM Key 5. Locked Account 6. USER ID 7. Status   From this screen, you can make modifications, changes, updates or add new users to the TX-UNPS system. |  |

# 2.0 Adding a New User

## 2.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) for a link to view the training video on adding a new user into TX-UNPS.

## 2.2. Adding a User

After completing the following steps, you should be able to successfully Add a New User in TX-UNPS. All steps MUST be completed as the User ID may not be generated correctly.

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Click on ***Add User*** | * Navigate to the CE System Logins screen and click the “Add User” link. |
| 1. Enter the User’s Information | * Enter the user’s full Name, Title, Email Address, and Phone Number. * Select Yes or No if the user is an administrator for MENU. * Click the “Save” button.   **All items with an \* are required.** |
| **Note:** If you have entered the user by mistake, click the X at the top right to cancel and delete the new entry. This must be done prior to clicking on Save. | |
| 1. Update the Security Groups. | * After saving the user information, the Security Group section will automatically populate. * Select ONLY the groups that the new user will need to complete their job duties. * Click the “Save” button. |
| After you have **selected** and **saved** the security groups, the system will automatically bring you back to the user’s detail page.    You can see at this point the User ID and Status are Not Assigned and Pending as shown in the User Login section.  The User will not have a User ID assigned until the following steps are completed. | |
| 1. Generate the User ID | * Within the User Login section, click the “Edit” button. * Next, click the “Generate” button to obtain a User ID.      * The system will generate the User ID in TDA format. Once generated, the User ID cannot be changed.      * Click the “Save” button. |
| After the User ID has been generated, the User Login section on the Details screen will be updated with the User ID and Status. This means the account is now ready.    Once the account is established, an email is sent to the user to set/reset their password.  **Note: UAM and the user will receive notifications to generate a User ID if account remains in pending status. Pending accounts will be removed from system after 30 days.** | |
| 1. Email notification | * Verify with the user they have received the email. * User should click the link to set/reset their password.   **NOTE: if the user does not log in within a few days, the account will be locked and have to be reset again.** |
| 1. User creates password | * User will create a new password following the requirements shown for a new password. |
| Whenever you make any updates or changes to someone's profile, you should always add a Note. Adding a note every time will assist you when trying to see the User’s history. | |
| 1. Add a Note | * On the Details page, click the “Add Note” button. * Add a note about adding a new member along with the date.      * Click “Save” button. |
| 1. Navigate back to main UAM screen | * Once the user’s information is completed in the system, you will be shown the Details screen for the user. Click the “Back” button. * You will be directed back to the UAM CE Systems Logins. |
| **END of Training** | **Congratulations!** You have added a new user as this was the final step. |

# 3.0 Modifying/Updating a User

## 3.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) to view the training video on modifying/updating a user.

## 3.2 Modifying/Updating a User

After completing the following steps, you should be able to successfully modify and update a user’s profile and security groups.

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Click Details. | * Navigate to the CE System Logins screen and click the “Detail” link next to the user to be updated. |
| **Editing the User’s Profile**   1. Edit user information. | * On the User section, click the “Edit” button. This will bring up the profile screen. |

| **Steps** | **Here’s how** |
| --- | --- |
| 1. Update the information. | * Update the user’s Name, Title, Email Address, and Phone as needed. * Once all updates are completed, click the “Save” button. |
| **Editing the Security Groups**   1. Edit the Security Groups. | * On the Security Groups section, click the “Edit” button. This will bring up the list of security groups available. |
| 1. Update the groups. | * Update the security groups as needed by placing a check or unchecking the box under “Has Group”. * Once all updates are completed, click the “Save” button. |

|  |  |
| --- | --- |
| **Steps** | **Here’s how** |
| Whenever you make any updates or changes to someone's profile, you should always add a Note. Adding a note every time will assist you when reviewing the User’s history. | |
| 1. Add a Note | * On the Details page, click the “Add Note” button. * Add a note about the updates made along with the date.      * Click “Save” button. |
| 1. Navigate back to main UAM screen | * Once the user’s information is completed in the system, you will be shown the Details screen for the user. Click the “Back” button. * You will be go back to the UAM CE Systems Logins. |
| **END of Training** | **Congratulations!** You have updated the user account as this was the final step. |

# 4.0 Resetting User Password

## 4.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) to view the training video on resetting a user’s password.

## 4.2 Resetting User Password

If a user has forgotten their password, you will be able to reset it. After completing the following steps, you should be able to successfully reset a user’s password

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Click Details. | * Navigate to the CE System Logins screen and click the “Detail” link next to the user to be updated. |
| 1. Reset password | * On the User Login section, click the “Reset Password” button. |
| 1. Email notification | * Once the button is clicked, an email will automatically be sent to the user with a link allowing them to reset their password.   NOTE: You may need to contact the user notifying them of the email. |
| 1. User creates password | * User will create a new password following the requirements shown for a new password. |
| Whenever you make any updates or changes to someone's profile, you should always add a Note. Adding a note every time will assist you when trying to see the User’s history. | |
| 1. Add a Note | * On the Details page, click the “Add Note” button. * Add a note about the updates made along with the date.      * Click “Save” button. |
| 1. Navigate back to main UAM screen | * Once the user’s information is completed in the system, you will be shown the Details screen for the user. Click the “Back” button. * You will be directed back to the UAM CE Systems Logins. |
| **END of Training** | **Congratulations!** You have reset a user’s password as this was the final step. |

# 5.0 Deactivating/Activating Users

## 5.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) to view the training video on deactivating a user

## 5.2 Deactivating User

Deactivating a user’s account should be completed immediately upon the user leaving the entity or permanently changing positions. The account will still be in the system for historical purposes but will be in an inactive status.

Aside from a user leaving the entity or changing positions, a user’s account can be inactivated if the user does not log into TX-UNPS within 120 days. The system will automatically deactivate the account.

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Click Details | * Navigate to the CE System Logins screen and click the “Detail” link next to the user to be deactivated. |
| 1. Deactivate account | * Under the User Login section, notice the Status is currently “Active”. * Click the “Deactivate User” button. |
| 1. Status changed | * The account is now reflecting a Status of “Inactive”. The account is no longer active in TX-UNPS.   NOTE: The user will not receive a notice indicating the account has been deactivated. If they attempt to sign into TX-UNPS, they will receive an error message. |
| Whenever you make any updates or changes to someone's profile, you should always add a Note. Adding a note every time will assist you when trying to see the User’s history. | |
| 1. Add a Note | * On the Details page, click the “Add Note” button. |
| 1. Enter the note details. | * Add a note about the updates made along with the date. * Click “Save” button. |
| 1. Navigate back to main UAM screen | * Once the user’s information is completed in the system, you will be shown the Details screen for the user. Click the “Back” button. * You will be directed back to the UAM CE Systems Logins. Since the account is now inactive you will need to update the Search filter to include those accounts.      * Select the “Inactive” box and click “Search”. * Now you will see the user that has been deactivated. |
| **END of Training** | **Congratulations!** You have deactivated the user account as this was the final step. |

## 5.3 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) to view the training video on activating a user.

## 5.4 Activating a User

There are several occasions when you may need to activate a user as opposed to creating a new user account. They are:

1. If a user departed the position (did not leave the entity) and is now returning to their position, they will already be in the system and will just need to be reactivated.
2. If a user has not logged in for over 120 days, the system will automatically change their status to inactive.

As the 120 days approaches, multiple email notifications will be sent to the user indicating their account is going to expire. It would be best to work with the user to ensure they keep their account active to avoid having to reactivate their account.

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Click Details   Since the user is Inactive, you will need to update the Search filter to include those accounts. | * Navigate to the CE System Logins screen and select the “Inactive” box on the Search section. Click “Search”. * Click the “Detail” link next to the user to be activated. |
| 1. Activate the account | * Under the User Login section, click the “Activate User” button. |
| 1. Status changed | * The account is now reflecting a Status of “Active”. |
| After activating a user’s account, you will need to review and update the security groups for the user. This will ensure they still require/contain the most current security groups for their job position. | |
| 1. Edit the Security Groups. | * On the Security Groups section, click the “Edit” button. This will bring up the list of security groups available. |
| 1. Update the groups. | * Update the security groups as needed by placing a check or unchecking the box under “Has Group”. Click “Save”. |
| More than likely, the user will not remember their old password; therefore, it would be best to reset their password. | |
| 1. Reset password | * On the User Login section, click the “Reset Password” button. * An email will automatically be sent to the user with a link allowing them to reset their password. The user will then create a new password following the requirements. |
| Whenever you make any updates or changes to someone's profile, you should always add a Note. Adding a note every time will assist you when trying to see the User’s history. | |
| 1. Add a Note | * On the Details page, click the “Add Note” button. |
| 1. Enter the note details. | * Add a note about the updates made along with the date. * Click “Save” button. |
| 1. Navigate back to main UAM screen | * Once the user’s information is completed in the system, you will be shown the Details screen for the user. Click the “Back” button. * You will be directed back to the UAM CE Systems Logins. |
| **END of Training** | **Congratulations!** You have activated the user account as this was the final step. |

# 6.0 Unlock User Accounts

## 6.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) to view the training video on unlocking a user account.

## 6.2 Unlock User Accounts

When viewing the Main UAM Screen, at times a Lock symbol may be displayed next to someone’s account. The Lock means that the user has had five unsuccessful attempts at logging into the system. Often, the user can wait 15 minutes and retry again. If that does not work, you may need to assist by removing the lock on the account and resetting their password.

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Click Details | * Navigate to the CE System Logins screen and notice the lock image next to a user’s name. * Click the “Detail” link to unlock their account. |
| 1. Deactivate account | * Under the User Login section, click the “Unlock User” button. |
| 1. Account unlocked | * The account no longer is locked. |
| Since the account was locked, it is more than likely, the user does not remember their old password. Therefore, it would be best to reset their password. | |
| 1. Reset password | * On the User Login section, click the “Reset Password” button. * An email will automatically be sent to the user with a link allowing them to reset their password. The user will then create a new password following the requirements. |
| Whenever you make any updates or changes to someone's profile, you should always add a Note. Adding a note every time will assist you when trying to see the User’s history. | |
| 1. Add a Note | * On the Details page, click the “Add Note” button. |
| 1. Enter the note details. | * Add a note about the updates made along with the date. * Click “Save” button. |
| 1. Navigate back to main UAM screen | * Once the user’s information is completed in the system, you will be shown the Details screen for the user. Click the “Back” button. * You will be directed back to the UAM CE Systems Logins. |
| **END of Training** | **Congratulations!** You have unlocked the user account as this was the final step. |

# 7.0 Using the Search and Filter

## 7.1 Viewing the Training Video Link

[Click here](https://tdafn.s3.amazonaws.com/Articulate/TXUNPS_UserAccessManagerTraining/story.html) to view the training video on Filtering a User’s Status.

## 7.2 Filtering User Status

The following steps will assist the UAM when trying to narrow down your search by a name or status. It is extremely helpful when there are several users.

| **Steps** | **Here’s how** |
| --- | --- |
| **Complete steps 1.1 Log-In prior to beginning this section.** | |
| 1. Selecting the Search Filters | * Navigate to the CE System Logins screen and notice the criteria available in the Search section. |
| 1. Filter only Active user | * Deselect the “Pending” and “Inactive” buttons in the Status area. * The results will only display users that are in an “Active” status. |
| 1. Filter only Pending users | * Deselect the “Active” and “Inactive” buttons in the Status area. * The results will only display users that are in an “Pending” status.   NOTE: Pending status indicates the user has not been assigned a User ID. Refer to 2.0 Adding a New User. |
| 1. Filtering only Inactive users | * Deselect the “Active” and “Pending” buttons in the Status area. * The results will only display users that are in an “Inactive” status. |
| 1. Filter by name | * Ensure all of the Status’ are selected (Pending, Active, Inactive). * Type a name of the person searching within the Filter field. All users with that name will be displayed. |
| **END of Training** | **Congratulations!** You have successfully used the search filter as this was the final step. |

# FAQs and Troubleshooting

Here are some examples of some issues you may be asked as a UAM. We have included some simple ways to fix them.

|  |  |
| --- | --- |
| **Question** | **Answer** |
| I am a UAM but I cannot find the CE System Logins tab (Main UAM Screen), am I missing something? | Yes, you might not have all the UAM rights, contact the TDA Customer Service Hotline at the TEXMEAL line (877-TEX-MEAL (839-6325)) to get your profile updated. |
| If I participate in multiple programs, do I need to go into each of the programs to make changes to a user’s profile? | No, once you click on the Security tab from any available program, this will cover all the different programs. |
| Do I need to make a Note each time I’m viewing someone’s details? | No, notes are used to assist you when trying to determine why a change was done. Only make comments when making updates to the user. |
| I cannot view someone who is Inactive but I can see the Pending or Active users, do I need to update my profile? | No, you need to select the Inactive box within the Search filter. |
| How do I view user’s status? | The last column on the CE System Logins page displays the Status for all the users. |
| Is there a way to only view users with an Active status? | Yes, deselect the Pending and Inactive boxes on the Search filter. |
| Do I need to delete a user when they leave the department? | No, just change their status to Inactive. |
| What can I do if the user isn’t receiving any emails with the log in information? | Verify the user’s email on their account. If incorrect, make the correction. You may need to reset their password. |
| Do I need to submit documentation to TDA when I update or add a user? | No, all documentation should be kept within the CE. Only the Security Authority to User Access Manager (FND-135) form must be submitted to TDA. |

# Security Groups

## School Nutrition Programs (SNP) Groups

|  |  |
| --- | --- |
| Security Group | Description |
| SNP CE Application | User who has edit access to application-related screens, including food safety inspections, verification, capital expenditures, Texas summer mandate, summer cost reporting, community eligibility provision (CEP), financial reporting, annual audit, Meal Pattern Compliance Dashboard, Attestation, and Menus. |
| SNP CE Claims | User who has edit access to claim-related screens, including Seamless Summer Option and Fresh Fruit and Vegetable, if applicable. User also has view access to summer mandate, summer cost reporting, and financial reporting. |
| SNP Compliance | User who has edit access to compliance screens as it relates to forms and corrective action document findings. User also has view access to compliance-related screens, including financial reporting. |
| SNP Read Only | User who has view only access to all application, claims, and compliance-related screens. |
| ELMS CE Admin | User who has access to the direct certification and direct verification processing. |
| FSMC Representative | User who is designated by the Contracting Entity as a Food Service Management Company (FSMC) employee operating under an approved FSMC contract.  User who has view only access to all application-related screens, including Meal Pattern Compliance Dashboard, Attestation, and Menus. User also has edit access to the Food Safety Inspections. |
|  |  |
|  |  |

## Child and Adult Care Food Program (CACFP) Groups

|  |  |
| --- | --- |
| Security Group | Description |
| CACFP Center CE Application | User who has edit access to application screens related to Centers, including advance requests and annual audit. |
| CACFP Center CE Claims | User who has edit access to claim screens related to Centers. User also has view only access to advance requests. |
| CACFP Center Read Only | User who has view only access to all application, claim, and compliance screens related to Centers. |
| CACFP DCH CE Application | User who has edit access to application screens related to Day Care Homes, including advance requests and annual audit. |
| CACFP DCH CE Claims | User who has edit access to claim screens related to Day Care Homes. User also has view only access to advance requests. |
| CACFP DCH Read Only | User who has view only access to all application, claim, and compliance screens related to Day Care Homes. |
| CACFP Compliance | User who has edit access to compliance screens as it relates to corrective action document findings for either Centers or Day Care Homes, if applicable. User also has view access to compliance-related screens. |

## Summer Food Service (SFSP) Groups

|  |  |
| --- | --- |
| Security Group | Description |
| SFSP CE Application | User who has edit access to application-related screens, including advance requests and annual audit. |
| SFSP CE Claims | User who has edit access to claim-related screens, including annual audit. User also has view only access to advance requests. |
| SFSP Compliance | User has edit access to compliance screens as it related to corrective action document findings. User also has view access to other compliance-related screens. |
| SFSP CE Read Only | User who has view only access to all application, claim, and compliance-related screens. |

## Food Distribution Program (FDP) Groups

|  |  |
| --- | --- |
| Security Group | Description |
| NSLP / SFSP | (For CEs who receive USDA Foods through a state-contracted warehouse and/or whose processing requests are managed by a Coop Coordinator.) User who has edit access to FDP-related contract, survey, and Contracting Entities order screens for both NSLP and SFSP and read-only access to allocations and entitlement screens. Note: This is only for CEs participating in either SNP or SFSP. |
| Direct Ship School | (For CEs who receives USDA Foods directly from USDA.) User who has edit access to FDP-related contract, survey, and Contracting Entities order screens for both NSLP and SFSP and read-only access to allocations and entitlement screens. Note: This is only for CEs participating in either SNP or SFSP and have a Direct Ship Agreement with TDA. |
| CSFP / TEFAP CE | User who has edit access to FDP related application, contract, inbound shipment, surveys, allocations, entitlement, and inventory and claim screens for TEFAP and CSFP. |
| FMNP/SFMNP CE | User who has edit access to FMNP/SFMNP related application, contract and claim screens |

# Appendix Page

## Resources

* User Access Manager Resources

<https://squaremeals.org/FandNResources/TXUNPSProgramResources/TXUNPSUserAccessManager.aspx>

* TX-UNPS Resources by Program

<https://squaremeals.org/Programs.aspx>

* Square Meals

<http://www.squaremeals.org/>

## Abbreviations and Acronyms (Most Commonly Used)

CACFP—Child and Adult Care Food Program

CE—Contracting Entities

DCH—Day Care Home

ELMS—Eligibility List Management System

FDP—Food Distribution Program

FMNP—Farmer’s Market Nutrition Program

FSMC-- Food Service Management Company

SFMNP—Senior Farmer’s Market Nutrition Program

SFSP—Summer Food Service Program

SNAP—Supplemental Nutrition Assistance Program

SNP—School Nutrition Program

TANF—Temporary Assistance to Needy Families

TDA—Texas Department of Agriculture

TX-UNPS—Texas Unified Nutrition Program System

UAM—User Access Manager

USDA—United States Department of Agriculture

## Definitions

**Activating:** Process of changing a user’s current status within the TX-UNPS system from Inactive to Active.

**Adding a New user:** This is required if a new member will be working with the TX-UNPS system. If an employee is returning to the same position, they will already be in the system and will just need to be reactivated.

**Deactivating:** Process of changing a user’s current status within the TX-UNPS system from Active to Inactive. This is required when a person leaves the position and no longer requires access to the system. Also, the system will automatically deactivate an account after 120 days of no activity.

**Filtering:** Refining the search menu to display the users within a particular status.

**Modifying a user:** Making changes to a user’s account due to corrections or updates. Just as an example, these changes could be anything from a name change, phone number change, or security status update.

**Unlocking:** Users of the system will be locked out of TX-UNPS after 5 failed login attempts.  The UAM will be able to unlock the user’s account.

## Food Distribution Program Users

The following FDP users are not managed by the UAM and will continue to request updates through the appropriate forms to TDA.

* Processors – submit the Security Authority for FDP Processors (FND-137)
* Warehouses – submit the Security Authority for FDP Processors (FND-138)
* Processing Co-Op Coordinators – submit the Certificate of Authority for External Users (FND-101)

# Helpful Information

## Recommended Internet Browsers

* TX-UNPS recommends browsers to be Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari (Apple computers only).

## Sharing of Login Information

* TX-UNPS authorized users must not share their assigned User ID and password with any other employee of the Contracting Entity (CE). Each user accessing TX-UNPS should have their own User ID/password. Sharing of log in information is considered a security violation and improper use of TX-UNPS which may result in the CE being disqualified from program participation and all user rights revoked.

## Avoiding/Resolving TX-UNPS Session Conflicts

* TX-UNPS does not allow users to sign in through multiple tabs or windows in the same environment. If a user attempts it, a session conflict will occur and must be resolved by the user. The instructions for resolving session conflicts can be found at <https://squaremeals.org/FandNResources/TXUNPSProgramResources/TXUNPSResourcesandTraining.aspx>.

## TX-UNPS Password Lockout

* Users of the system will be locked out of TX-UNPS after 5 failed login attempts. Once a lock-out has occurred, users are required to wait 15 minutes before attempting to log in again. Users may utilize the *“Forgot Your Password?”* feature as needed.

## Resetting Your Password

* Click the *"Forgot Your Password?"* link on the Log-On screen to have temporary password automatically generated and emailed to you. If you do not receive the email, check your Junk Mailbox. If further assistance is needed, please call 1-877-TEX-MEAL (839-6325).

REMINDER: When resetting your password, your new password must be at least 10 characters long and contain at least one number, one upper-case character and one special character such as # % & $ \* !.

***Updates to Security Access for TXUNPS***

*EXAMPLE*

**IMPORTANT: Users must log into TX-UNPS every 120 days or the account will deactivate.**

|  |  |
| --- | --- |
| sec A | **ACTION** |
| **ADD NEW USER  MODIFY EXISTING USER  UPDATE USER INFORMATION  DEACTIVATE USER** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SECTION B** | **USER INFORMATION** | | | | |
| **First Name** (Legal names only, no nicknames) | **Middle Initial** | | **Last Name** | |
| **Title** | **TX-UNPS User ID** | | | |
| **Business E-mail** | | **Business Phone**  (       )       - | | **Extension** |
| **Update User Information – Type of Change Requested:**  Title  Business E-mail  Business Phone | | | | |

|  |  |  |
| --- | --- | --- |
| **SECTION C** | **TX-UNPS SECURITY GROUPS TYPE** | |
| |  |  |  | | --- | --- | --- | | **School Nutrition Programs (SNP)** | **Add** | **Remove** | | SNP CE Applications |  |  | | SNP CE Claims |  |  | | SNP CE Compliance |  |  | | SNP CE Read-Only |  |  | | ELMS CE Admin |  |  | | Food Service Management Company (FSMC) Representative |  |  |  |  |  |  | | --- | --- | --- | | **Summer Food Service (SFSP)** | **Add** | **Remove** | | SFSP CE Application |  |  | | SFSP CE Claims |  |  | | SFSP CE Compliance |  |  | | SFSP CE Read-Only |  |  | | |  |  |  | | --- | --- | --- | | **Child and Adult Care Food Program (CACFP)** | **Add** | **Remove** | | CACFP Center CE Application |  |  | | CACFP Center CE Claims |  |  | | CACFP Center CE Read-Only |  |  | | CACFP Day Care Home (DCH) CE Application |  |  | | CACFP Day Care Home (DCH) CE Claims |  |  | | CACFP Day Care Home (DCH) Read-Only |  |  | | CACFP CE Compliance |  |  |  |  |  |  | | --- | --- | --- | | **Food Distribution Program (FDP)** | **Add** | **Remove** | | FDP NSLP / SFSP |  |  | | FDP Direct Ship School |  |  | | CSFP / TEFAP CE |  |  | | FMNP/SFMNP CE |  |  | |

|  |  |  |
| --- | --- | --- |
| secTION d | **USER ACCESS MANAGER** | |
| **Action Completed:** | |
| **User Access Manager Signature** | **Date (mm/dd/yy):** |
| **Notes** | |