PrognoCIS Login Credentials

Once a user is created, appropriate credentials can be assigned to provide access to the system. Initial permissions are determined by the user's primary role under which his/her profile is created. Individual users can then be given additional/different permissions by assigning additional User Roles as applicable. This enables you to have multiple security levels, such as Intake MA, Clinical MA, Script MA, etc. as applicable per local workflow.

When defining a **User Id** and **Password**, the User ID does not change and is not case-sensitive. Passwords may be changed at any time and are case-sensitive. Whenever a password is defined (whether new or reset), it is good for one time only and immediately expires the first time it is used. By default, passwords do not expire automatically unless appropriate settings are configured per local preference.

Creating a User

1. Select **Settings ⇨ Configuration ⇨ Medics**
2. Select the appropriate User Type

Clinic	Medics	Vendors
Locations	Designation	Lab
Holidays	Specialty	Radiology
Pref ICD	Providers	Pharmacy
Pref Cpt/Hcpc	Resource	Insurance
Pref Drug	Medical Assistant	Employer
Pref LAB	Clinical Staff	Items
Pref RAD	Admin Staff	Attorney
Enc Types	Ref Doctors	Ins Adjuster
In-House Drug	Billing Staff	EDI Codes
Pref Family History	Address Book	Clinic Codes

   a. **Providers** – Physicians, Nurse Practitioners, or Physician Assistants who have a PrognoCIS license
   b. **Medical Assistants** – clinical users who are not otherwise designated as nurses, technicians, etc.
   c. **Clinical Staff** – clinical users such as nurses, technicians, phlebotomists, etc.
   d. **Administrative Staff** – non-clinical users such as receptionists, verifiers, schedulers, etc.
   e. **Billing Staff** – applicable only for users of the Practice Management module

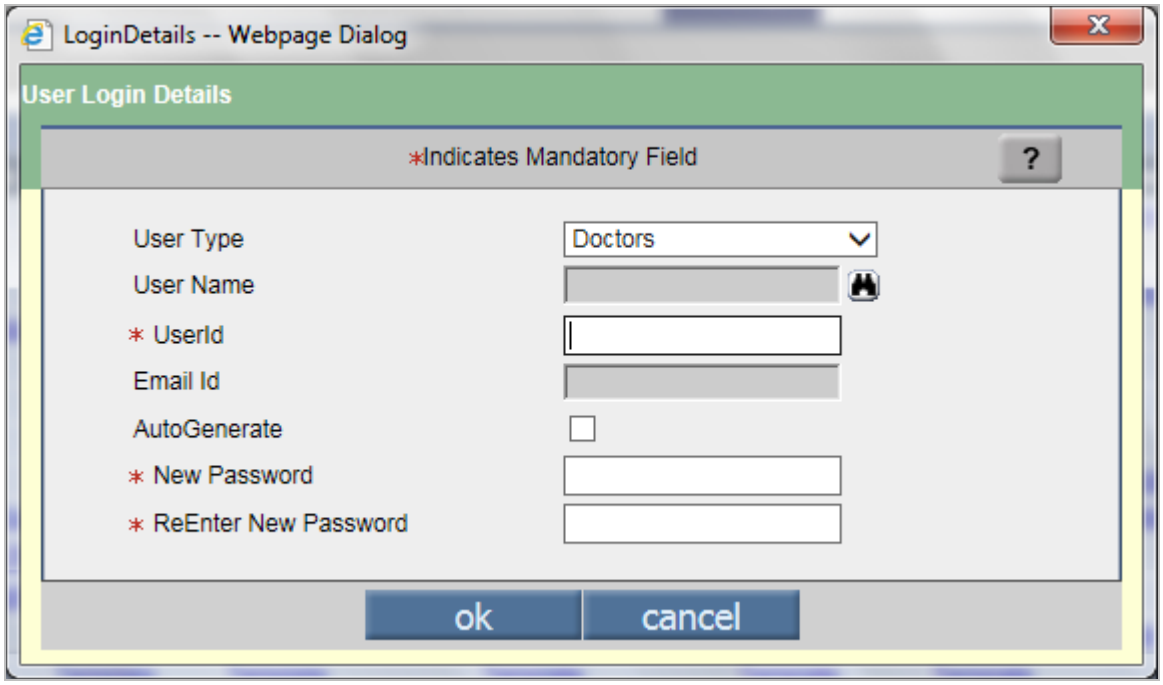
For each user, only the first and last names are mandatory to save the profile. You are able to store other details about the user if applicable within your practice. It is recommended to also assign an appropriate **Designation** (or title) to help distinguish rights under the **User Role** function.

Note: *For practices who like to have system-generated passwords for confidentiality, the user's email is required so the system can email the password when it is changed. When no email is entered, passwords will have to be manually set and communicated to the user.*

Defining a User Login

Initial permissions are determined by the user's primary role under which his/her profile is created. User IDs are not case-sensitive and can be up to 50 characters long. Passwords are case-sensitive and must be alpha-numeric. The length of the password by default is between 8 & 10 characters, but this can be modified to a maximum of 20 characters per local preference. Credentials can be system-generated for randomness, or you can override them when manually creating the record for a user.

1. Select **Settings ⇨ Configuration ⇨ Admin ⇨ Login Details**



2. Select the **User Type** by clicking .

3. Select the **User Name** by clicking .
   Note: *The Search screen that displays will reflect the User Type selected in the previous step*.

4. Define the desired **UserId**.
   Note: *The system defaults to a system-generated string based on the user's name; however, this may be changed to any desired string of text unique to the user. It is not case-sensitive*.

5. The **Email Id** will default from the user profile if it was entered.

6. Select the **Auto Generate** check box ( ) if you would like the system to generate a unique password for the user. If this option is selected, you can skip steps 7 and 8, as those fields will be disabled.
   Note: *This requires that an Email Id be assigned to the person in order for the password to be communicated to the user securely.*

7. Enter the desired **New Password**.
   Note: *By default, passwords must be between 8 and 10 digits long; must include at least 1 alpha and at least one numeric character. Alpha characters are case-sensitive. Some special characters are not allowed.*

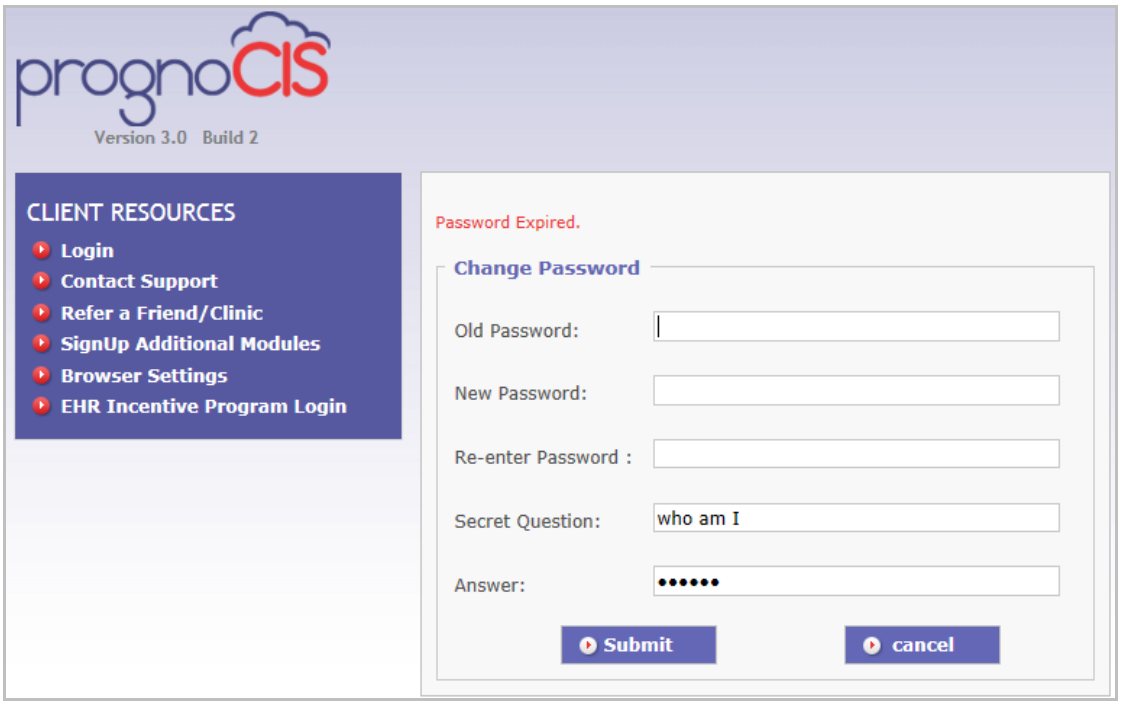
8. To verify accuracy, **ReEnter New Password**.
   Note: *This must be re-typed exactly as it was originally defined above*.

9. Click **OK**.

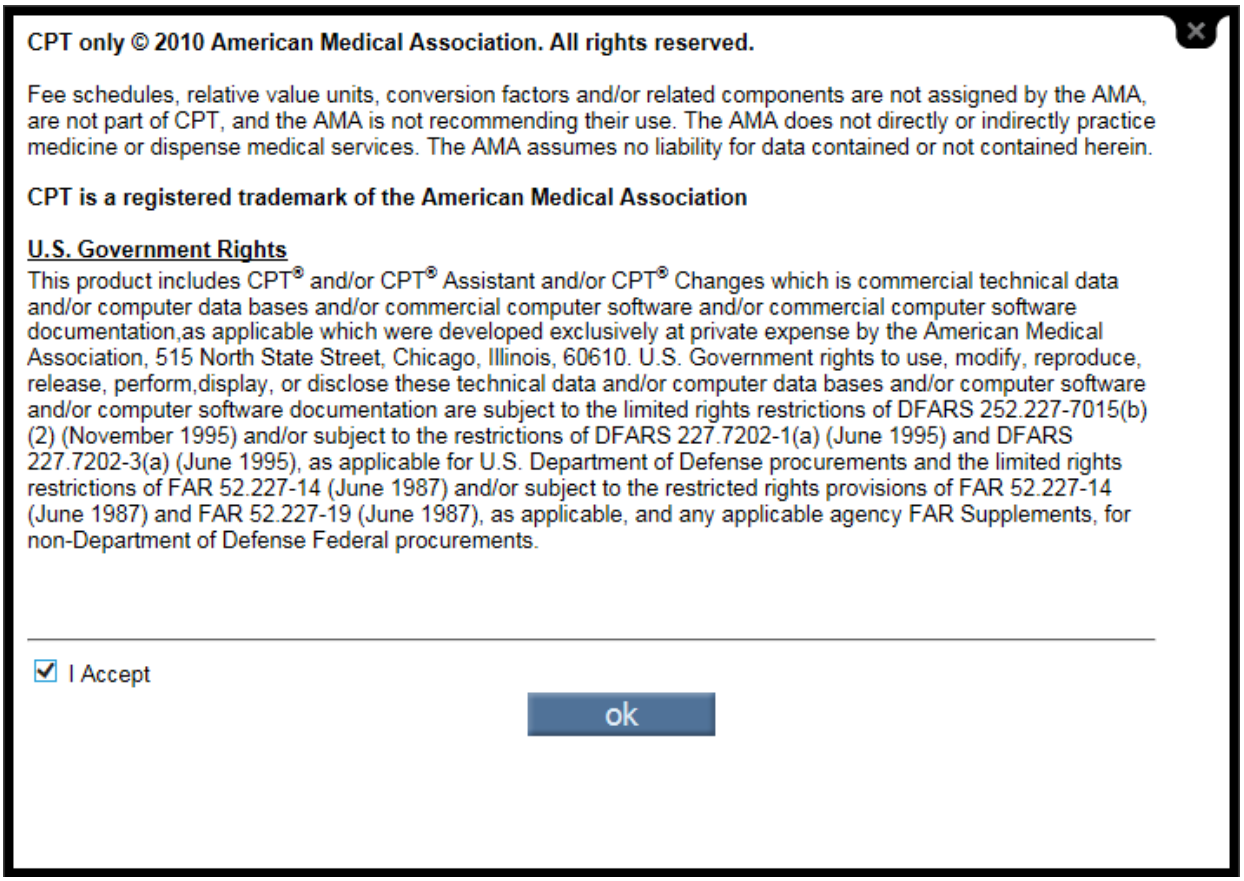
Note: *Though not shown above, practices who use the multi-location setup will have the additional step of selecting each location or locations the user requires access to. There will be a Location drop-down field in these cases. A multi-location setup is* ***not the same*** *as a practice with multiple office locations.*

Logging into PrognoCIS the First Time

For all users, the first time a password is used to login to PrognoCIS, it will expire. This applies to first time users with a brand new password as well as existing users whose password must be reset. Every time an administrator creates or resets a password, it is valid for one use only and immediately expires the first time it is used.



- Enter the old password again
- Enter the new password you desire twice
- Enter a security question and answer
- Click **Submit**. The login screen will display and you can login using the new password. The License Agreement page will display for you to acknowledge and accept (☑). This occurs only once for every new (or reset) password.



Defining User Permissions

Based on the Medics type under which the user's profile is created, the primary permissions are defined (such as Read, Update, Create, Approve, or Deny) per each feature within each module of the application. These defaults can be modified locally; however, changes made are applicable at the Role level, meaning they apply to all users created under that Medic type.

To accommodate individual permission requirements, such as "Super Users" or "Managers" who require the base permissions + additional elevated permissions, we have the User Role. A user can have unlimited User Roles in addition to his/her primary role dictated by the user profile. In addition, you can locally create special "User Roles" to accommodate very specific scenarios in your practice.

Please see the *User Permissions and User Role* User Quick Guide or Training Video for more information.