

3 Maintaining User Accounts in CCQAS 2.8

The maintenance of user accounts is the joint responsibility of the account holder and the CC/MSSP/CM who is responsible for managing user accounts. Over time, it is likely that a user's account will require updating to reflect changes in personal information, job responsibilities, or location. Guidance regarding updating and maintaining user accounts is provided in the following sections.

3.1 Updating User Personal and Contact Information

Updates to demographic and contact information stored in CCQAS should be made as soon as possible after changes occur. Reviewers and other Privileging module users should be encouraged to update their own information through the "User Profile" feature in CCQAS which may be accessed directly by the account holder through their "System" main menu (Exhibit 3.1-1).



Exhibit 3.1-1. User Profile Menu Item for Other (Module Users)

The first tab from the user account, the Demographics tab, will be returned (Exhibit 3.1-2).

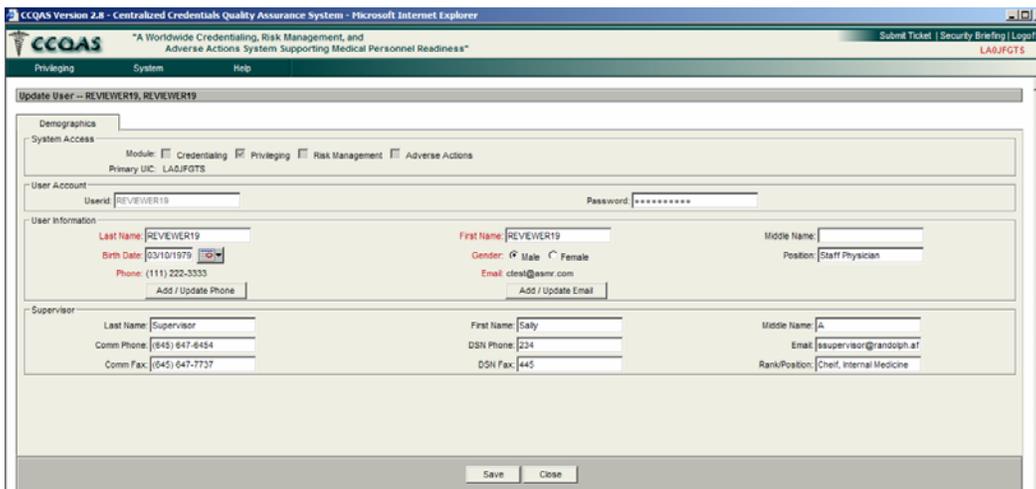


Exhibit 3.1-2. Update User Screen for Other (Module Users)

Users may add or update their own contact information or that of their supervisor. Once the changes are saved, the account holder’s information will be updated in CCQAS.

Note: Users with *Provider* access only in CCQAS do not have access to the “System” main menu, and therefore, cannot access the “User Profile” functionality. Providers should update their contact information when they submit their application for renewal or transfer of privileges. If their contact information changes between privileging cycles, they should contact the credentials office to have updates made to their user account.

CCs/MSSPs/CMs may also update demographic and contact information for any user in their facility or unit by selecting “User Processing” from the System main menu (Exhibit 3.1-3).

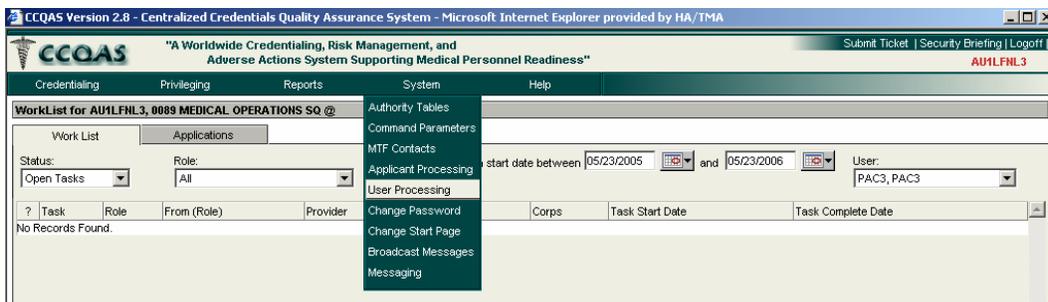


Exhibit 3.1-3. User Processing Menu Item

Selecting “User Processing” will return the “User Listing” screen (Exhibit 3.1-4).

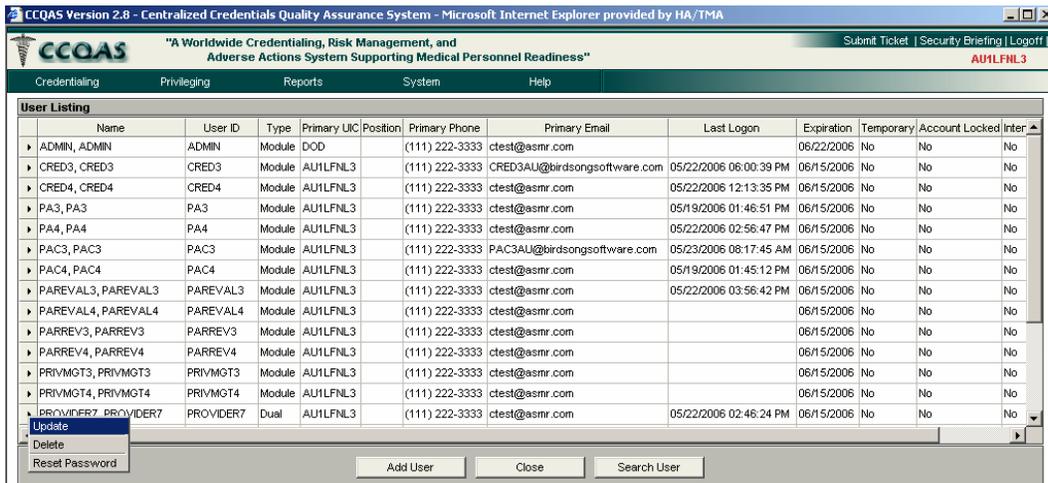


Exhibit 3.1-4. User Profile Menu Item

For each user listed, a hidden menu of actions may be viewed by clicking on the arrow to the left of the user’s name. The personal information about the user and the permissions assigned to the user account may be viewed by selecting “Update” (Exhibit 3.1-4).

Exhibit 3.1-5. Update User Screen

The “Update User” screen (Exhibit 3.1-5) will be returned, displaying the “Demographics” tab. The user’s contact and supervisor information may then be updated, as appropriate. After clicking <Save>, the changes will be updated immediately in the CCQAS database. Changes to the user’s access to CCQAS are performed on the “MTF” and “Permissions” tab. These actions are addressed in the chapters below.

3.2 Changing an Active Password

A Privileging or other module user may change their password at any time, and should do so immediately, if they feel its integrity has been compromised. To change their password, a user clicks the “System” main menu and selects “Change Password” (Exhibit 3.2-1).

Name	User ID	Type	Primary UIC	Authority Tables	Primary Email	Last Logon	Expiration	Temporary	Account Locked
ADMIN, ADMIN	ADMIN	Module	DOD	MTF Contacts	ctest@asmr.com		06/22/2006	No	No
CRED3, CRED3	CRED3	Module	AU1LFNL3	Applicant Processing	CRED3AU@birdsongssoftware.com	05/22/2006 06:00:39 PM	06/15/2006	No	No
CRED4, CRED4	CRED4	Module	AU1LFNL3	User Processing	ctest@asmr.com	05/22/2006 12:13:35 PM	06/15/2006	No	No
PAC3, PAC3	PAC3	Module	AU1LFNL3	Change Password	ctest@asmr.com	05/19/2006 01:46:51 PM	06/15/2006	No	No
PA4, PA4	PA4	Module	AU1LFNL3	Change Start Page	ctest@asmr.com	05/22/2006 02:56:47 PM	06/15/2006	No	No
PAC3, PAC3	PAC3	Module	AU1LFNL3	Broadcast Messages	PAC3AU@birdsongssoftware.com	05/23/2006 08:17:45 AM	06/15/2006	No	No
PAC4, PAC4	PAC4	Module	AU1LFNL3	Messaging	ctest@asmr.com	05/19/2006 01:45:12 PM	06/15/2006	No	No
PAREVAL3, PAREVAL3	PAREVAL3	Module	AU1LFNL3	(111) 222-3333	ctest@asmr.com	05/22/2006 03:56:42 PM	06/15/2006	No	No

Exhibit 3.2-1. Change Password Menu Item

If a user’s password is within 30 days of the expiration date, the user will also receive a password expiration warning each time they log into CCQAS (Exhibit 3.2-2).



Exhibit 3.2-2. Password Expiration Warning

The user may update a password using the “Change Password” function at any time prior to the password expiration date.

Note: Users with *Provider* access only in CCQAS do not have access to the System menu, and therefore, cannot initiate a password change. When providers need to have their password changed, they should contact the credentials office for assistance.

The CC/MSSP/CM may also initiate a password change on any user account by selecting the “Reset Password” from the hidden menu of actions on the “User Listing” screen (Exhibit 3.2-3).

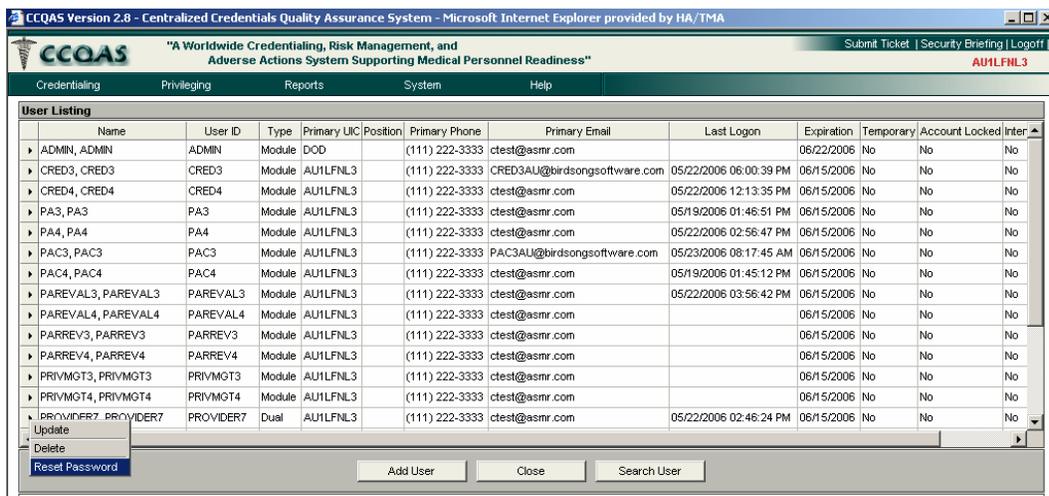


Exhibit 3.2-3. Reset Password Menu Item

When the CC/MSSP/CM initiates the password change, the user receives an automated email notification that contains their new, temporary password that will be valid for the next 90 days.

3.3 Locking and Unlocking User Accounts

User Accounts may be locked and unlocked by the CC/MSSP/CM on the “Update User” screen. A CCQAS user account may be automatically locked by the application under the following circumstances:

- The account holder has failed to enter the correct password during each of three consecutive attempts to log into the CCQAS application
- The password on the user account has expired

The account holder must then contact the CC/MSSP/CM or the MHS Helpdesk to unlock the account.

When a user's account has been locked in this manner, the Administrator may unlock the account by clicking on the **“Account Locked”** box to remove the check mark. This action will generate an automated email message to the account holder with a new, temporary password. The account holder must then log into CCQAS and obtain a new, permanent password that is valid for the next 90 days.

Under certain circumstances, it may be appropriate to lock a user's account intentionally to prevent the user from accessing CCQAS. If the CC/MSSP/CM initiates the locking of a user account, the screen will display a message indicating the account was intentionally locked (Exhibit 3.3-1).

The screenshot shows the 'Update User -- PROVIDER7, PROVIDER7' form in a Microsoft Internet Explorer browser window. The browser title is 'CCQAS Version 2.8 - Centralized Credentials Quality Assurance System - Microsoft Internet Explorer provided by HA/TMA'. The page header includes the CCQAS logo, the tagline 'A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness', and navigation links for 'Submit Ticket', 'Security Briefing', and 'Logout'. The user is logged in as 'AU1LFNL3'. The form has tabs for 'Demographics', 'MTF', and 'Permissions'. The 'System Access' section shows module checkboxes for Credentialing, Privileging, Risk Management, and Adverse Actions, with 'Primary UIC: AU1LFNL3'. The 'User Account' section shows 'Userid: PROVIDER7' and a masked 'Password' field. A red indicator shows 'Account Locked' with a checked box and the text 'Intentionally Locked'. An 'Issue New Password' button is present. The 'User Information' section includes fields for Last Name (PROVIDER7), First Name (PROVIDER7), Middle Name, Birth Date (12/29/1978), Gender (Male selected), Position, Phone ((111) 222-3333), and Email (ctest@asmr.com). The 'Supervisor' section has fields for Last Name, First Name, Middle Name, Comm Phone, DSN Phone, Email, Comm Fax, DSN Fax, and Rank/Position. 'Save' and 'Close' buttons are at the bottom.

Exhibit 3.3-1. Account Locked Indicator

Once the issue with the account has been resolved, the account may be unlocked by clicking again on the **“Account Locked”** box to remove the check mark. This action will generate an automated email message to the account holder with a new, temporary password. The account holder must then log into CCQAS and obtain a new, permanent password that is valid for the next 90 days.

3.4 Adding the Provider Role to an Existing “Other (Module Users)” User Account

In most cases, individuals who use the Privileging module, such as reviewers, the privilege authority, and PAR evaluators, will also be providers. If an individual initially applies for a user account as a Privileging module user, he/she is likely to need the role of provider added to their user account at some later point in time.

Note: The role of *Provider* should not be added to the user’s account until the provider is due to fill out a first e-application for privileges in CCQAS either to renew current privileges or apply for privileges at another facility or unit for an ICTB or PCS.

The addition of the *Provider* role may be initiated in one of several ways:

- If the provider already has an active credentials record in CCQAS, the CC/MSSP/CM may use the “Grant Provider Access” function in the Credentialing module (see Section 2.4)
- The provider may re-register for a user account and specify “**Type = Provider Applicant**” on the registration form. The CC/MSSP/CM may then begin processing the request via the “Applicant Processing” function (see Section 2.3)
- The CC/MSSP/CM may initiate the process of adding a new user via the User Processing function, and specify “**Type = Provider Applicant**” on the “User Application” screen (see Section 2.2)

Regardless of whether the user or the CC/MSSP/CM initiated the creation of the user account, once the processing begins, CCQAS will check against the existing user accounts to determine if an individual with the same name and birth date is already a CCQAS user. If a match is found, CCQAS will enable the CC/MSSP/CM to link the registration form with the existing user’s account via the “Similar People Found” screen (Exhibit 3.4-1).

User ID	User Type	Name	Date of Birth	UIC(s)	Position	Email Address	Contact Phone	Provider	Last Logon
BEANV	User	BEAN, VANILLA	04/23/1976	W003AA, W2L6AA	Credentials Clerk	VANILLA.BEAN@US.ARMY.ML	Business Direct: (202) 207-5833	Yes	08/11/2008

Exhibit 3.4-1. Similar People Found Screen

The registration form may be linked to the existing user account by clicking on the small arrow to the left of the matching user’s record. CCQAS will open the existing user account for the individual. The “MTF” tab in the user’s account will reflect the addition of the *Provider* role by displaying a record line on the bottom half of the screen (Exhibit 3.4-2).

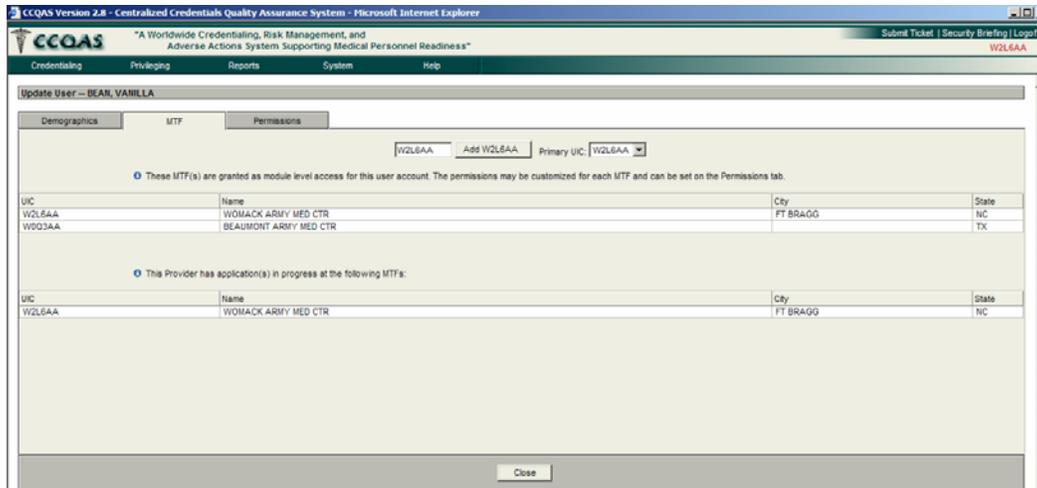


Exhibit 3.4-2. MTF Tab for a Dual User's Account

The “Permissions” tab should continue to reflect the roles and permissions that were originally assigned to the user account. The addition of the *Provider* role does not alter any of the previously-assigned roles or permissions.

When the role of *Provider* is added to the user's account, the 1st e-application is also generated for the provider to request clinical privileges online using the CCQAS application.

Note: If the “Similar People Found” screen is returned but none of the users listed on the screen matches the provider who is being added to CCQAS, the CC/MSSP/CM may click <Close> to cancel the process or <Add New User> to proceed with the process of creating a new user account in CCQAS for the provider.

3.5 Adding “Other (Module Users)” User Role to an Existing Provider Account

Depending on where they are in their privileging cycle when they become CCQAS users, some users may require access to CCQAS in the role of Provider first, and later need access as “*Other (Module Users)*”. The process for adding the *Other (Module Users)* role to an existing provider account may be initiated by selecting “User Processing” from the “System” main menu. The “User Listing” screen is returned. Only the *Other (Module Users)* are displayed on the “User Listing” screen. To locate the existing provider's user account, click <Search User> (Exhibit 3.5-1).

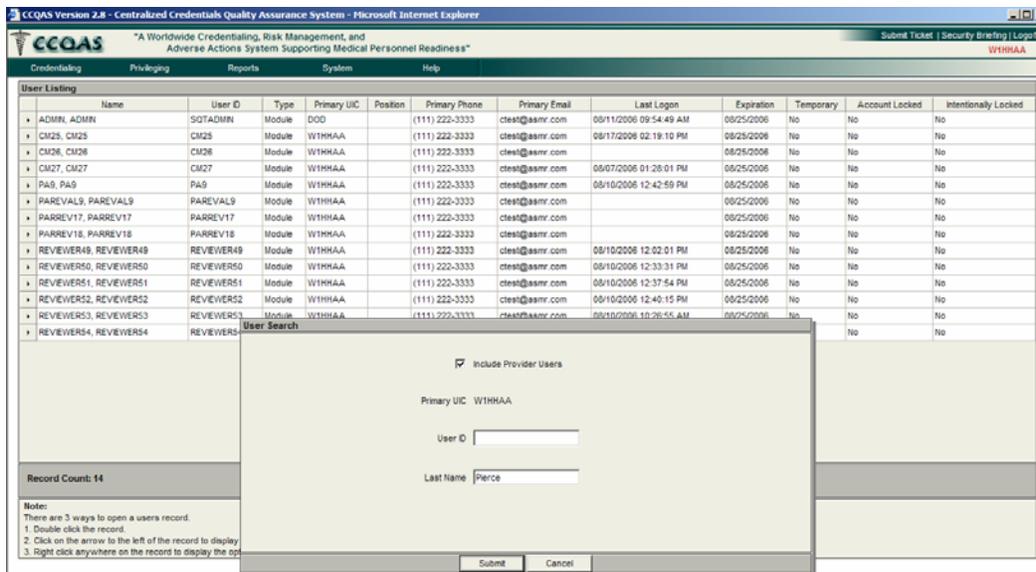


Exhibit 3.5-1. The User Search Screen

Check the **“Include Provider Users”** box, enter the provider’s **Last Name** and click **<Submit>**. The **“User Listing”** screen should be returned (Exhibit 3.5-2), displaying all existing user accounts at the facility or unit that meet the search criteria.



Exhibit 3.5-2. The User Listing Screen After a Search

Once the user account is opened, the process of adding the *Other (Module Users)* role is initiated on the **“MTF”** tab. Initially, the provider’s user account will have no UICs listed on the upper half of the screen (Exhibit 3.5-3).

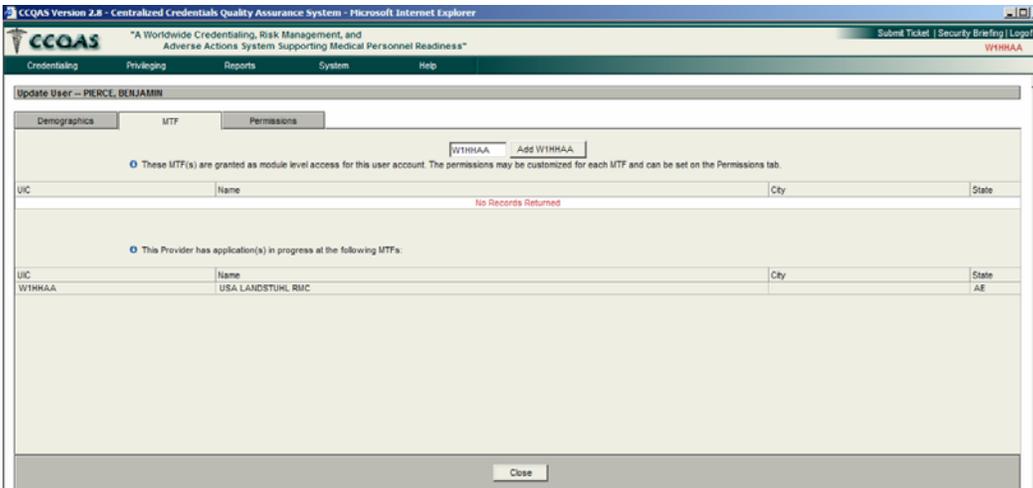


Exhibit 3.5-3. The MTF Tab for a Provider User Account

To grant the provider access to the Privileging module, click <Add [UIC]> at the top of the screen. This action will automatically create a UIC record in the upper portion of the screen (Exhibit 3.5-4), indicating that *Other (Module Users)* access has been attached to the provider’s account.

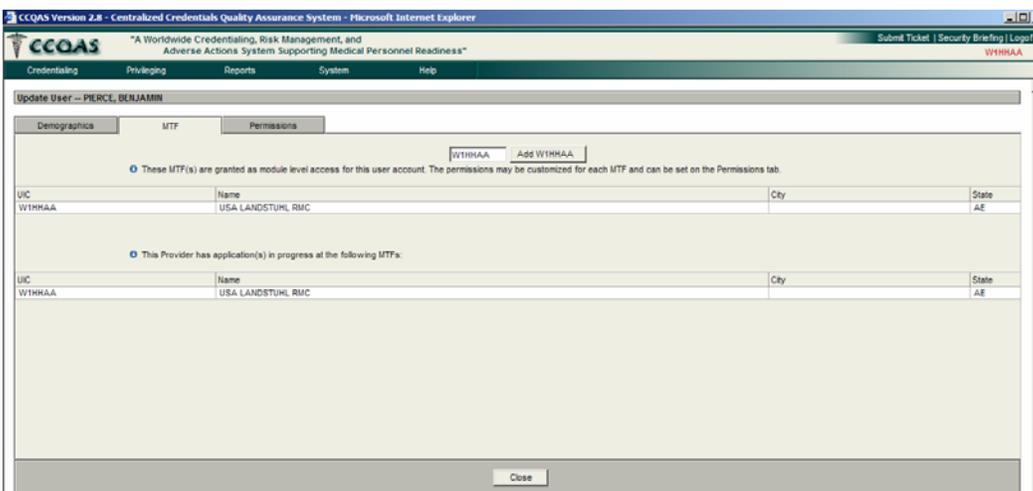


Exhibit 3.5-4. The MTF Tab for a Dual User’s Account

The appropriate roles and permissions may then be assigned to the user on the “Permissions” tab. Once the changes on the “Permissions” tab are saved, and the user’s account is closed, the provider will have access to CCQAS with assigned roles and permissions associated with his/her user account.

3.6 Deleting User Accounts

Occasionally, it will be necessary for the CCQAS Administrator to delete a user account.

Deletion of a user account may be done through the “User Processing” function, available from the “System” main menu. On the “User Listing” screen, the CC/MSSP/CM may select “Delete” from the menu of actions available for each record (Exhibit 3.7-1).

The screenshot shows the CCQAS User Listing interface. At the top, there is a navigation bar with tabs for Credentiaing, Privileging, Reports, System, and Help. Below this is a table with columns: Name, User ID, Type, Primary UIC, Position, Primary Phone, Primary Email, Last Logon, Expiration, Temporary, Account Locked, and Inter. The table lists various users including ADMIN, CRED3, CRED4, PA3, PA4, PAC3, PAC4, PAREVAL3, PAREVAL4, PARREV3, PARREV4, PRIVMGT3, PRIVMGT4, and PROVIDER7. A context menu is open over the PROVIDER7 row, showing options: Update, Delete, and Reset Password. The 'Delete' option is highlighted. Below the table are buttons for 'Add User', 'Close', and 'Search User'.

Name	User ID	Type	Primary UIC	Position	Primary Phone	Primary Email	Last Logon	Expiration	Temporary	Account Locked	Inter
ADMIN, ADMIN	ADMIN	Module	DOD		(111) 222-3333	ctest@asmr.com		06/22/2006	No	No	No
CRED3, CRED3	CRED3	Module	AU1LFNL3		(111) 222-3333	CRED3AU@birdsongssoftware.com	05/22/2006 06:00:39 PM	06/15/2006	No	No	No
CRED4, CRED4	CRED4	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com	05/22/2006 12:13:35 PM	06/15/2006	No	No	No
PA3, PA3	PA3	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com	05/19/2006 01:46:51 PM	06/15/2006	No	No	No
PA4, PA4	PA4	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com	05/22/2006 02:56:47 PM	06/15/2006	No	No	No
PAC3, PAC3	PAC3	Module	AU1LFNL3		(111) 222-3333	PAC3AU@birdsongssoftware.com	05/23/2006 08:17:45 AM	06/15/2006	No	No	No
PAC4, PAC4	PAC4	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com	05/19/2006 01:45:12 PM	06/15/2006	No	No	No
PAREVAL3, PAREVAL3	PAREVAL3	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com	05/22/2006 03:56:42 PM	06/15/2006	No	No	No
PAREVAL4, PAREVAL4	PAREVAL4	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com		06/15/2006	No	No	No
PARREV3, PARREV3	PARREV3	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com		06/15/2006	No	No	No
PARREV4, PARREV4	PARREV4	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com		06/15/2006	No	No	No
PRIVMGT3, PRIVMGT3	PRIVMGT3	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com		06/15/2006	No	No	No
PRIVMGT4, PRIVMGT4	PRIVMGT4	Module	AU1LFNL3		(111) 222-3333	ctest@asmr.com		06/15/2006	No	No	No
PROVIDER7, PROVIDER7	PROVIDER7	Dual	AU1LFNL3		(111) 222-3333	ctest@asmr.com	05/22/2006 02:46:24 PM	06/15/2006	No	No	No

Exhibit. 3.6-1. Delete Menu Item

Once a user account is deleted from CCQAS, it may not be recovered. Nor is any record retained of its prior existence. Thus, the prudent CC/MSSP/CM will make certain it is appropriate to delete a user account before actually doing so.

3.7 Frequently Asked Questions

FAQ: The UIC for the UIC field and on the <Add> button for adding the “Other (Module Users)” role is already prepopulated. What if I want to grant a provider access to another UIC different from where he has a Provider role?

Answer: The UIC in the field and on the button will be defaulted to the UIC where the user has a Provider role already. If you want to grant a provider “Other (Module Users)” permissions to a different UIC, type in the correct one in the field and click the <Add...> button).

FAQ: Will the providers in my facility require a different userid and password for each of their roles in the privileging module?

Answer: No. Each user (with one or many roles) will require only one userid and password.