

2 Creating New CCQAS 2.8 User Accounts

The deployment of CCQAS 2.8 which introduced the online privilege application, review, and approval functionality, significantly expanded the number of CCQAS users relative to previous versions of the application. In addition to the administrative personnel who use the credentials and risk management functionality, providers who are applying for clinical privileges and those personnel who are responsible for reviewing, approving, and granting clinical privileges also require access to CCQAS. The responsibility for creating user accounts for each of these individuals in the military treatment facility (MTF) or unit belongs to the CC/MSSP/CM who, in all probability, will also be the designated MTF or unit CCQAS Administrator and User Account Manager.

All individuals who require access to CCQAS and do not yet have a user account are considered “new CCQAS users.” This includes all new providers who are beginning to work in the military health system for the first time, providers who are currently privileged to render patient care, staff members who are directly involved in review and approval of privilege applications, and others. The manner in which each CCQAS user account is created will depend on the user’s role in the privileging process. The creation of new user accounts may be initiated in one of three ways:

- A prospective user may self-register for a new user account. The request form is then processed by the CC/MSSP/CM via the “Applicant Processing” function (Sections 2.1 and 2.3)
- The CC/MSSP/CM may create a new user account through the “User Processing” function (Sections 2.2 and 2.3)
- The CC/MSSP/CM may initiate the creation of a user account for a provider with an existing credentials record in CCQAS via the Credentialing module (Section 2.4)

The sections below discuss the creation of a new user account by each of these methods. The on-going management and modification of user accounts is addressed in Section 3 of this guide.

2.1 Self-Service Registration

Any prospective CCQAS user may apply online for an account using the self-service registration function. The online registration form is accessed from the CCQAS logon screen, by clicking <**Registration**> (see Exhibit 2.1-1).



Exhibit 2.1-1. CCQAS User Registration Button

Instructions for completing the online form are provided at the top of the screen. Those data fields labeled with red text are required in order for CCQAS to accept the application.

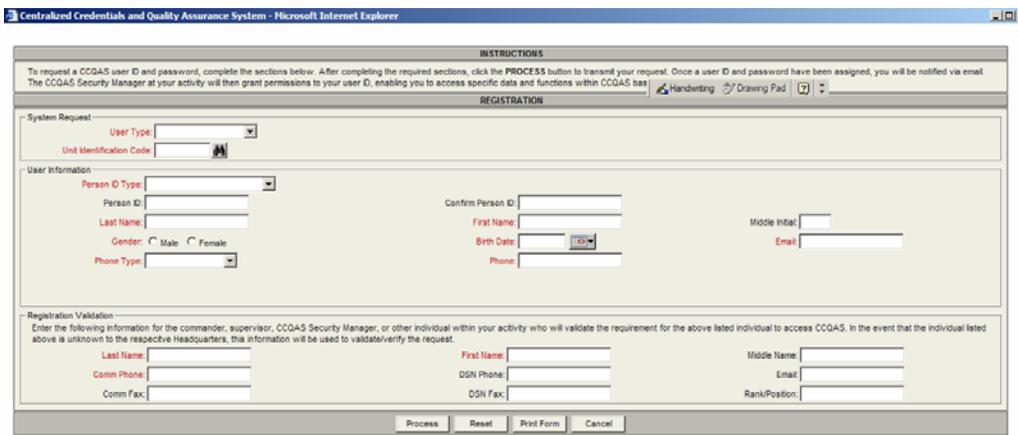


Exhibit 2.1-2. CCQAS User Registration Screen

The requirements for completing the registration form will vary depending upon the value selected for “**User Type**”. For the purposes of user account creation, applicants are classified either as “*Provider Applicant*” or as “*Other (Module Users)*.”

The applicant should select “**User Type = Provider Applicant**” if they are a provider who requires access to CCQAS for the purpose of requesting clinical privileges or submitting their credentials as a member of the Clinical Support Staff. When “**User Type = Provider Applicant**” is selected, “**Person ID Type**” becomes a required field and the applicant must then enter either his or her *Social Security Number* or *Foreign Identification Number*. This number will eventually become the unique identifier for the provider’s credentials record in CCQAS. When “**User Type = Provider Applicant**,” the user is also required to designate himself or herself as a military or civilian provider.

Exhibit 2.1-3. CCQAS User Registration Screen – Provider Applicant

Note: Applicants should designate their “**Status = Military Provider**” if they are applying for privileges or Clinical Support Staff positions at the designated facility or unit as uniformed service members (active duty service members, reserve or guard providers on annual training, service members on temporary assignment, or deployed service members. Applicants who apply to render patient care as civilian employees or contractors at that facility or unit should designate their “**Status = Civilian Provider.**”

Applicants should select “**User Type = Other (Module Users)**” (Exhibit 2.1-4) if they will review or approve applications for clinical privileges, or if they are administrative staff members who require access to CCQAS for the purpose of managing credentials records or other functions supported by the Risk Management or Adverse Actions functionality in CCQAS. If “**User Type = Other (Module Users)**” is selected, applicants are required to select the modules to which they are requesting access. Reviewers of privileging applications, the Privileging Authority, personnel responsible for generating and reviewing clinical performance appraisals, personnel who approve state license waiver requests, and staff members who manage facility privilege lists should request access to the Privileging module.

Exhibit 2.1-4. CCQAS User Registration Screen – Other (Module Users)

Note: If “**User Type = Other (Module Users)**” is selected, the applicant is not required to enter **Person ID Type** or **Person ID**. These fields are only required if “**User Type = Provider Applicants**” is selected.

All applicants must specify the **UIC** for their application. The **UIC** search function contains only privileging UICs. The UIC associated with the location where the provider, reviewer, or staff member will be working should be selected.

Though not all remaining fields on the form are labeled with red text, applicants should be encouraged to populate the form as much as possible, since the information on this form will be used by the CC/MSSP/CM to verify the applicant’s identity and need for system access. An accurate email address is critical, since the applicant will be issued an individual userid and temporary password via email.

After all information has been entered on the form, the applicant clicks <**Process**> (see Exhibit 2.1-4). The application is then sent to the CCQAS Administrator for processing.

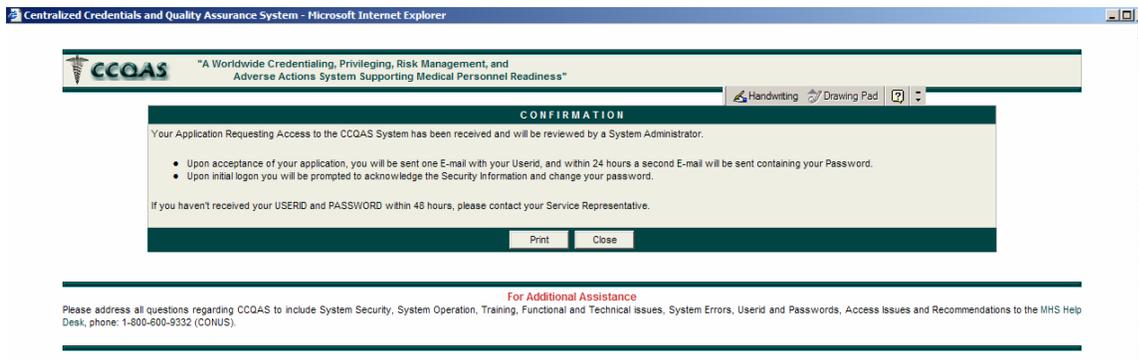


Exhibit 2.1-5. CCQAS Registration Confirmation Screen

CCQAS will return a confirmation of application submission which may either be printed or closed by the applicant (see Exhibit 2.1-5). When <**Close**> is selected, the applicant will be returned to the log in screen.

2.2 CC/MSSP/CM-Generated Applications

The CC/MSSP/CM may wish to create the CCQAS user account directly, without requiring the applicant to complete the online registration form. In this method, the CC/MSSP/CM may create a new user account directly via the “User Processing” function which is accessed through the “System” main menu (Exhibit 2.2-1).

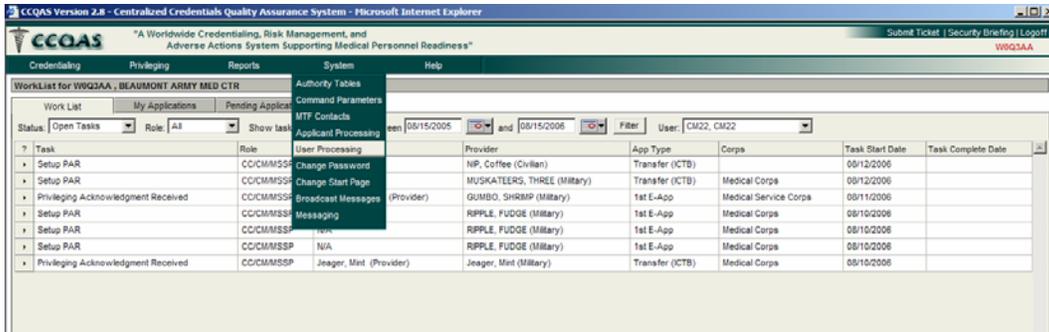


Exhibit 2.2-1. User Processing Menu Item

The “User Listing” screen will be returned.

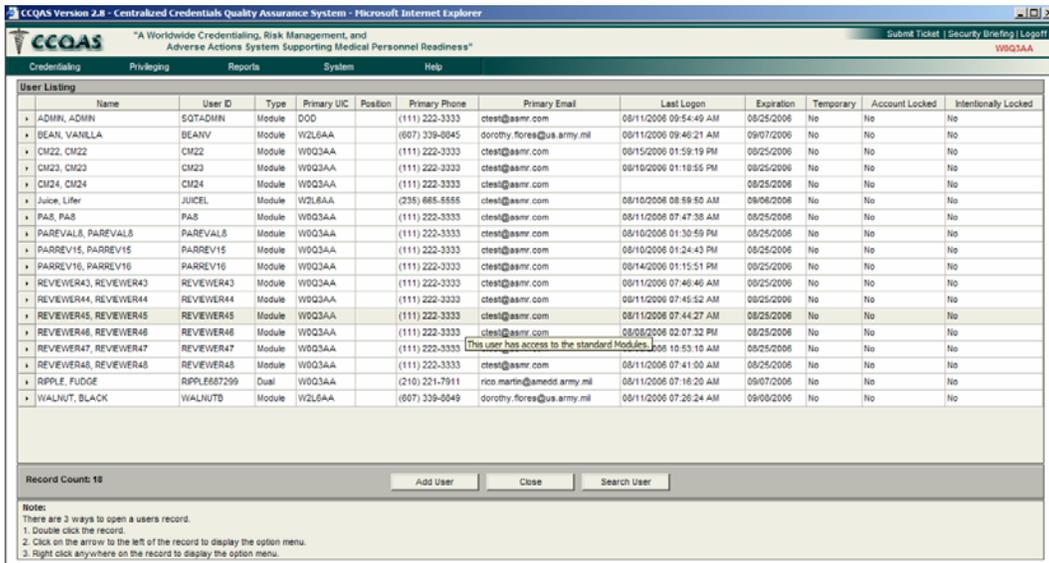


Exhibit 2.2-2. User Listing Screen

Addition of a new user may be initiated by clicking “Add User” at the bottom of the screen (Exhibit 2.2-2).

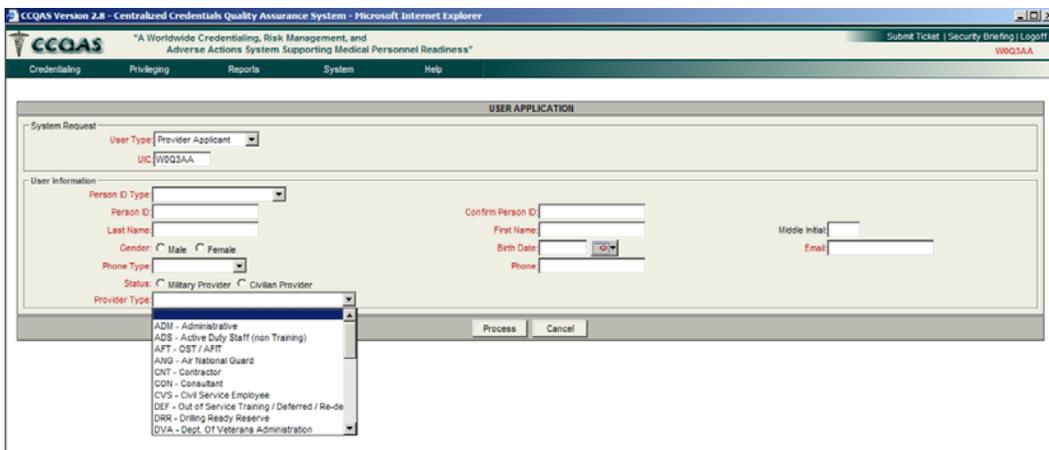


Exhibit 2.2-3. User Application Screen

The User Application screen is returned. The CCQAS Administrator will then complete the application on behalf of the applicant according to the guidance provided in Section 2.1. An additional data field, **Provider Type**, which describes the capacity in which the applicant will be functioning at the designated UIC, must be populated in order to move forward with the processing of the new user account.

As long as the CC/MSSP/CM has already validated the applicant's need to access CCQAS and the level of permissions required, the application may then be processed by clicking <**Process**> (see Exhibit 2.2-3). A discussion of processing applications for new user accounts is presented in the following section.

2.3 Processing Applications for New CCQAS Users

2.3.1 Verifying Applicants' Need for Access to CCQAS

The CC/MSSP/CM who is assigned the responsibility for managing user accounts at a facility or unit must verify each applicant's need for access to CCQAS prior to processing the request for a user account. It is important for the CC/MSSP/CM to clearly understand the applicant's job responsibilities and role in the privileging process in order to assign the correct permissions to the account. The CC/MSSP/CM should confirm the 'need to access' with the appropriate supervisor in the same department where the applicant will be using CCQAS.

2.3.2 Processing the Application

CCQAS will alert the CC/MSSP/CM to new requests for user accounts with a message (Exhibit 2.3-1) which will display when the CC/MSSP/CM logs onto CCQAS.



Exhibit 2.3-1. New Applicant Message

Once logged in, the CC/MSSP/CM may process a new user's application by selecting "Applicant Processing" from the System menu (Exhibit 2.3-2).

Note: "Applicant Processing" will only be used to process applications submitted via the self-service registration screen. If the CC/MSSP/CM initiates the new user account through the "User Processing" screen, the application will be processed directly from within the "User Processing" functionality.

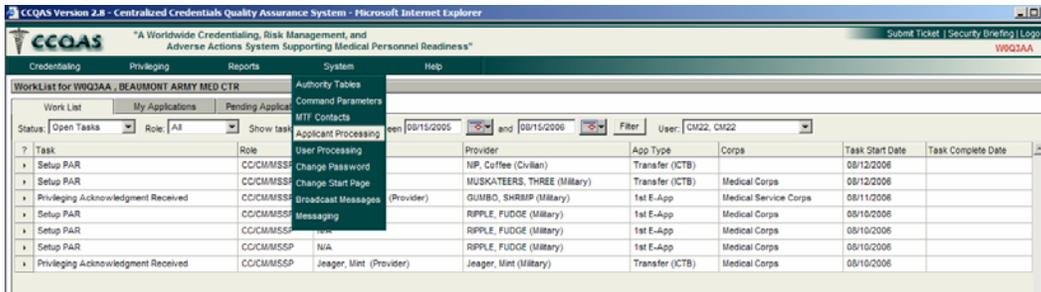


Exhibit 2.3-2. Applicant Processing Menu Item

The new application record may be opened by selecting <Process> from the hidden menu of actions for the applicant’s record.

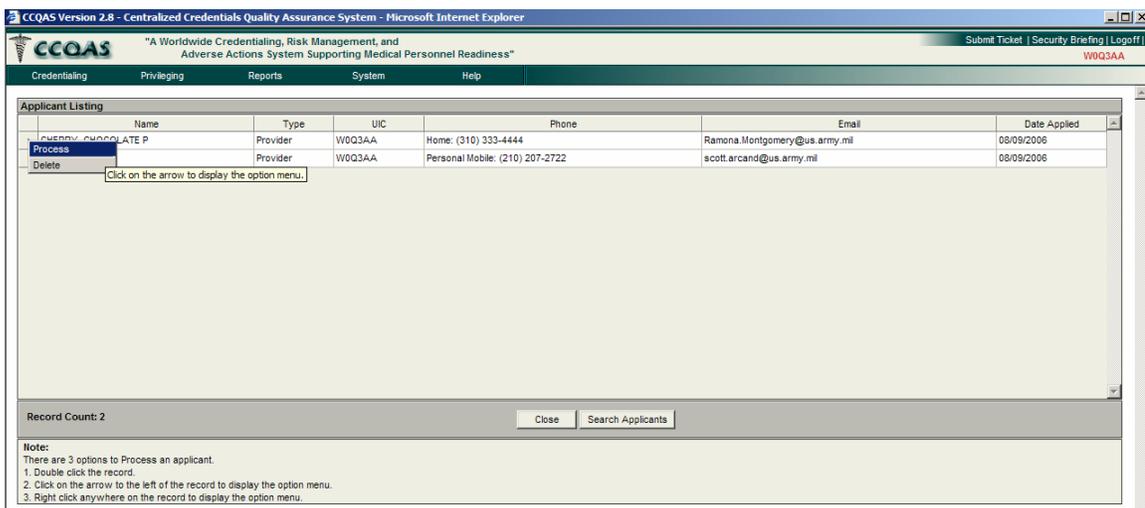


Exhibit 2.3-3. Applicant Processing Screen

The “User Application” is returned (Exhibit 2.3-4), displaying the information submitted by the applicant.

Note: From this point forward, the processing of the application is the same regardless of whether the applicant applied for the user account via the self-service registration screen, or the user account was created by the CC/MSSP/CM through the “User Processing” screen.

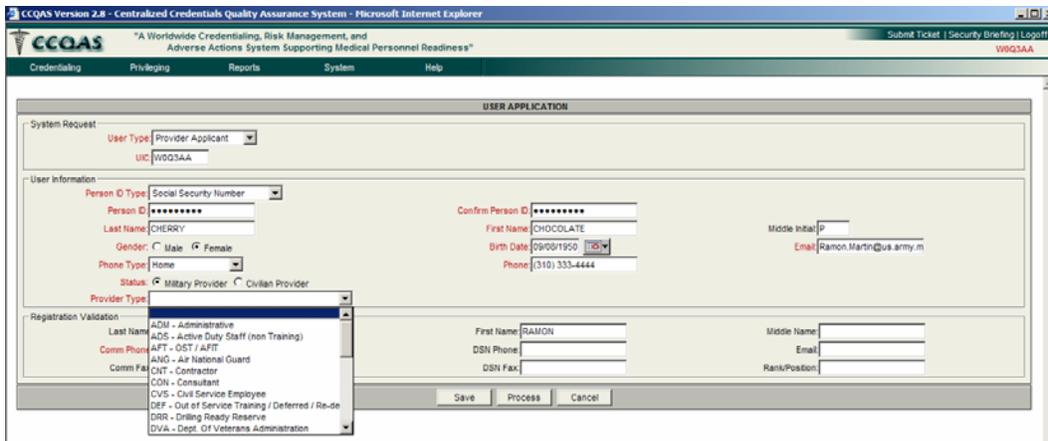


Exhibit 2.3-4. User Application Screen

A value for “**Provider Type**” which describes the capacity in which the applicant will be functioning at the indicated UIC, must be selected from the pick list. Updates to the applicant’s personal information may also be made on this screen. Click <**Save**> and then <**Process**> to set up the permissions for the applicant’s new user account. Once <**Process**> is selected, the user will receive a message (Exhibit 2.3-5) that a new user’s account has been added to CCQAS.



Exhibit 2.3-5. User Added Message

2.3.3 User Accounts for New Provider Applicants

Once the user has been added to CCQAS, the user’s account is presented on the “Update User” screen as a series of tabs.

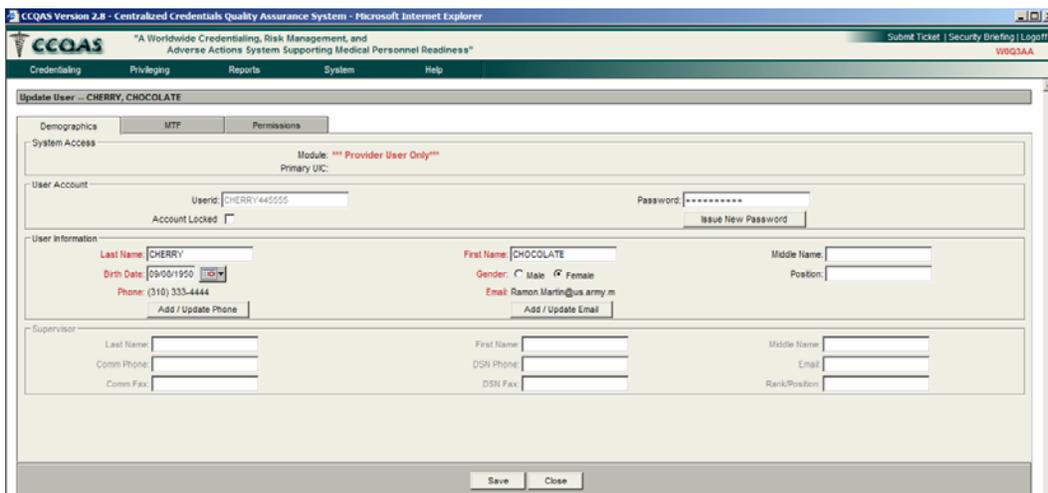


Exhibit 2.3-6. Demographics Tab for a Provider Applicant

The first of the three tabs, the “Demographics” tab, will be used in the future to update the user’s personal information, lock and unlock the user’s account, and issue new passwords to the user as necessary. The user account displayed on the “Demographics” tab in Exhibit 2.3-6 is an account for a provider.

Note: If the applicant is a *Provider Applicant*, no further action is needed. The creation of the user account has been completed. The provider will receive their userid and password via two separate emails sent to the email address listed on the Demographics tab. They will also receive a third email notification, indicating the presence of an item in their work list with “Task = *Complete Application*”. The work list is discussed in detail in Section 5. If the application is for an *Other (Module User)*, processing must be continued to designate the role and permissions that are assigned to the user’s account. This action will be described in more detail in the next section.

The second of the three tabs, the “MTF” tab, provides two important pieces of information. The upper portion of the screen lists the UICs for the facilities and units where the user requires access to CCQAS as an *Other (Module user)*. The user in Exhibit 2.3-7 is a provider applicant only, and therefore has no UICs listed in this section of the screen.

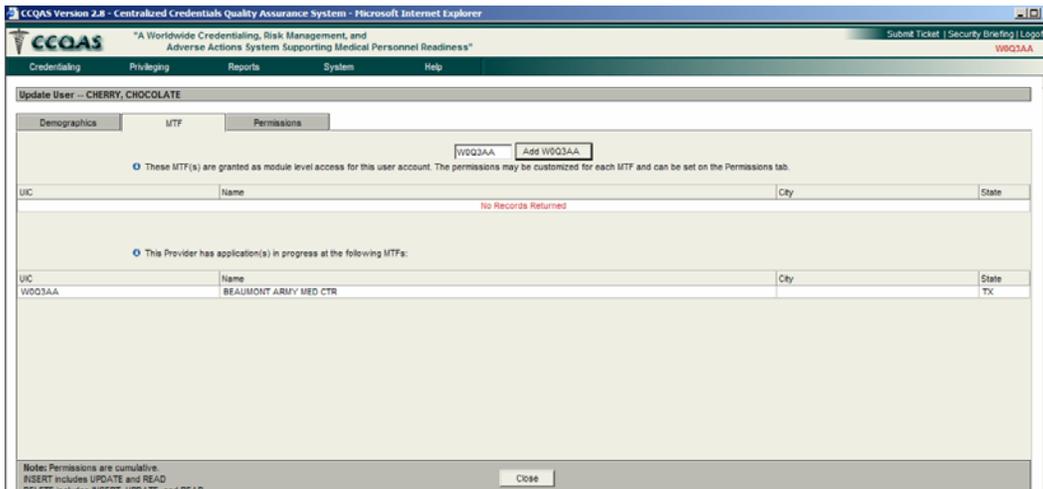


Exhibit 2.3-7. MTF Tab for a Provider Applicant

The UICs listed on the lower portion of the screen are the facilities and units where the user, in the role of a provider, holds clinical privileges or where an application for clinical privileges is currently under review. The provider in Exhibit 2.3-7 has one privilege application in progress at one UIC. This privilege application was created when the user was granted access to CCQAS as a *Provider Applicant*.

The third tab, the “Permissions” tab (Exhibit 2.3-8), is where roles and permissions are assigned to the user’s account.

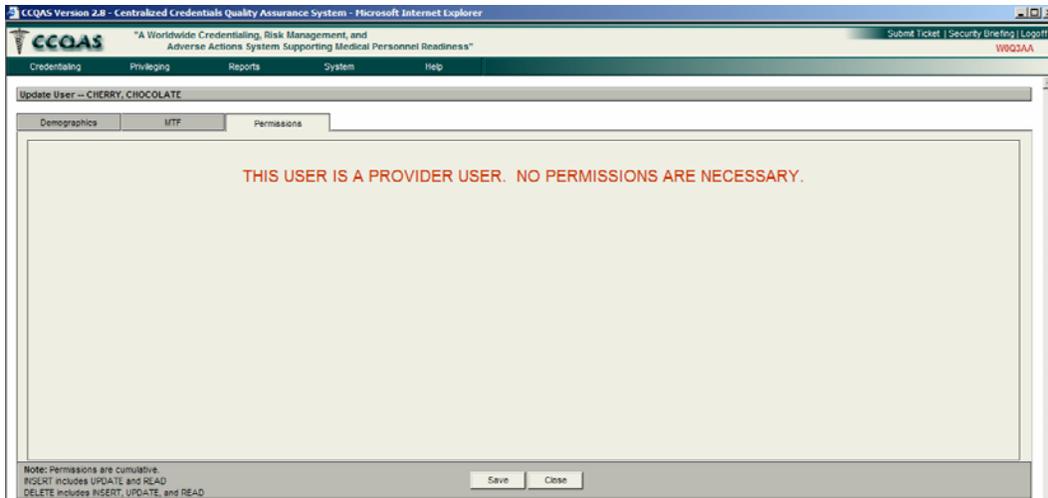


Exhibit 2.3-8. Permissions Tab for a Provider Applicant

For *Provider Applicants*, no roles or permissions need to be configured for their user account. By processing the application as described above, the provider will automatically be granted the appropriate level of access needed to complete and submit applications for clinical privileges and the provider's 1st E-Application for clinical privileges will automatically generate (Section 5). Once created, additional roles as an *Other (Module Users)* may be added to the provider's user account. The process of adding roles to an existing account is discussed in Section 3.

2.3.4 User Accounts for Other (Module Users)

The "Demographics" tab for *Other (Module Users)* is similar to that for *Provider Applicants*, but also includes an indication of the CCQAS modules to which the user has access.

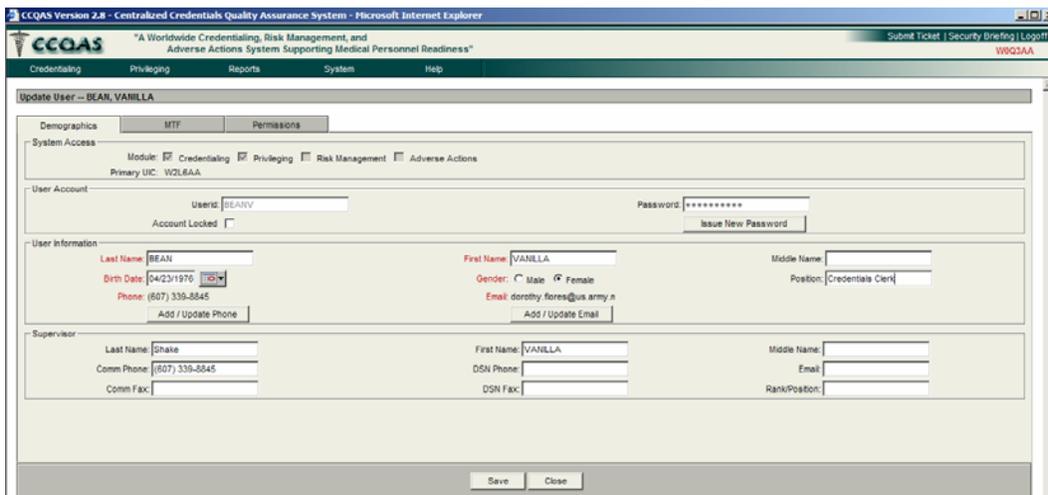


Exhibit 2.3-9. Demographics Tab for an Other (Module Users)

The user account displayed on the “Demographics” tab in Exhibit 2.3-9 is an account for a user who requested access to the “Credentialing” and “Privileging” modules in CCQAS.

The upper portion of the “MTF” tab lists the UIC where the *Other (Module Users)* was granted access to CCQAS. This record was automatically created by CCQAS when the user was granted access to CCQAS. If the user has access to CCQAS at more than one facility or unit, multiple UICs will be displayed here.

The lower portion of the screen will reflect the facilities or units where the user, in the role of a provider, holds clinical privileges or where an application for clinical privileges is currently under review. The provider in Exhibit 2.3-10 has access as an *Other (Module User)* at UIC W0Q3AA and no active privilege applications anywhere in CCQAS.

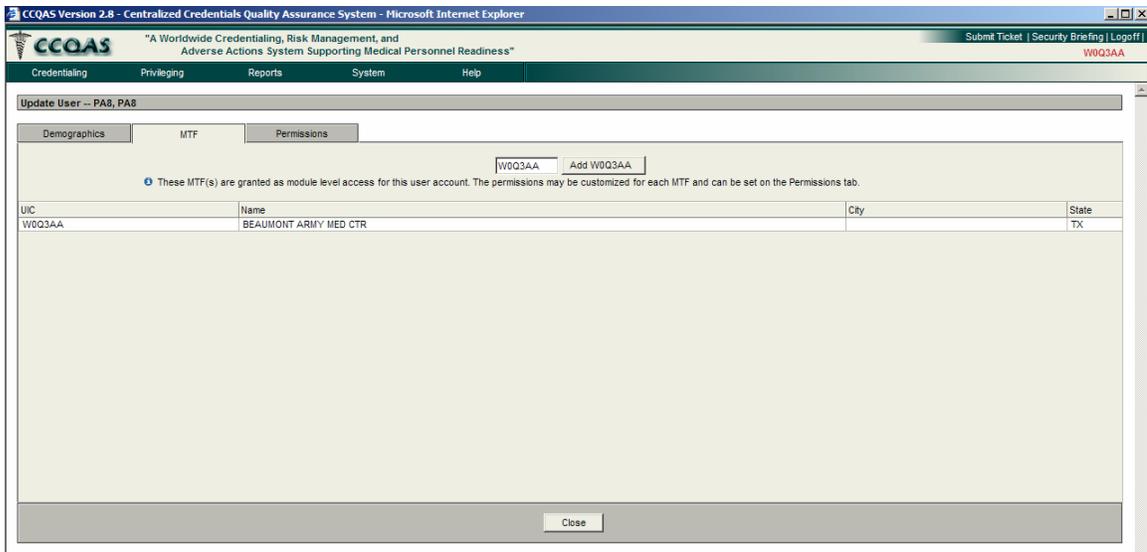


Exhibit 2.3-10. MTF Tab for an Other (Module Users)

To add another MTF for an *Other (Module User)*, simply enter the UIC in the field provided for it and click the button next to it. Disregard the fact that “Add [UIC]” is already on the button. After you click this button, another field will appear next to it, labeled “Primary UIC”, and the field will have a drop-down list of all UICs to which the user has been granted access. (Exhibit 2.3-11)

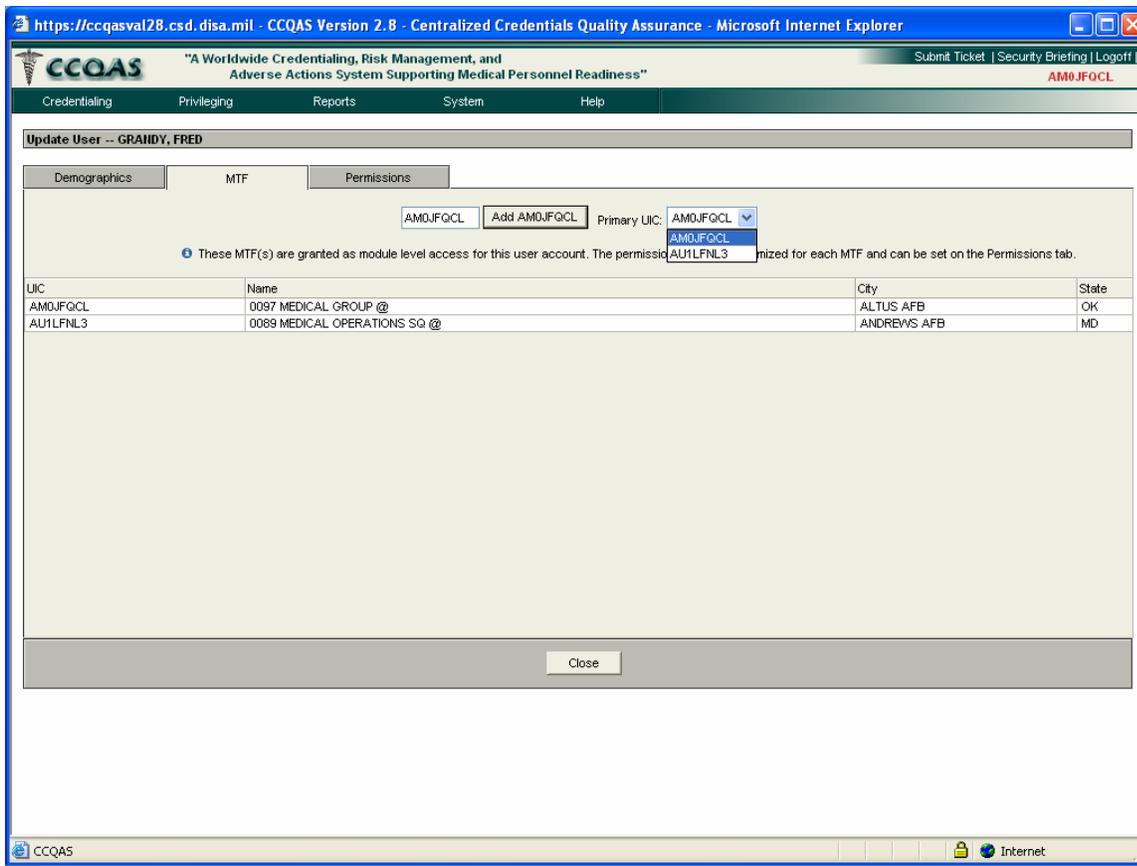


Exhibit 2.3-11. MTF Tab Showing Multiple UICs for an *Other (Module)* User

The individual permissions for *Other (Module Users)* for each UIC are assigned on the Permissions tab (Exhibit 2.3-12).

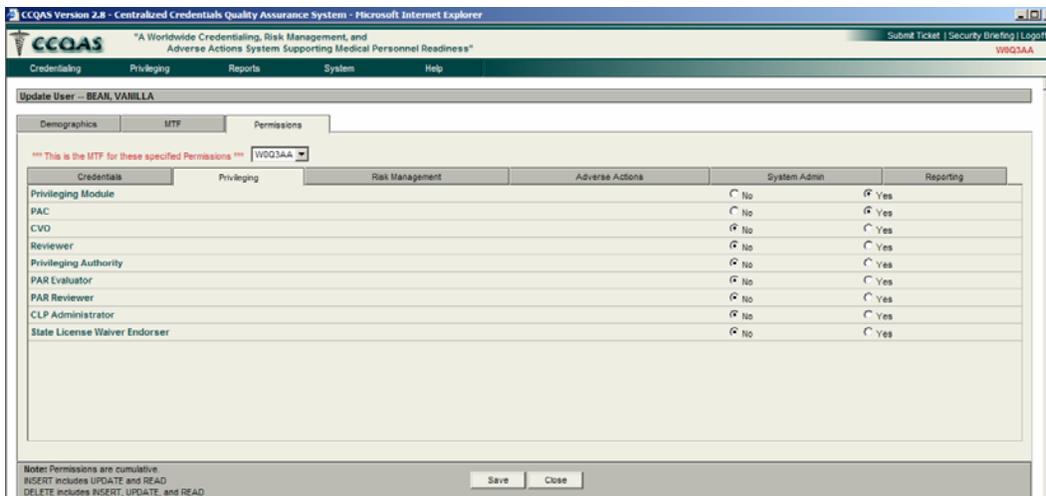


Exhibit 2.3-12. Access Permissions to Privileging Module for *Other (Module)* User

Each user will be granted a specific set of permissions based on their role in the privileging process. The CCQAS 2.8 privileging module defines eight unique roles to which are attached a pre-defined set of permissions for the Privileging module:

- **CC/MSSP/CM (Credentials Coordinator[Army]/Medical Staff Services Professional [Navy]/Credentials Manager[AF]):** Professional Affairs office staff who are responsible for ensuring providers' credentials are in order, for tracking and managing the review and approval of an application for clinical privileges, and for managing CCQAS user accounts for their facility or unit
- **CVO (Credentials Verification Office):** Credentials Verification Office staff members or other credentialing personnel who perform the primary source verification (PSV) of provider credentialing data; PSV function may also be performed by individuals who are assigned the CC/MSSP/CM role
- **Reviewer:** Clinical staff privileging committee members who have been assigned the responsibility for reviewing and recommending actions on applications for privileges. Reviewers may include the provider's supervisor, the specialty, service or section chief, the department chair, and/or the members and chair of the executive committee of the medical (dental) staff (ECOMS/ECODS)
- **PA (Privileging Authority):** Usually the medical treatment facility (MTF) commander or other designated person who is responsible for final approval of applications for clinical privileges
- **CLP Administrator:** The individual(s) who has or have been assigned responsibility for managing the privilege catalog at their unit or facility. Depending on the size of the MTF or other determining factors, this role may also be played by the CC/MSSP/CM. The privilege catalog is based on *common language privileging*, hence the abbreviation "CLP"
- **PAR Evaluator:** Supervisors, service chiefs, department chairs or other clinical personnel who are responsible for completing and submitting a performance assessment report (PAR) on a provider
- **PAR Reviewer:** Clinical staff members who are responsible for reviewing a PAR submitted by a PAR evaluator
- **SLW (State License Waiver) Endorser:** Person at the MTF (usually the privileging authority) or Command (usually the Command Surgeon) who is responsible for review and approval of physician SLW requests. Authority to approve the SLW is usually delegated to such an individual from the Office of the Assistant Secretary of Defense for Health Affairs (OASD/HA)

All permissions will default to "No", so that action must be taken only on permissions that should be granted to the user. With the exception of the CC/MSSP/CM and CVO roles, most users only require access to the Privileging module and the permissions may be set by selecting the appropriate radio buttons for each role that the user will perform.

Note: When granting access to the Privileging module, it is important to select the "Yes" radio button for **Privileging Module**, in addition to the individual role(s) that need to be assigned to the user. This will ensure that the user has access to the Privileging main menu when they log into CCQAS.

Persons performing the CC/MSSP/CM and CVO roles typically require access to multiple modules to include Privileging, Credentialing, System Administration, and Reporting modules. Access to these other modules may be granted by designating tab- and screen-level permissions for the other modules listed on the Permissions tab.

The Service administrator, or whoever the Service designates as the system administrator for CCQAS, should pay special attention to the permissions within the System Admin and Reporting tabs especially for the CVO if it is required to perform batch NPDB queries. The “Batch NPDB Request Flag” permission in the System Admin tab and the “NPDB Query” permission within the Reporting tab (Exhibits 2.3-13 and 2.3-14) should be enabled for the CVO if it is intended for this office to perform batch NPDB queries.

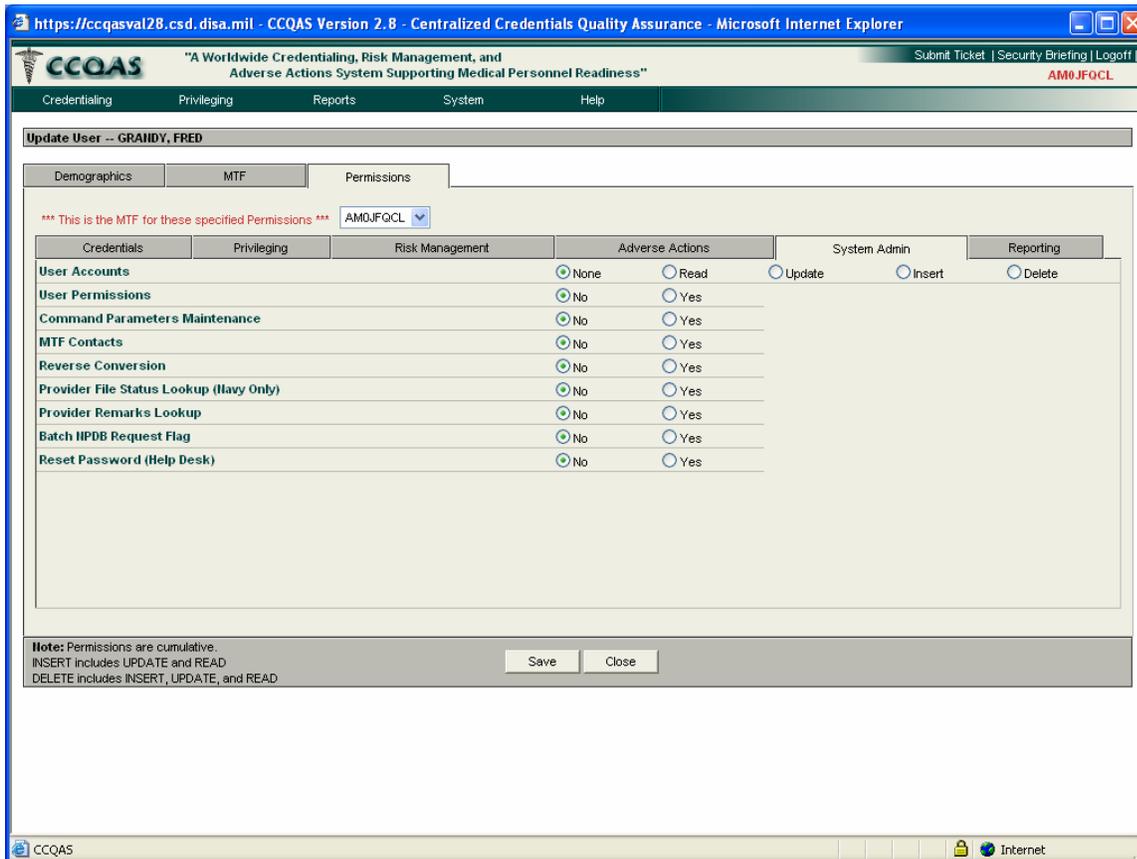


Exhibit 2.3-13. Access Permissions Within the System Admin Tab

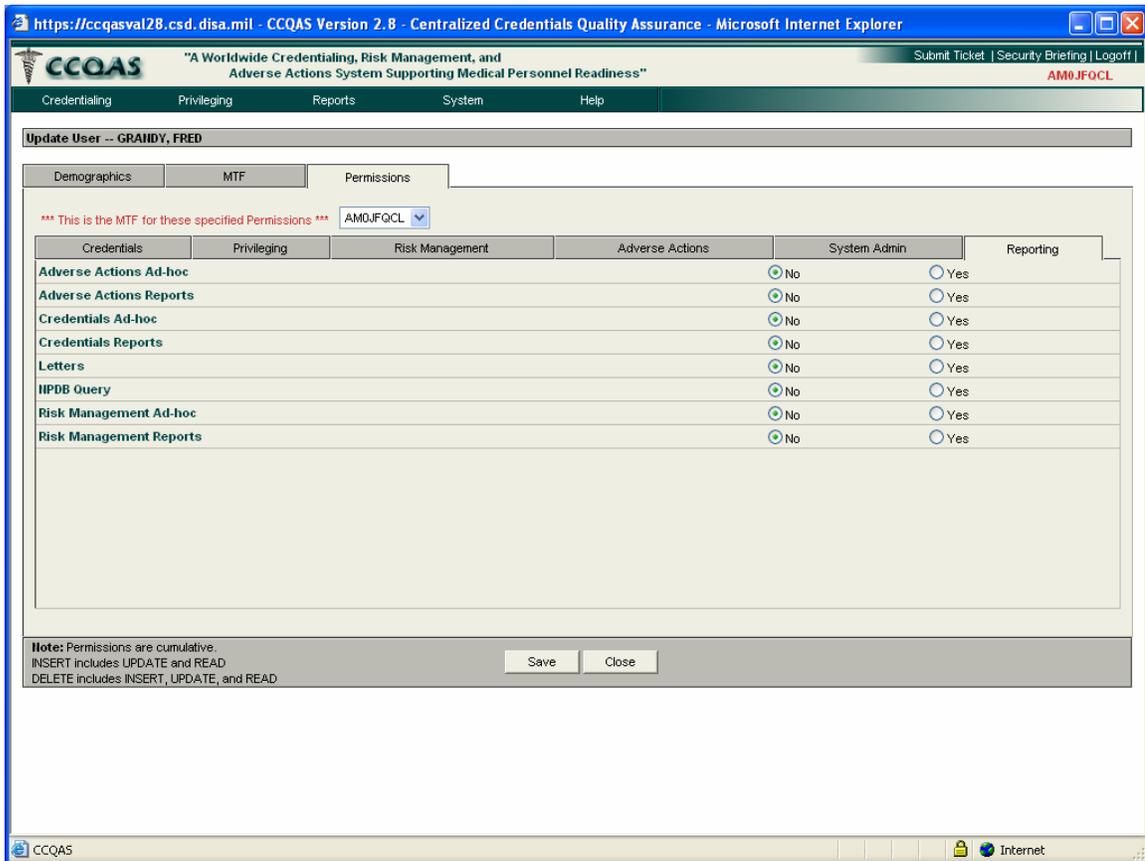


Exhibit 2.3-14. Access Permissions Within the Reporting Tab

User Management within CCQAS allows anyone who has permission or permissions to grant other users permission(s) equal to what the “grantor” already holds. Permission to access the Risk Management and Adverse Actions modules (Exhibit 2.3-15 and 2.3-16), for example, cannot be granted by a CC/MSSP/CM or CVO who does not him- or herself have permission to access these modules/tabs/screens. CC/MSSP/CMs who have been assigned the responsibility of processing CCQAS user accounts should have the capability to grant any of the roles on the “Privileging” tab to users at their respective units. Their ability to grant permissions to the “Credentialing” and other CCQAS modules, however, will be limited to only those permissions that they themselves hold. CCQAS will not allow a CC/MSSP/CM to grant to others permissions in these modules that are more expansive than their own.

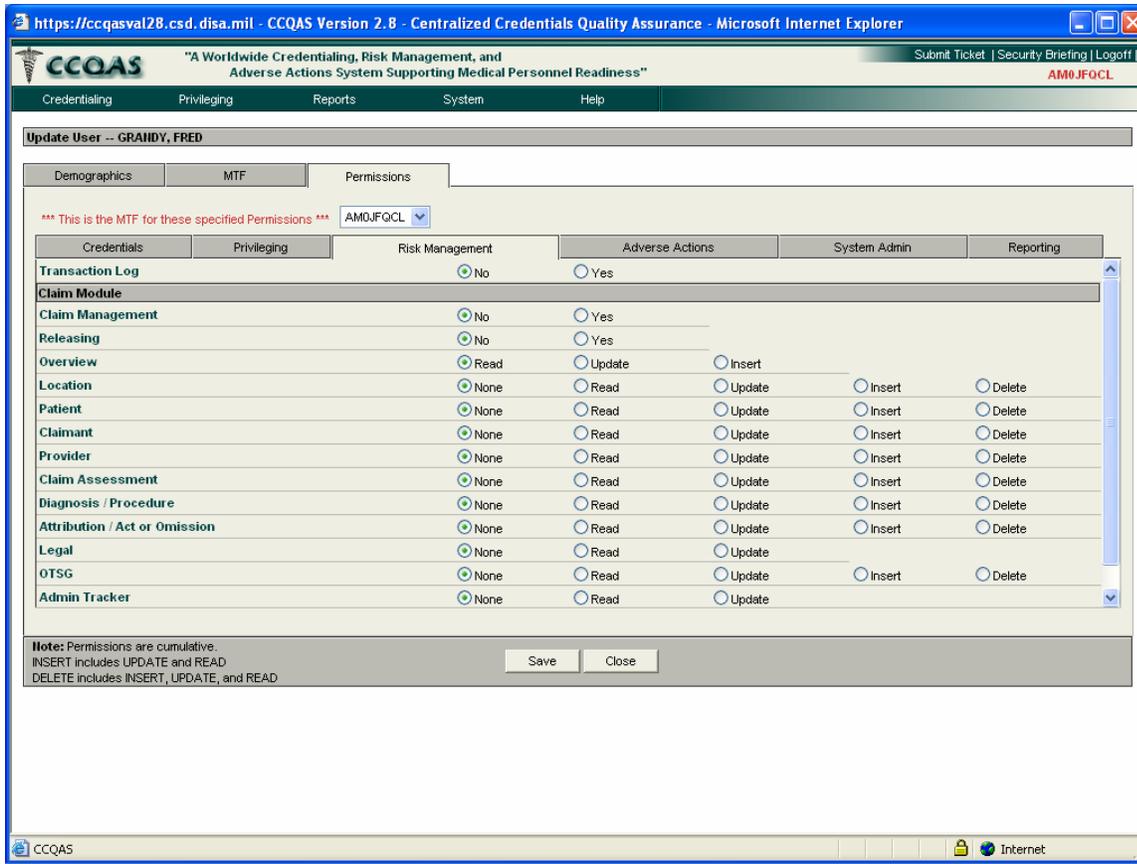


Exhibit 2.3-15. Access Permissions within the Risk Management Tab

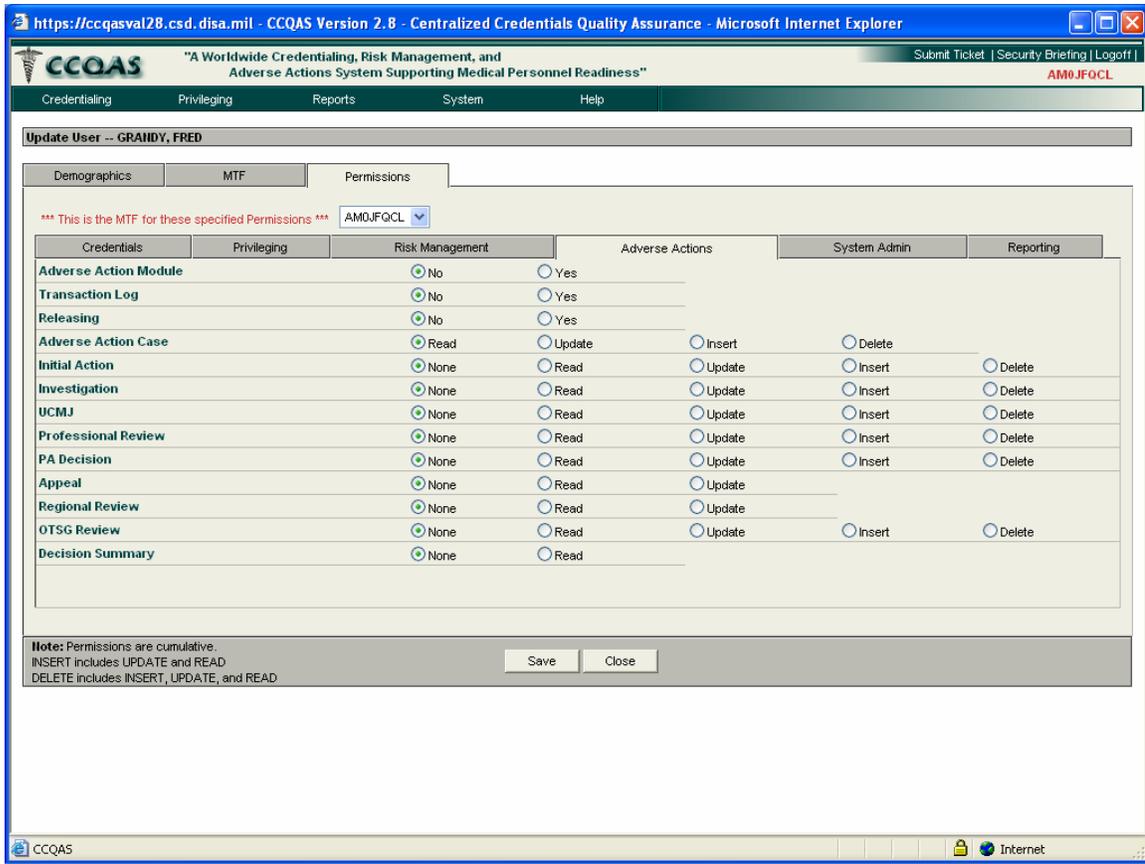


Exhibit 2.3-16. Access Permissions within the Adverse Actions Tab

The permissions may be saved to the user account by clicking <Save> and then <Close> to complete the processing of the application.

Once created, the role of *Provider* and additional roles as *Other (Module Users)* may be added to the user's account. The process of adding roles to an existing account is addressed in Section 3.

2.4 Generating User Accounts from Existing Provider Credentials Records

CCQAS allows CC/MSSP/CMs to generate a user account for providers who already have an active credentials record in the CCQAS database. To initiate this process, the CC/MSSP/CM will perform a search for the provider's record in the Credentialing module. On the "Search Results" tab, click on the hidden menu of actions for the provider's credentials record and select "Grant Provider Access" (Exhibit 2.4-1).

Note: The "Grant Provider Access" option can also be used for providers with access to CCQAS as an *Other (Module Users)* but who have not as yet been granted access as "*Provider Applicant*".

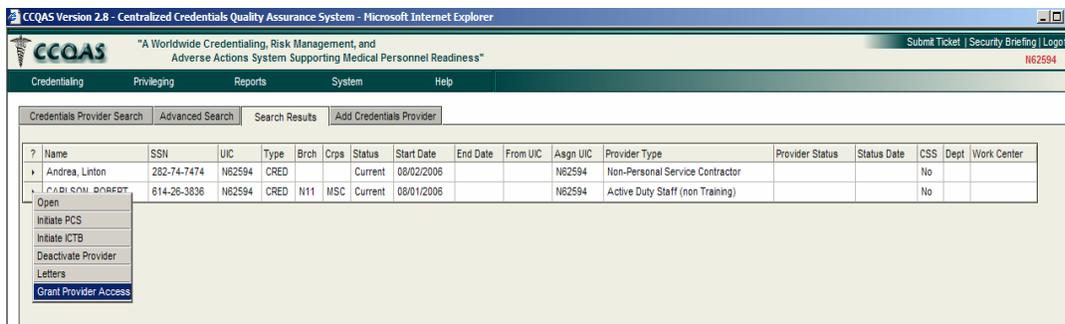


Exhibit 2.4-1. Grant Provider Access Menu Item

CCQAS will use the information inside the provider’s credentials record to create the new user account, and return the CC/MSSP/CM to the “User Application” screen (see Exhibit 2.3-4). The CC/MSSP/CM may then proceed with processing the user account, as described in Section 2.3.

The “Grant Provider Access” function has several important features:

- This function will only associate the Provider role with the user account; it cannot be used to grant other roles such as Reviewer, or Privileging Authority to the individual
- This function may only be performed once. The menu item will disappear once an active credentials record has been associated with a user account
- The provider’s 1st E-Application for clinical privileges will automatically generate. This application will be prepopulated with the credentials data from his/her current credentials record (see Chapter 5 for a discussion of the 1st E-Application)

Once created, additional roles as a “Privileging” module user may be added to the provider’s user account. The process of adding roles to an existing account is addressed in Section 3.

2.5 Receiving a New Userid and Temporary Password

Once a new user account has been set up, CCQAS will notify the new user of their userid and a temporary password via an automated email message. Passwords for CCQAS are automatically generated and consist of a random string of characters, numbers, and symbols that conform with DoD Information Systems security requirements as follows:

- Eight characters in length
- Contain at least one uppercase letter
- Contain at least one lower case letter
- Contain at least one number
- Contain at least one special character

The userid and the password are both case-sensitive.

Note: Do not use the Caps Lock feature when entering the userid and password.

The userid and temporary password issued to a new user will be valid for 90 days from the date the account was created. If the new user does not log onto the application at least once within this 90 day time period, the CCQAS-issued password will be deactivated and the user will have to request a new password from the CC/MSSP/CM.

2.6 Accessing CCQAS for the First Time

A number of actions are required the first time a user accesses CCQAS. These include:

- Loading security certificates
- Reviewing and acknowledging the security briefing
- Changing the temporary password
- Verifying user roles and permissions

Optional actions that help users streamline their access to the CCQAS include:

- Creating a desktop icon for CCQAS
- Changing the start page

Each of these actions is described in the sections below.

2.6.1 Loading Security Certificates

Certain rules pertaining to security have to be adhered to when accessing an automated information system within the Department of Defense network. When accessing CCQAS for the first time, network protocols may present the first-time user with a message requiring the loading of security certificates into his/her computer to protect data that is sent across the Internet. The user will be brought to another link for instructions and a wizard function for these certificates which must be downloaded and retained in the user's computer hard drive prior to using CCQAS.

2.6.2 Logging onto CCQAS

To log on to CCQAS, the user enters their userid and password in the appropriate fields on the Log-on screen (Exhibit 2.6-1) and clicks <**Login**>. Both the userid and password for CCQAS are *case sensitive*. Use the [Shift] key, rather than the [Caps Lock] key. The userid is always upper case.

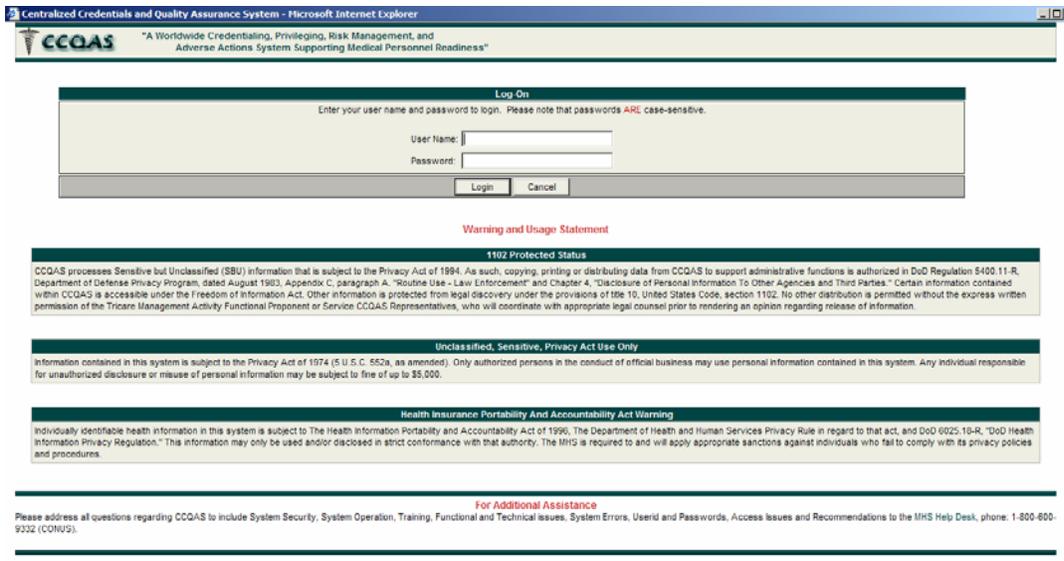


Exhibit 2.6-1. Log-On Screen

If the user unsuccessfully attempts to log on more than three times, their user account will receive a message that their account has been locked. The user must contact their CC/MSSP/CM or the CCQAS Helpdesk to have their account unlocked before proceeding.

2.6.3 Security Briefing

Upon logging on, the user will be presented with a security briefing (Exhibit 2.6-2).

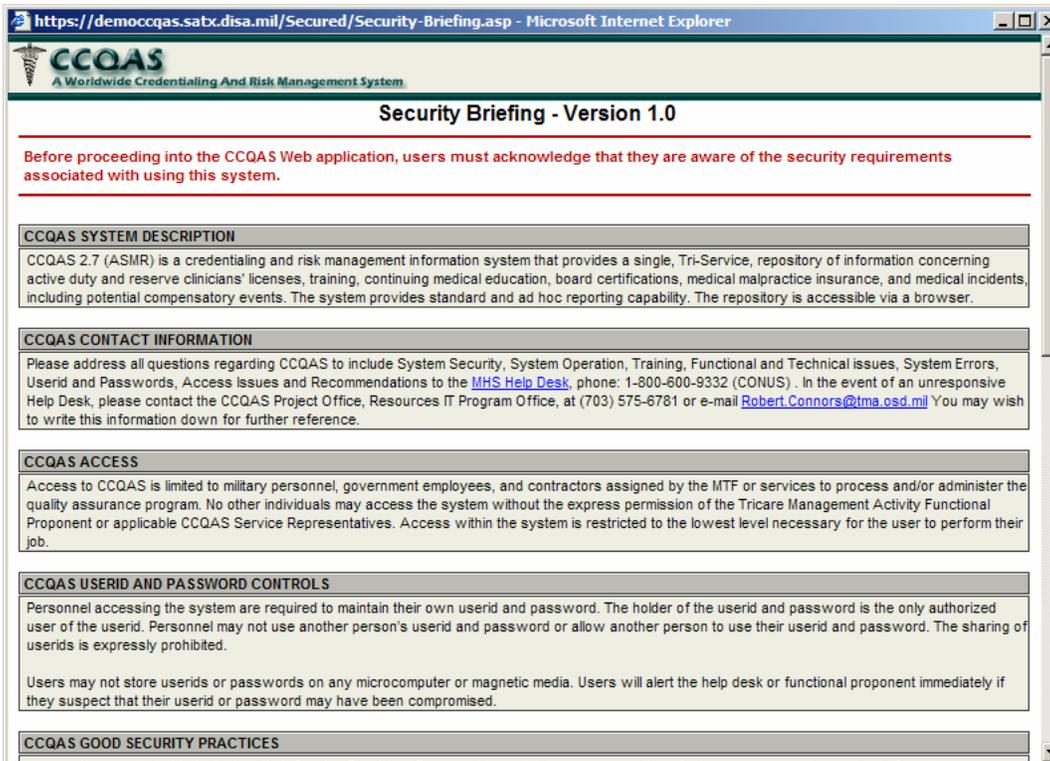


Exhibit 2.6-2. Security Briefing

The user must read the briefing, acknowledge their understanding of the information it contains by selecting the appropriate radio button at the bottom of the briefing, and clicking <Submit>. After doing so, the logon process will be completed.

2.6.4 Changing a Temporary Password

Upon logging on for the first time, the user will be prompted to change their temporary password (the userid will remain unchanged). CCQAS will randomly generate a new password for the user. The user has to click on the <I like this password> button if the password is acceptable; otherwise the system will generate a new one every time the <I do not like this password> button is clicked. Once this new password is issued, it will be known only to the user; the CM/MSSP/CC will not have any record of the new password. The userid and new password should be committed to memory by the user. The storage of this information in written form on or around the user's workstation puts the integrity of the password at risk. Once assigned, an active password will be valid for 90 days.

2.7 Frequently Asked Questions

FAQ: A user received their userid and temporary password via email a few weeks ago, but CCQAS will not accept the password that was given to them. What should I do?

Answer: If more than 90 days have lapsed since the user received the email message containing their new userid and temporary password, then their password has expired and a new temporary password will need to be issued. This can be done through the “User Processing” function. Open the System menu and select “User Processing”. Then open the user’s account and click <**Issue New Password**> on the “Demographics” tab. The user will then receive a new temporary password via an email message. The user will then have 90 days to log on to CCQAS using the temporary password and select a new password.

FAQ: A user’s CCQAS password has expired. What should I do?

Answer: If a user’s password has expired, a new temporary password will need to be issued. Follow the guidance provided in the previous FAQ to issue the new password.

FAQ: A user forgot their password. What should I do?

Answer: If a user has forgotten their password, a new temporary password will need to be issued. Follow the guidance provided in the first FAQ to issue the new password.

FAQ: CCQAS will not allow one of my users to log in, but I know they are using a valid password. What should I do?

Answer: If a userid and password are both current and valid, it is likely that the user’s account has been locked. An account will be locked after three consecutive logon attempts fail using the same userid. Most often, lock outs occur as a result of user error when entering the case-sensitive password. Please consult Section 3 of the guide for a discussion of locking and unlocking accounts.