

Security Overview



USER ACCESS MANAGER

(UAM)



USER ADMIN

(UA)



TEXAS DEPARTMENT OF AGRICULTURE
COMMISSIONER SID MILLER

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)



Food and Nutrition Division
Nutrition Assistance Programs

This product was funded by USDA.
This institution is an equal opportunity provider.



Updated 3/28/2024
www.SquareMeals.org

Security Basics

Contracting Entity administration of security access differs between Texas Unified Nutrition Program System (TX-UNPS) and Web-Based Supply Chain Management (WBSCM) system. However, there are more guidelines that apply to both systems.

- A Contracting Entity can have a maximum of 2 user administrators/managers in each system.
- The user administrator/manager must be approved by TDA.
- The user administrator/manager must be employed by the CE.
- The user administrator/manager must not be a temporary, contract, FSMC representative, or a Cooperative Coordinator.

| TX-UNPS | WBSCM |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>User Access Manager (UAM)</i> | <i>User Admin (UA)</i> |
| Security Authority for User Access Manager (FND-135) Form | Security Authority for WBSCM User (FND-136) Electronic Form |
| | |
| UAM Permissions | UA Permissions |
| <ul style="list-style-type: none"> • Add new users (except another UAM) • Modify existing user's information and security permissions • Deactivate existing users • Reset password and unlock user accounts | <ul style="list-style-type: none"> • Add new users (except another UA) • Modify existing user's information and security permissions • Deactivate existing users • Unlock user accounts • Resend new user registration email for initial setup |

User Administrator/Manager Assignment

TX-UNPS

- By default, the Highest Official of the entity is considered the UAM. However, the official does have the option to delegate the UAM responsibility to another employee.
- Complete the Security Authority for User Access Manager (FND-135) form and submit it to TDA.
 - Only UAM assignment requires an FND-135; all other users will be created/updated by the UAM.
 - Highest Official can delegate the UAM responsibility by completing Section B of the form.

WBSCM

- The UA is assigned by completing the Security Authority for WBSCM User (FND-136) electronic form. TDA will review and process the electronic form.
 - Each UA assignment requires an FND-136; all other users will be created/updated by the UA.
- A UA has the technical ability to assign UA rights to another user due to WBSCM system constraint. However, TDA requires an approved FND-136 form each UA. Therefore, admin access will be removed for any assigned UA without an approved FND-136 form on record.

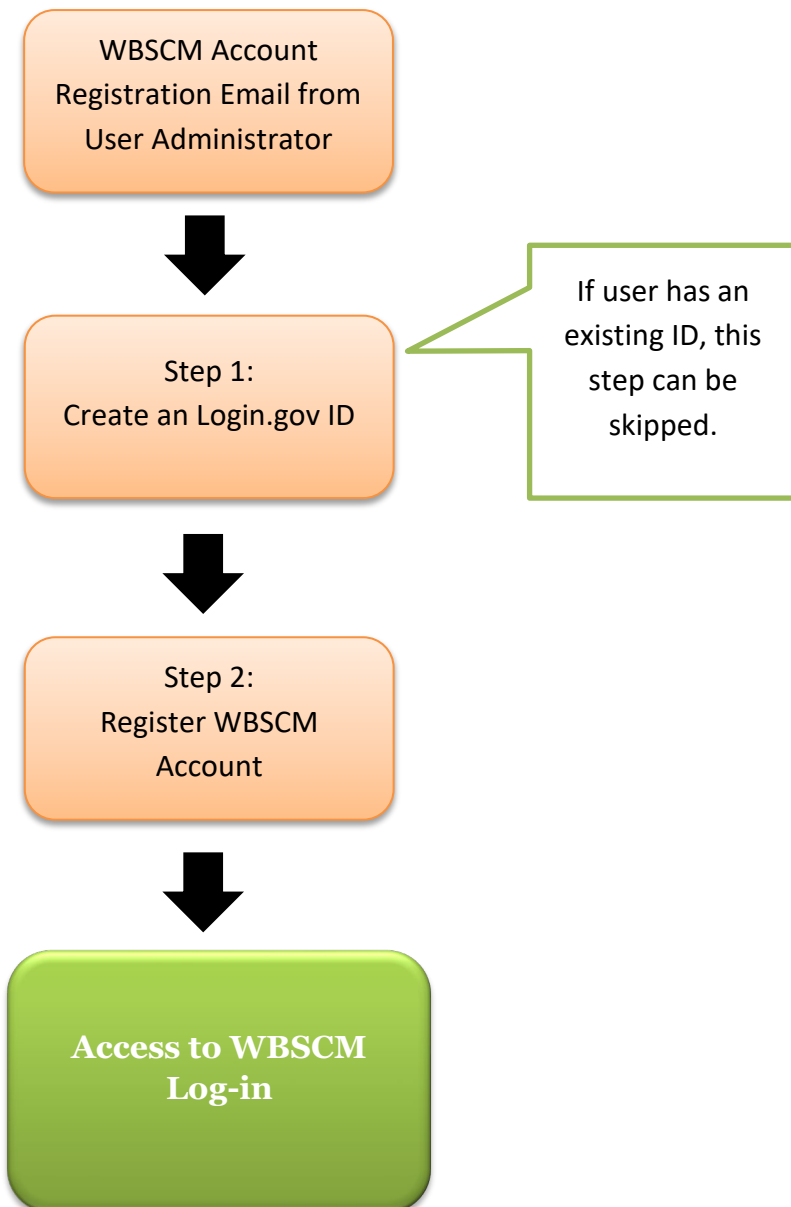
Each entity can have a maximum of 2 user administrator/managers at a time.

- If a user administrator/manager leaves the entity, all users' access continues as normal.
- A new security form is needed to assign a new user administrator/manager.
- If an entity does not have any user administrator/manager assigned, one must be assigned prior to any updates to existing users or adding of new users.

WBSCM Account Registration Process

USDA requires each user to have an eAuthentication ID (eAuth) registered through their system. The eAuth account is used for all USDA web application such as FFAVORS and is also linked to the WBSCM account.

Once the UA adds a user to WBSCM, an email is sent to the user to complete a two-step registration process prior to accessing WBSCM. If the user does not receive the email, the UA can resend it manually in the Manage Users window.



Helpful Hints

| TX-UNPS | WBSCM |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> Each user accessing TX-UNPS should have their own User ID/Password. Sharing login information is considered a security violation and improper user of TX-UNPS which may result in an entity being disqualified from program participating and all user rights revoked. | |
| <ul style="list-style-type: none"> Adding a New User is a 3-part process – User Information, Security Groups and Generating the User ID. The last step is generally missed and the user is placed in a “Pending” status. The account is not set up until the User ID is generated by the UAM. When resetting a password, the new password must meet all criteria as listed including at least 10 characters long and contain at least one number, one upper-case character and one special character. If all green checkmarks are not received, then the password cannot be reset. When your password is changed, TX ELMS does take 24 hours until the password is updated in the DCDV system. It is best to clear all previously saved passwords in TX ELMS prior to entering the new password. | <ul style="list-style-type: none"> The Security Authority for WBSCM Users (FND-136) electronic form must be approved by the Highest Official at the entity. The UA must setup the user in WBSCM first to generate the eAuthentication email from USDA. When a new account is setup, the eAuthentication process must be completed within a certain number of days. Otherwise, the UA may have to resend the email notification again to the user. The UA can generate a User Security Report to view their entity user’s security access to assist with managing the roles and responsibilities. |



CE Systems Login Screen

The CE Systems Login screen is used by the UAM to manage their users. The screen is accessible through SNP, CACFP, and SFSP modules on [TX-UNPS](#) and will display all users for all programs. For the Food Distribution Program, the UAM only provides access to TEFAP, CSFP, FMNP and SFMNP users. All other programs are managed through WBSCM.

| Item | Description |
|------------------|------------------------------------|
| Change Password | Change Password for Logged-In User |
| User Manager | User Manager |
| CE System Logins | Contracting Entity System Logins |

The CE System Login screen consists of several different areas:

1. **Security Groups** – list of the security groups assigned to the UAM which can be assigned to users.
2. **Search** – ability to filter by a user’s name or status (Pending, Active, or Inactive).
3. **Add User** – For UAM use only. Allows UAM to add a new user account (3 step process).
4. **UAM Key** – key to identify user who is delegated as the User Access Manager.
5. **Lock Symbol** – identifies whether user’s account is locked after too many password attempts.
6. **Details** – For UAM use only. Allows UAM to update the user’s account information.
7. **User ID** – displays User ID associated to user.
8. **Last Login** – displays when the user last logged into TX-UNPS which can assist in monitoring to avoid the 120-day deactivation process.
9. **Status** – identifies the current status of the user.

Contracting Entity System Logins

00654 Status: Active
BEAUMONT ISD
 DBA:
 3395 Harrison
 BEAUMONT, TX 77706-5009
 County District Code: 123-910
 ESC: 5 TDA Region: 3

| Security Groups | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------|-------------------|
| SNP MENU CE Support Staff MENU CE Support Admin ELMS CE Admin SNP CE Read-Only SNP CE Compliance SNP CE Claims SNP CE Application | CACFP CACFP CE Compliance CACFP Center CE Read-Only CACFP Center CE Claims CACFP Center CE Applicatn | SFSP SFSP CE Read-Only SFSP CE Compliance SFSP CE Claims SFSP CE Application | FDP FDP CE Administration | No Program |

Search

Filter: Status: Pending Active Inactive

| Users | | | | | | | | |
|--------|-----|------|------------|-----------|-------------|----------------|------------|--------|
| Action | UAM | Lock | First Name | Last Name | User ID | Phone Number | Last Login | Status |
| Detail | | | Tiffany | Eckenrod | TEckenrod10 | (409) 617-5065 | 01/28/2020 | Active |
| Detail | | | Delois | Harris | DHarris12 | (409) 617-5067 | 08/11/2019 | Active |
| Detail | | | Nytisha | Keys | NKEYS | (409) 617-5071 | 01/23/2020 | Active |
| Detail | | | | Lewis | BLewis12 | (409) 617-5069 | 01/23/2020 | Active |
| Detail | | | | Mendoza | MMendoza13 | (409) 617-5062 | 11/13/2019 | Active |



Manage Users Screen

The Manage Users screen is used by the UA to manage their users. It is accessible at <https://portal.wbscm.usda.gov/> through Admin > Manage Users > Manage Users link in WBSM.

The Manage Users screen consists of several different areas:

1. **Report Incident** – ability to submit a ticket to USDA on an issue with the system.
2. **Admin > Manage Users** – section for user administrator to view users.
3. **Manage Users** – allows UA to view users and create or update users.
4. **User Security Report** – report to view all users information including roles assigned.
5. **Active Organization** – entity organization name.
6. **Search** – ability to search for a user by Last Name and First Name.
7. **User Information** – list of users within the entity including the Last Logon Date.
8. **Create New User** – link to create a new user.

The screenshot shows the WBSM Manage Users interface. At the top, there is a navigation bar with the USDA logo, 'United States Department of Agriculture', 'Web Based Supply Chain Management', and the WBSM logo. A search bar and links for 'New Session', 'Report Incident', and 'Log off' are also present. Below the navigation bar, there are tabs for 'Home', 'Admin', 'Reports', and 'Help'. The 'Admin' tab is selected, and the 'Manage Users' sub-tab is active. The main content area is titled 'Welcome to Manage Users' and contains two sections: 'Organization Selection' and 'User Selection'. The 'Organization Selection' section has a search criteria field and a list of active organizations, with one organization 'A.TDA Test Live - R03' highlighted. The 'User Selection' section has a search criteria field and a table of users. The table has columns for 'First Name', 'Last Name', and 'Last Logon Date'. A 'Create New User' button is located below the table. Numbered callouts (1-8) point to various elements: 1 points to the 'Report Incident' link, 2 points to the 'Admin' tab, 3 points to the 'Manage Users' sub-tab, 4 points to the 'User Security Report' link, 5 points to the active organization list, 6 points to the search criteria field in the 'User Selection' section, 7 points to the user table, and 8 points to the 'Create New User' button.

| First Name | Last Name | Last Logon Date |
|------------|-----------|---------------------|
| Jane | Doe | 2024-01-24 10:28:50 |
| | | |
| | | |
| | | |