MCO PRISM Access Management

Purpose: This Standard Operating Procedure (SOP) outlines the MCO Provider User Administrator responsibilities and functionality.

RESPONSIBILITIES OF THE PROVIDER USER ADMINISTRATOR: The EXT MCO Provider User Administrator profile is considered privileged access for the purpose of user management. This profile will be initially assigned to the user(s) designated by the MCO. This profile has the responsibility of approving all new users for the Plan's domain, maintaining user information in the system, maintaining appropriate access documentation, performing periodic activity reviews, and removal of access.

This Standard Operating Procedure (SOP) covers the following procedures:
- User Utah-ID and password
- User completes the PRISM MCO Provider User Access Agreement
- Provider User Administrator Functionality

ACCESS TO PRISM DOMAINS

I. USER UTAH-ID AND PASSWORD

A UtahID is required for access to PRISM. Individuals may already have a UtahID if they accessed MMCS in the past. For help with password recovery or creating a new UtahID visit https://idhelp.utah.gov/ .

In order to access the PRISM Provider Portal, providers will need a Utah-ID password that meets the following standards:
- At least eight characters in length
- Passwords must have a combination of letter, numeric digits, and special characters
- Passwords must include at least one character from three of the following attributes:

- o Uppercase characters (A-Z)
- o Lowercase characters (a-z) o Numeric Characters (0-9)
- o Special Characters (i.e:!, @, #, $, %, ^, &, *,)

If the Utah-ID password created by the user does not meet these standards, users will be forced to change their password to gain access to PRISM.

II. USER COMPLETES THE MCO PROVIDER USER ACCESS AGREEMENT

The MCO Provider User Administrator is responsible for obtaining a completed MCO Provider Access Agreement for all staff given access to PRISM.   The Administrator is required to save the completed form for 6 years.   The CMS access control standard below explains the requirements for authorization forms and administrators for systems containing PII/PHI.
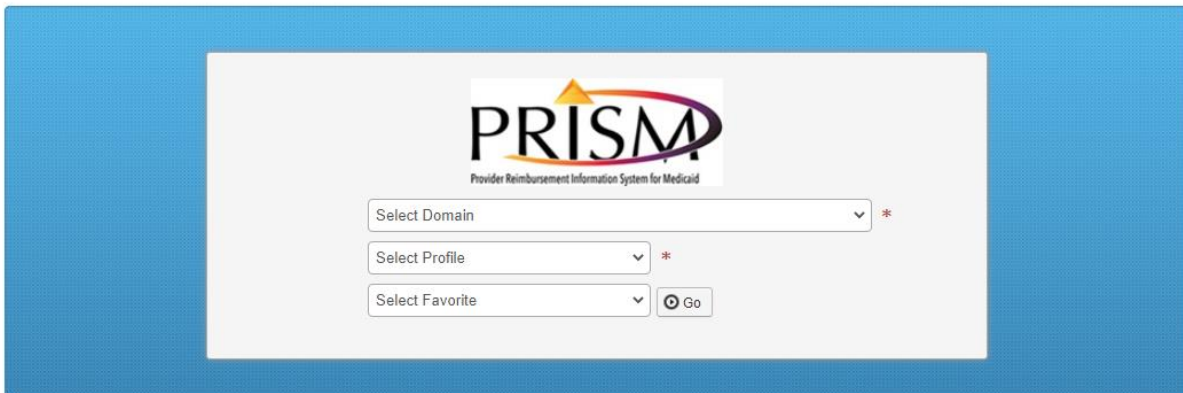
AC-2: Account Management

Implementation Standards

1. Remove or disable default user accounts. Rename active default accounts.
2. Implement centralized control of user access administrator functions.
3. Regulate the access provided to contractors and define security requirements for contractors.
4. Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.
5. Prohibit use of guest, anonymous, and shared accounts for providing access to PII.
6. Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties.
7. Implement access controls within the IS based on users' or user group's need for access to PII in the performance of their duties.
8. Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.
9. Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for each user to complete privacy training every 365 days otherwise the account would be disabled.
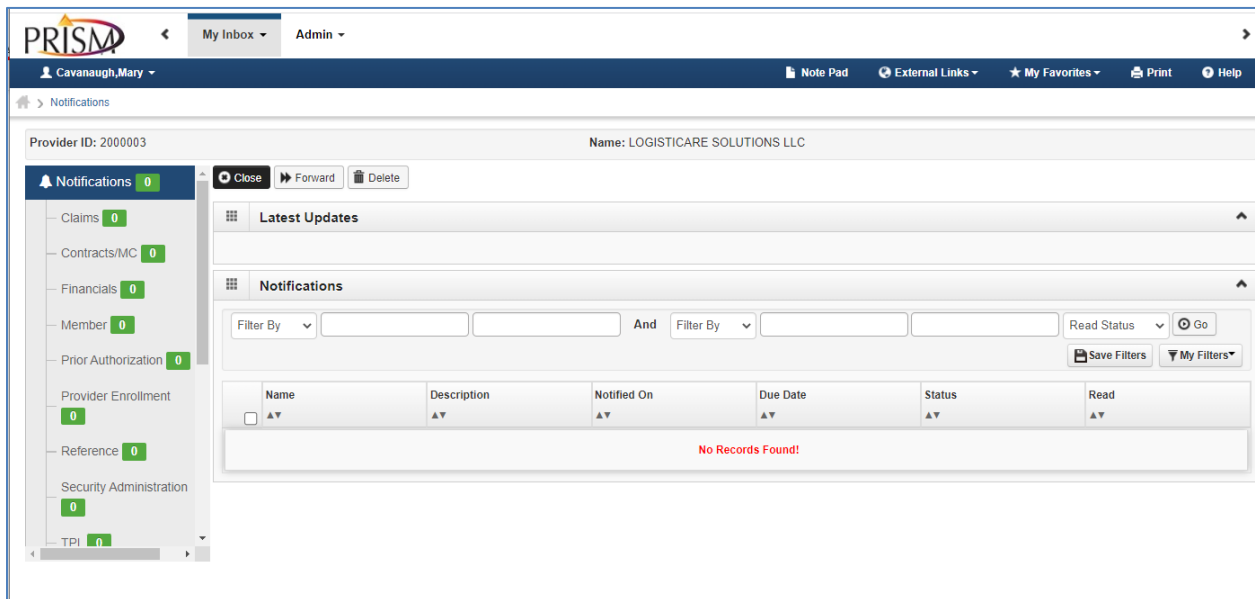
MCO PROVIDER USER FUNCTIONALITY

The following section covers the EXT MCO Provider User Administrator profile ability to add a user and assign profiles, modify a user, and review user access activity.

I. Add a User

Once you have the new user's User Access Agreement (UAA) and UtahID, log into the PRISM Portal

1. Select Domain from the dropdown.

    - The "Domain" is the PRISM enrollment record and includes the Plan Name, PRISM ID, and the word MCO. You may have multiple domains. Ensure that you are selecting the correct domain for the access needed.

2. Select Profile "EXT MCO Provider User Administrator" from the dropdown.
    - The "Profile" determines what screens and functionality you will have in PRISM. You may have multiple profiles depending on what access the MCO Administrator has authorized.

3. Click Go
    - The My Inbox will display

- The banner at the top will list the areas of functionality the selected profile has access to.   The "EXT MCO Provider User Administrator" profile has access to My Inbox and Admin

4. Select the User List from the Admin dropdown.
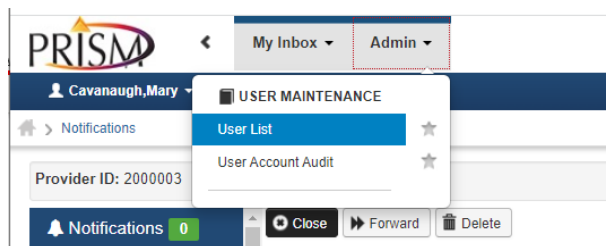
5. The User List will display. From this page you can Add a user as well as review existing users.
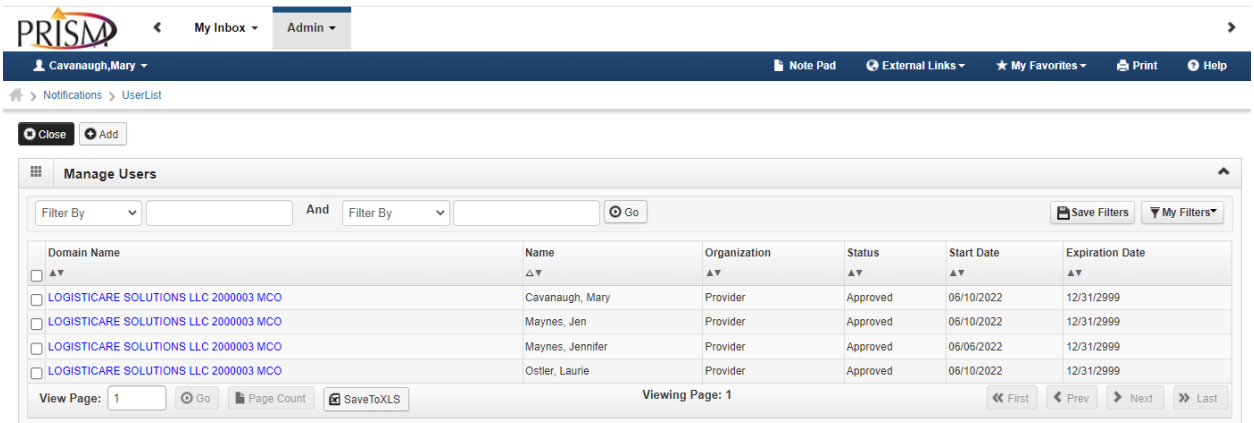
- From the User List page, the MCO Admin can add new users and modify existing users.

6. Click the ⊕ Add add user button.
    - The Add Provider User page will open
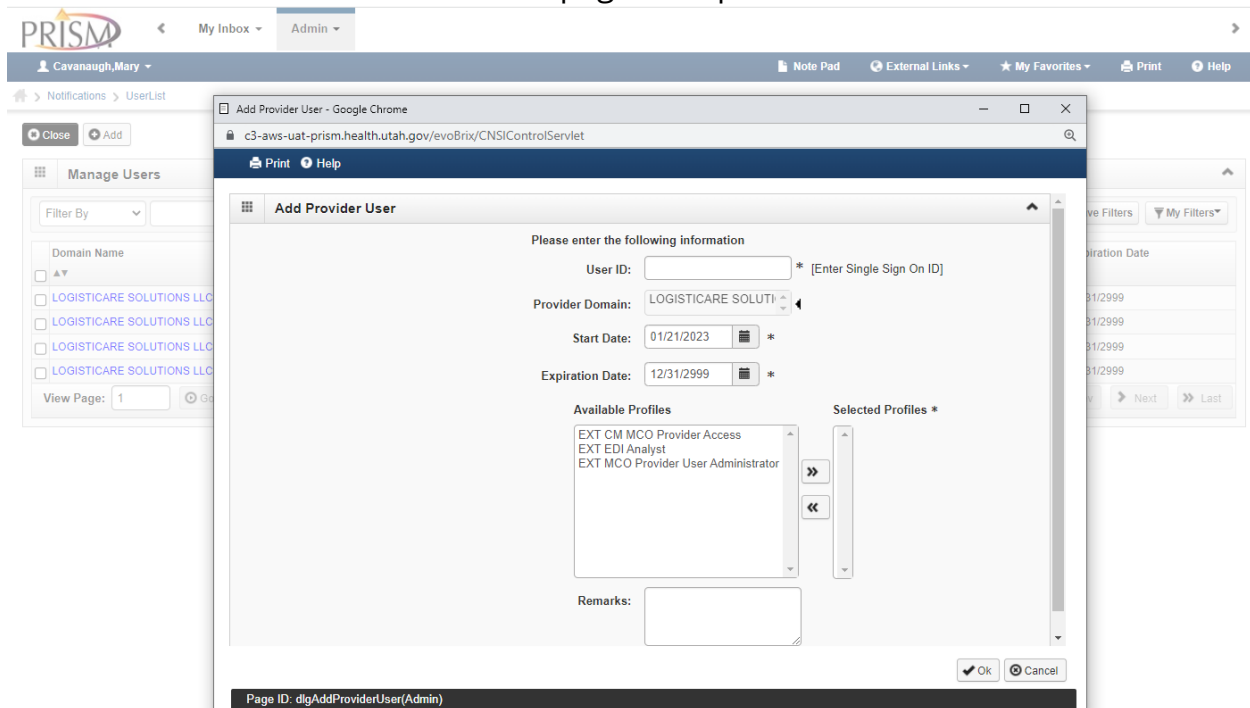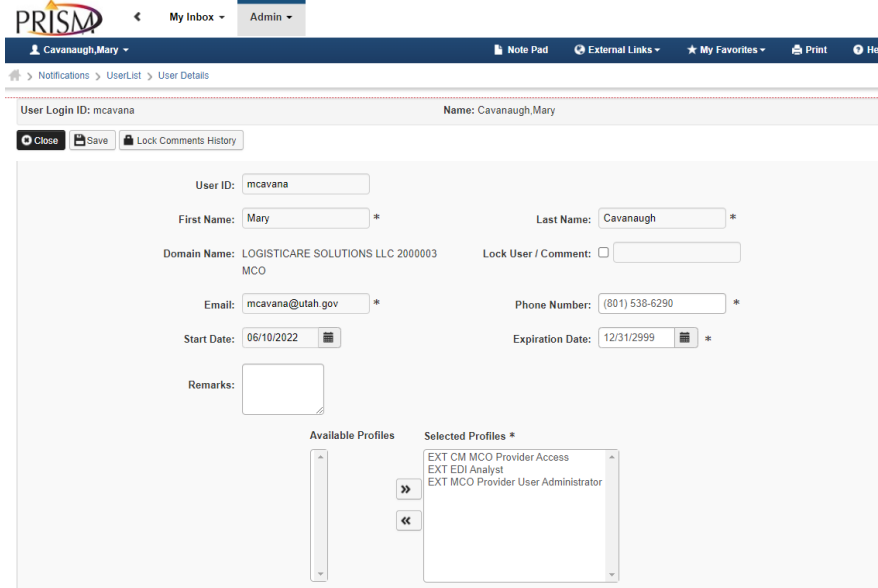
7. Enter the UtahID in the User ID field of the new user being added.

8. Update the start date and end date as applicable.

9. Click on the profile(s) you would like to assign to the registering user and use the double arrow button at the center of the screen to move the desired profile to the Selected Profiles list box.

   If applicable, repeat this process for all the profiles being assigned to the user. The user may also hold the Ctrl key, select the appropriate profiles, and then hit the arrow key to select multiple profiles all at once. All the selected profiles will then move to Selected Profiles.

   To remove profiles from the Selected Profiles list box, select the profile and click the Exclusion arrow (<<).

10. Click OK at the bottom right corner to complete the user access and return to the User List page.

11. The user will now appear in the list of users.

12. <u>Verify that the correct user was given access</u> by validating the UserID and the email address.   Click on the Domain Name hyperlink (in blue) for the corresponding user record.

   - The Update Provider User page will display the User Details where the email address associated to the UtahID is displayed. If the email address does not match the intended user, the wrong UtahID was entered.

- To remove access to the "wrong" user and prevent access to the domain
  - Check the Lock User/Comment box
  - Update the Expiration Date to match the Start Date
  - Click Save
  - Click Close to exit the page

II. Modify a User Access

1. From the Manage Users list on the User List page, click on the Domain Name hyperlink (in blue) for the user record being modified

   - The Update Provider User page will display the User Details
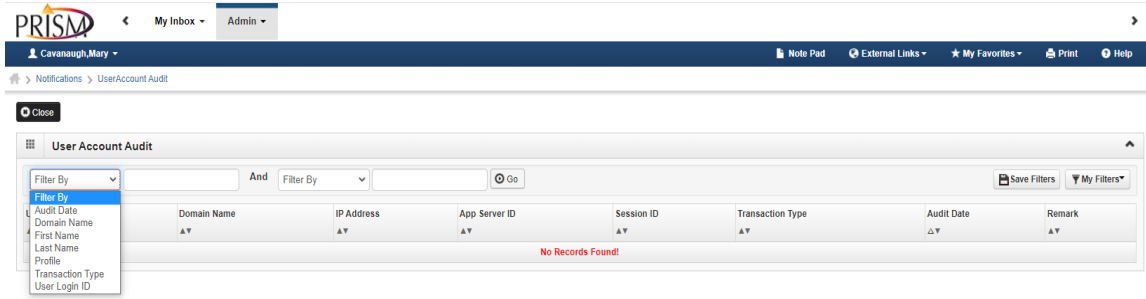
- The Phone Number, access Expiration Date and the Profile access can be modified from this screen
- Click Save to save modifications
- Click Close to return to the User List page

III. Review User Access Activity

1. From the Admin dropdown, select User Account Audit
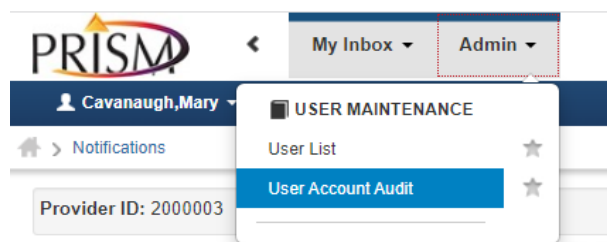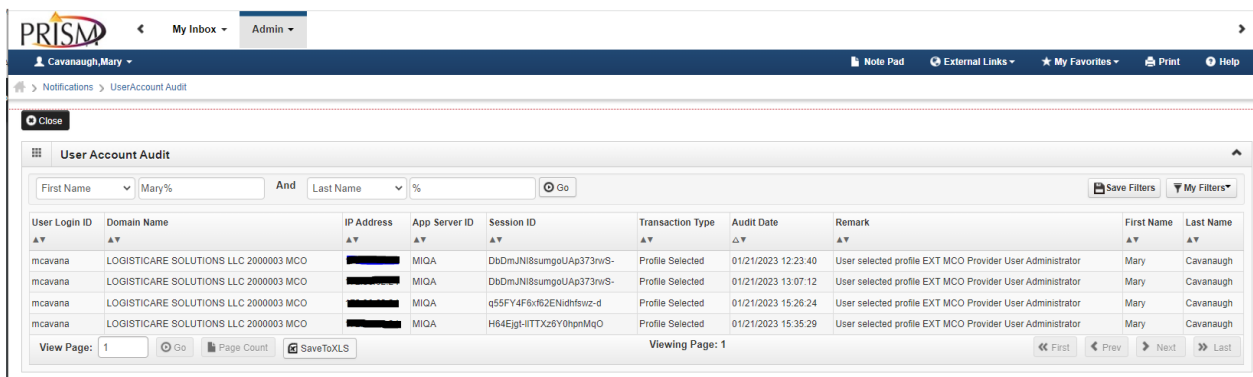
2. The User Account Audit page will display. From this page you can review user and profile access logs.

3. Use the Filter By dropdowns for a targeted search. You can search by using one or both Filter By dropdowns.

4. Enter values to search based on the Filter By option selected.   You may use a wildcard of % if the exact identifier is not known.