

Welcome!

CAREWare Quick Starts will walk you through the basics of setting up, managing and using basic CAREWare functions. They're not a replacement for the CAREWare User Manual, which is where you'll need to go to learn about more advanced functions. This material is for non-technical users who just need to get information in and out of CAREWare with no worries.

About This Guide #9: User and System Administration

Other guides in this series are:

1. *Downloading and installing CAREWare*
2. *Creating contracts and services*
3. *Entering Clients and their Service and Clinical Data*
4. *Customizing tabs and fields*
5. *Customizing clinical data*
6. *Prebuilt reports (including the Ryan White Annual Program Data Report)*
7. *Creating basic custom reports*
8. *Creating more advanced reports*
9. *User and System Administration*

First Things First

What do I need to get started?

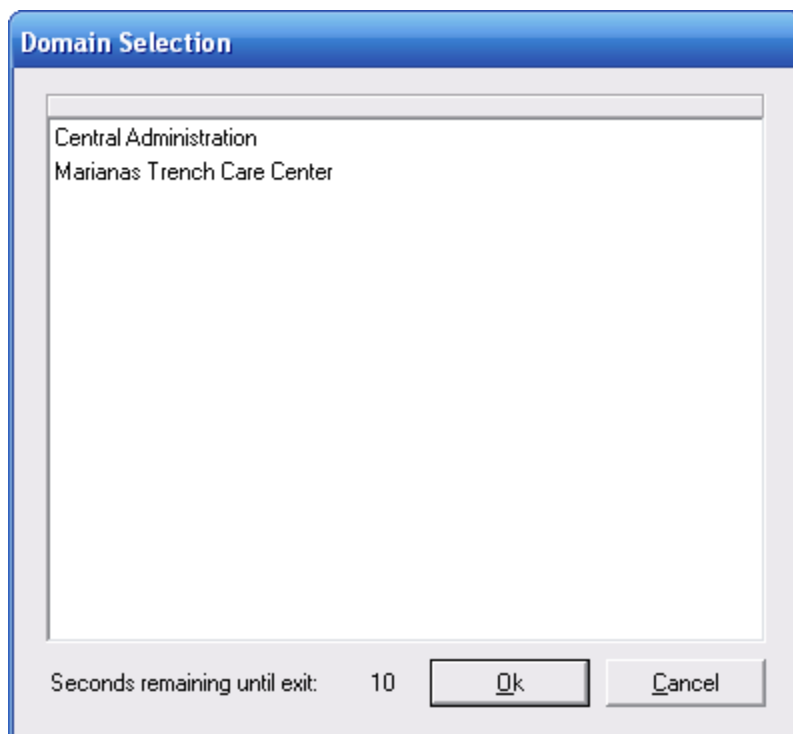
You must have the appropriate administrative privileges to add/modify users and their privileges.

Creating new Central Administration users

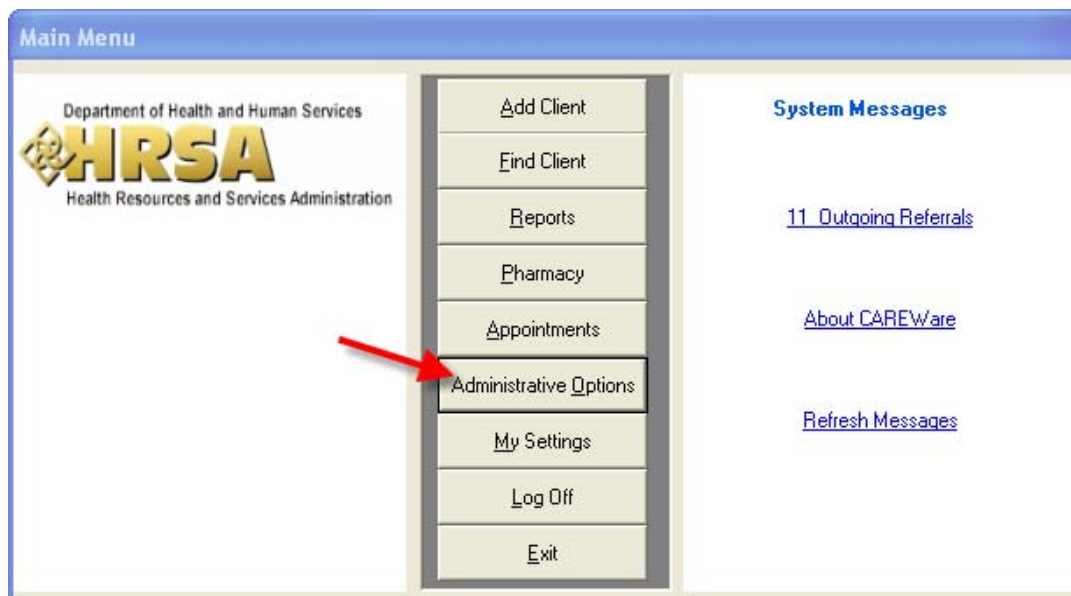
CAREWare comes with a single, preinstalled user, **cwtemp**, with the default password **TEMPCW100**. All passwords in CAREWare are **case-sensitive**, meaning that if you create a password like “connie,” you can’t type “Connie” when you log in. User **cwtemp** comes with all system privileges, so you can log in initially and create your real users and their system privileges.

The Health Insurance Portability and Accountability Act (HIPAA) requires us to take certain steps to protect the privacy and security of our clients’ protected health care information. One of these steps includes eliminating the **cwtemp** user after you’ve set up your real users, as this is a publicly available login ID that anyone could find on the Internet and use to log into your database if you haven’t deleted it.

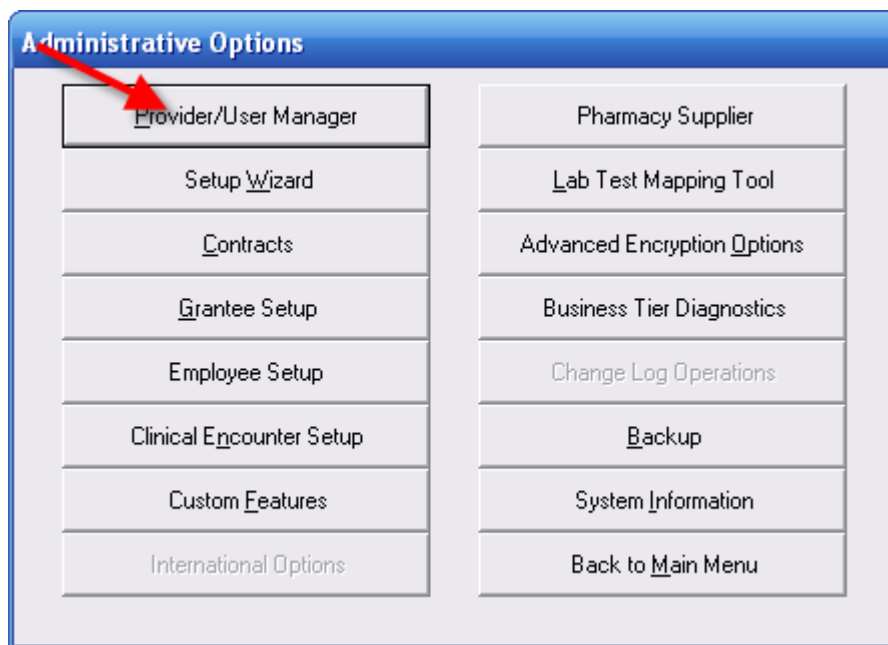
1. If you are just setting up CAREWare, log in with the cwtemp login. Otherwise, log in with a user ID that already has full administrative privileges. You will see a screen that will give you the option to log in to **Central Administration** or either **Default or Your Provider Name**, depending on how far your system has already been configured. Our sample database has already been configured, so its name appears here.
2. Choose **Central Administration**. For security reasons, you only have 20 seconds to choose one or the other.



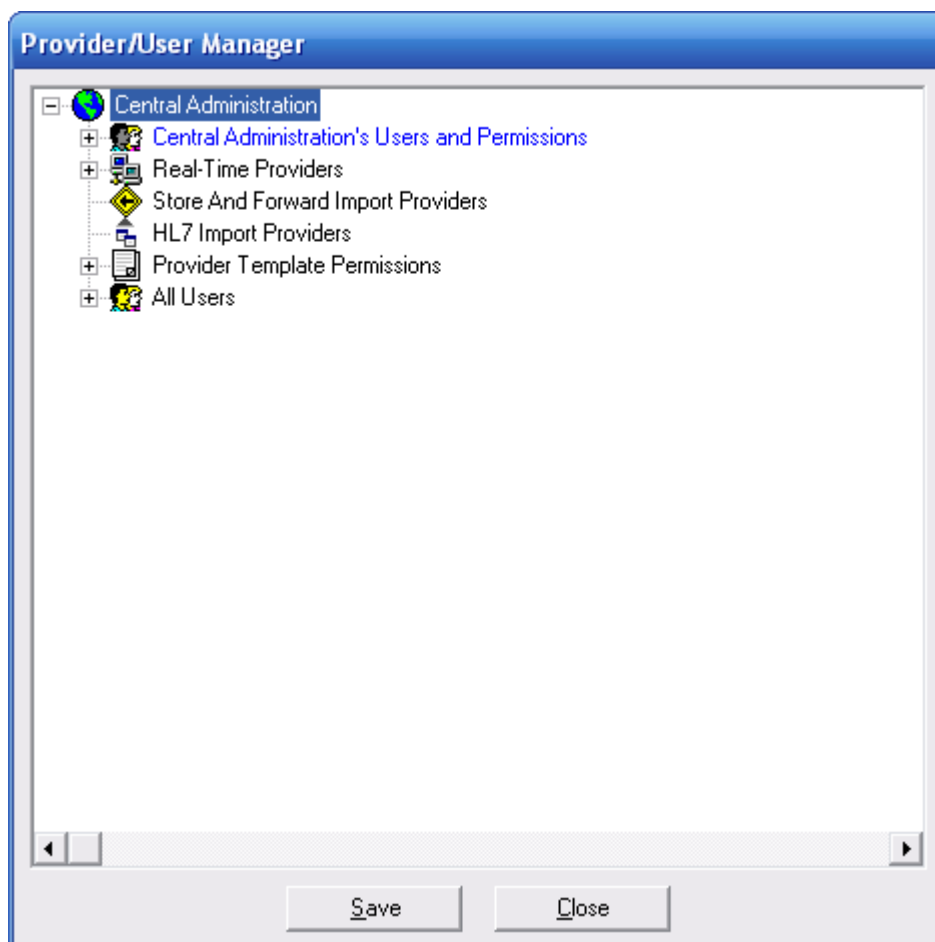
3. The main menu will appear. Select **Administrative Options**.



4. The menu will appear. From that menu, select **Provider/User Manager**.



5. The **Provider/User Manager** screen will appear.



There are two levels of users in CAREWare:

Central Administration Users. With these privileges, you can:

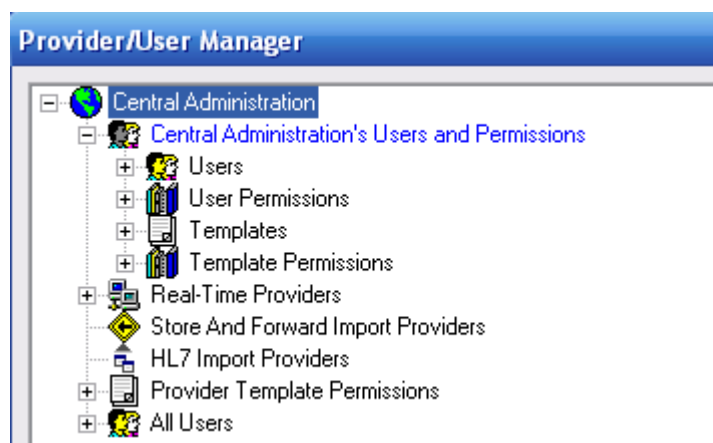
- Configure other admin users and their permissions
- Configure providers and their permissions
- Configure provider users and their permissions

Provider Users. With these privileges you can:

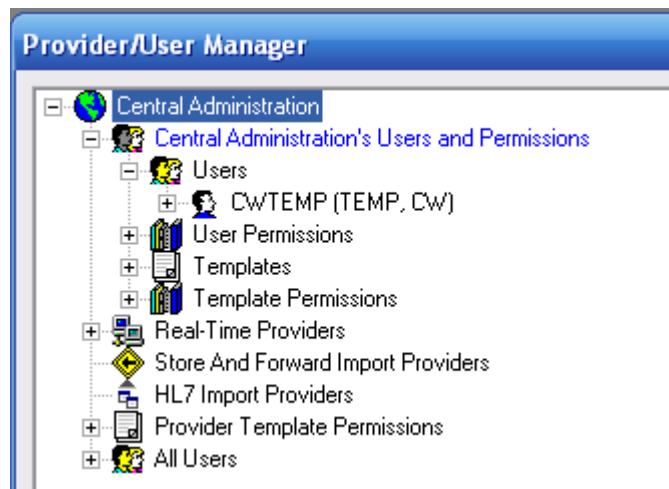
- Configure provider users and their permissions.

Central administration is divided from the provider because many Part A (formerly Title I) agencies have a CAREWare database shared by a number of providers, and one office that performs central administration. Even if you are a stand-alone provider, you will have to start at the top level and use Central Administration to configure your agency.

6. Click on the + sign next to **Central Administration's Users and Permissions.**



7. Click on the + sign next to **Users.**



If you are configuring CAREWare for the first time, you'll only see the one user, **cwtemp**. Be careful – all user names appear in CAPS in the Provider/User Manager, regardless of whether or not the real user name is part or all caps. You might want to make all your user names lower case.

8. Right click on **Users**. You'll see the option to **Add User...** Select it.



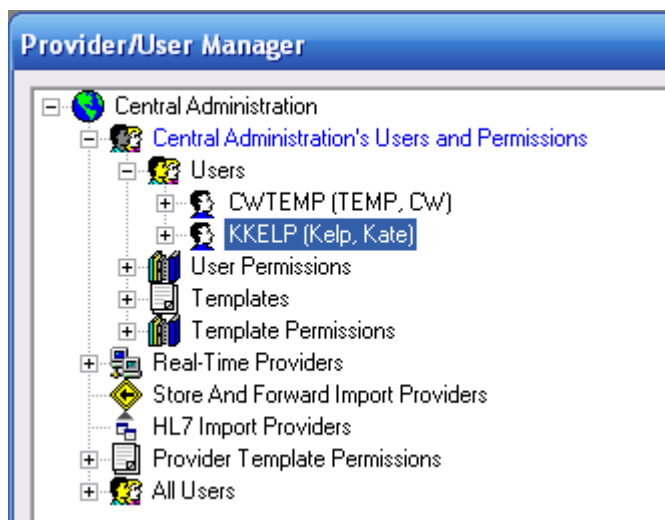
9. You'll see a menu similar to the one you use to enter new clients. You must enter a username (it will appear in all caps), first and last name, and a password of at least 8 characters. Passwords are case-sensitive. **HIPAA compliance** requires you to select a password that:
 - a. Is not easy to guess (i.e. many, many systems use “password” as their password)
 - b. Has an alphanumeric combination (i.e., you might want to select a word and replace its vowels with numbers and symbols, i.e., “d1d@ct1c” for “didactic”)
 - c. Is changed on a regular basis (every 90 days is typical in many corporate environments).

The 'Add User' dialog box contains the following fields and buttons:

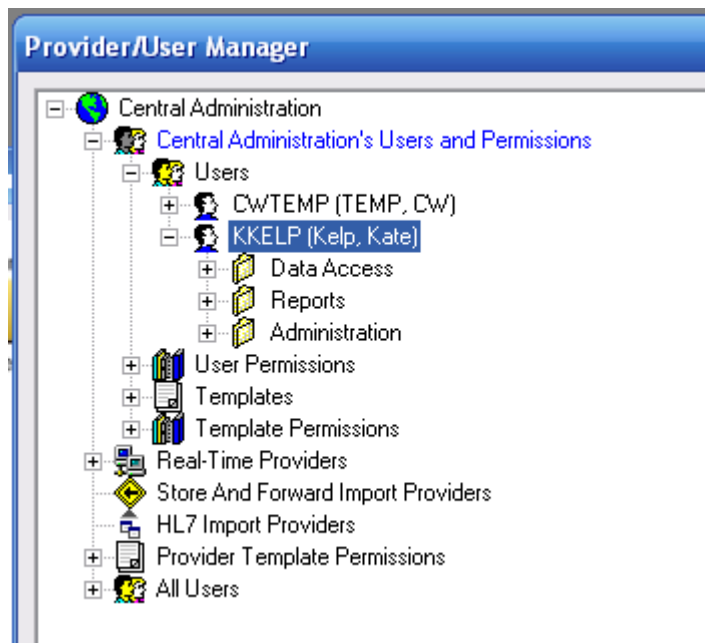
- User Name / Login ID: KKELP
- First Name: Kate
- Last Name: Kelp
- Phone: (empty field)
- Email: (empty field)
- Password: (masked with asterisks)
- Repeat Password: (masked with asterisks)
- Buttons: Add, Cancel

Phone and email are optional fields.

10. Click **Add**. You'll see the new Central Administration user.



11. Click the + next to the new user.

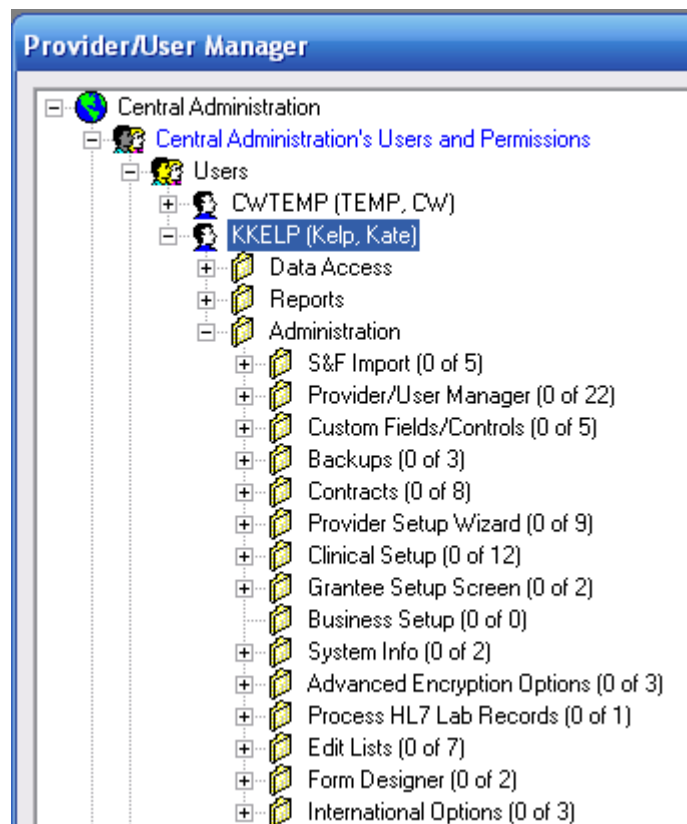


In both Central Administration and Provider levels, permissions are divided into three categories: **Data Access**, **Reports**, and **Administration**. **Data Access** permissions cover viewing and entering all demographic, service, clinical, and other data. **Reports** covers access to prebuilt and custom reports. **Administration** covers user management, modifying contracts, services, custom fields, medications and lab lists, and any other alterations to CAREWare.

HIPAA compliance requires you to set up your users on a “need to know” basis, i.e., with only the privileges they need to do their job. You will need at least one person who has all permissions, which should be the person who will be administering your system, as well as another person who can act in

their stead (for instance, you may have an office manager who does the system administration, with your executive director as a backup person).

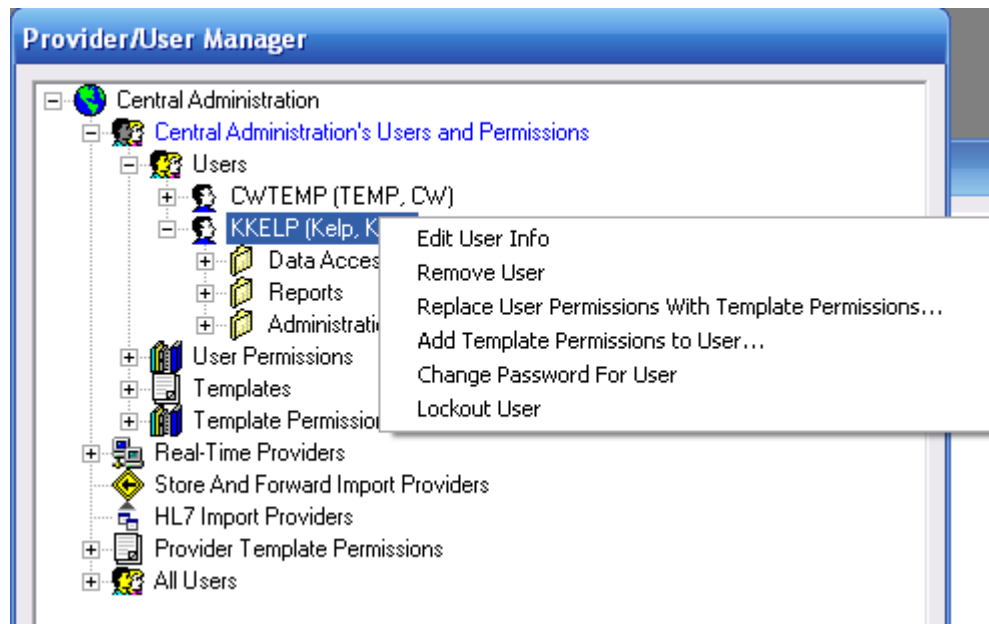
12. Click on the + sign next to your new user's **Administration** privileges. New users are created with no privileges, so you will see "0 of 22" next to Provider/User Manager, etc.



While you can add groups of permissions or individual permissions to each user, we recommend using **templates**. Templates are sets of permissions configured for a certain type of user, for instance, a receptionist, a case manager, a clinical provider would each have certain "need-to-know" privileges. We'll walk through creating templates shortly.

Right now, we're going to apply the one template that comes with CAREWare, which is "All Permissions."

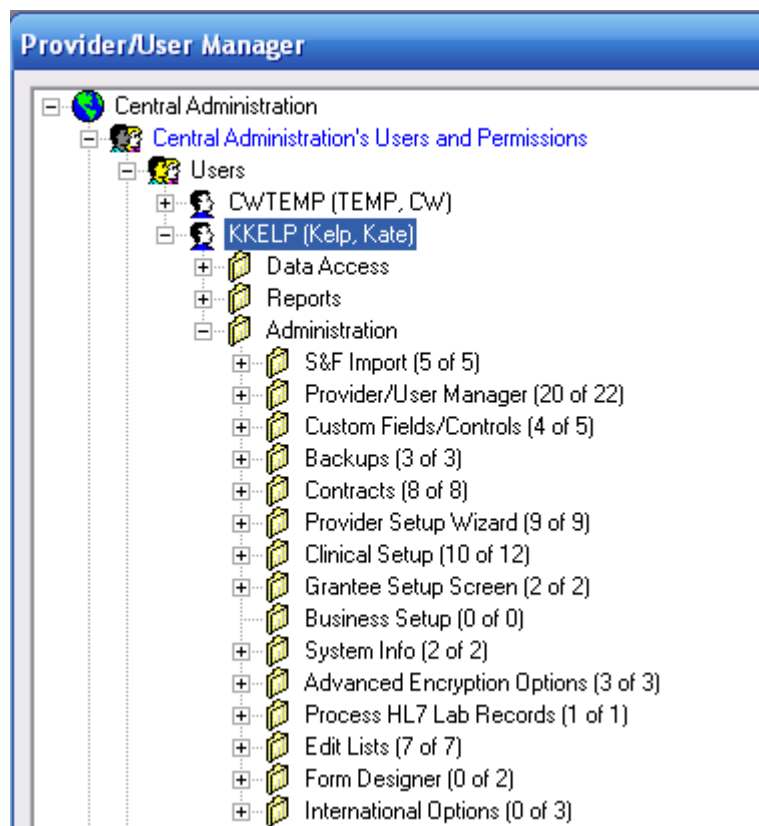
13. Right click on your new user's user name. You'll see a list of options. Choose "Replace User Permissions with Template Permissions."



14. You'll see the following window. You can use the drop down menu to see all the templates in your system; at first, only "All Permissions" is listed.



15. Click **Replace**, then click on the + sign next to your new user's **Administration** privileges. Now, instead of "0 of 22," etc., you see your new user has full administrative privileges in Central Administration. (Permissions still listed as "0 of" are either not applicable to domestic CAREWare installations or are configured elsewhere.) Click on the + sign next to **Data Access** and **Reports** to see that these privileges have also been granted.

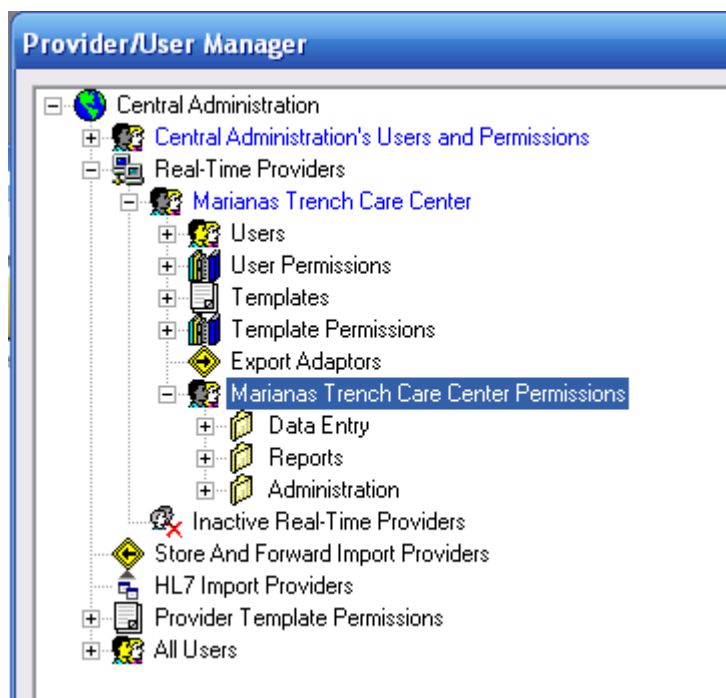


16. Click the **Save** button at the bottom of the window to save your changes.

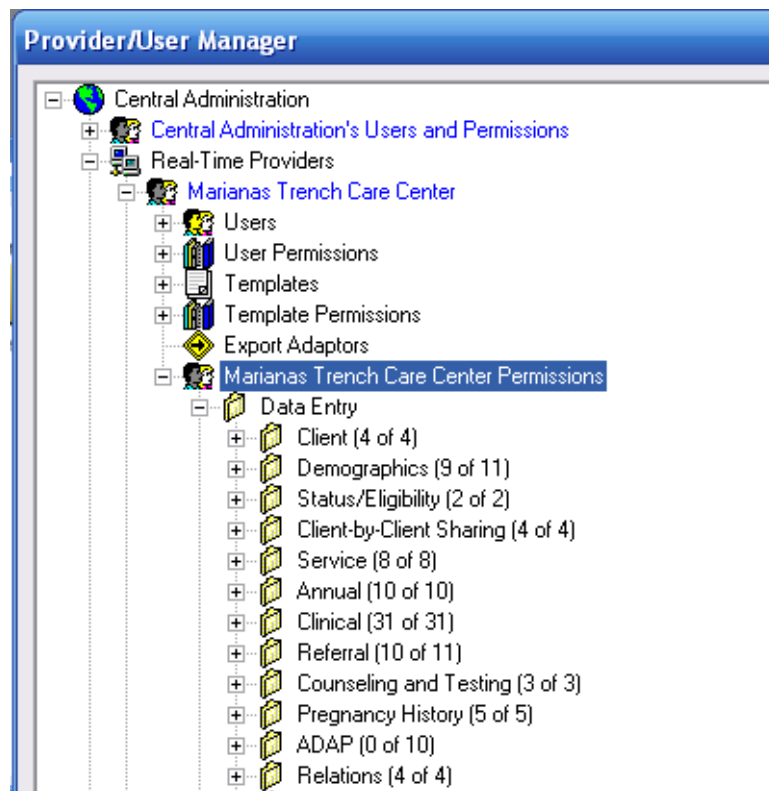
Configuring Provider Permissions

Once you've set up your Central Administration user, it's time to set up your provider permissions. These will restrict the permissions available to users at the provider level. For instance, as the central administrator, you may want to control whether or not your provider or providers can make changes to contracts. By restricting the provider's permissions, you make it impossible for any user at that provider to change those configurations. These permissions have to be administered at the Central Administration level.

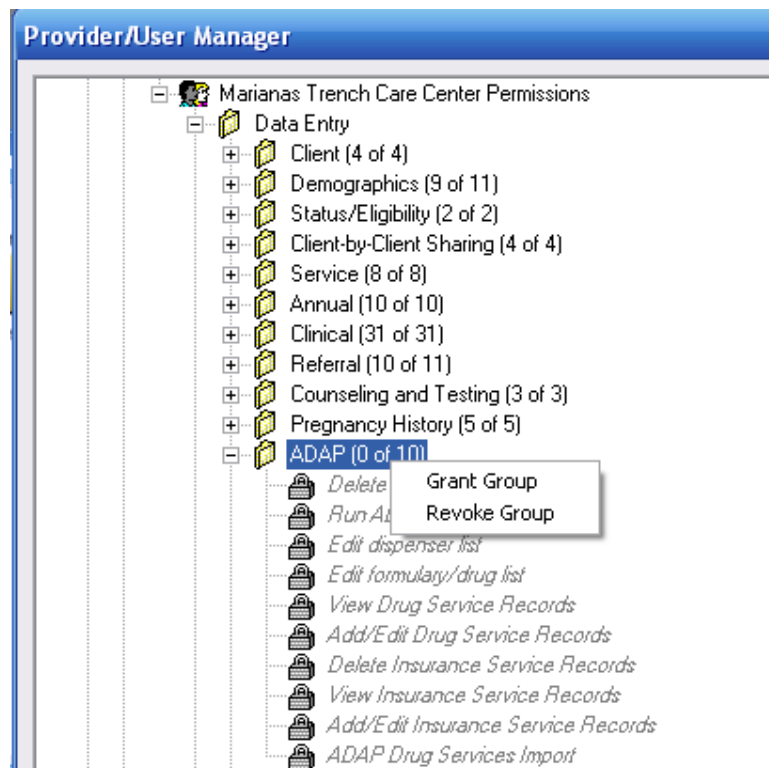
1. Click the – button next to any users or permissions you have open, then click the + sign next to **Real-time Providers**. If you only see “Default,” don't worry; we'll change that later. Then click the + sign next to **Default Permissions** (or your agency's name if it's already there).



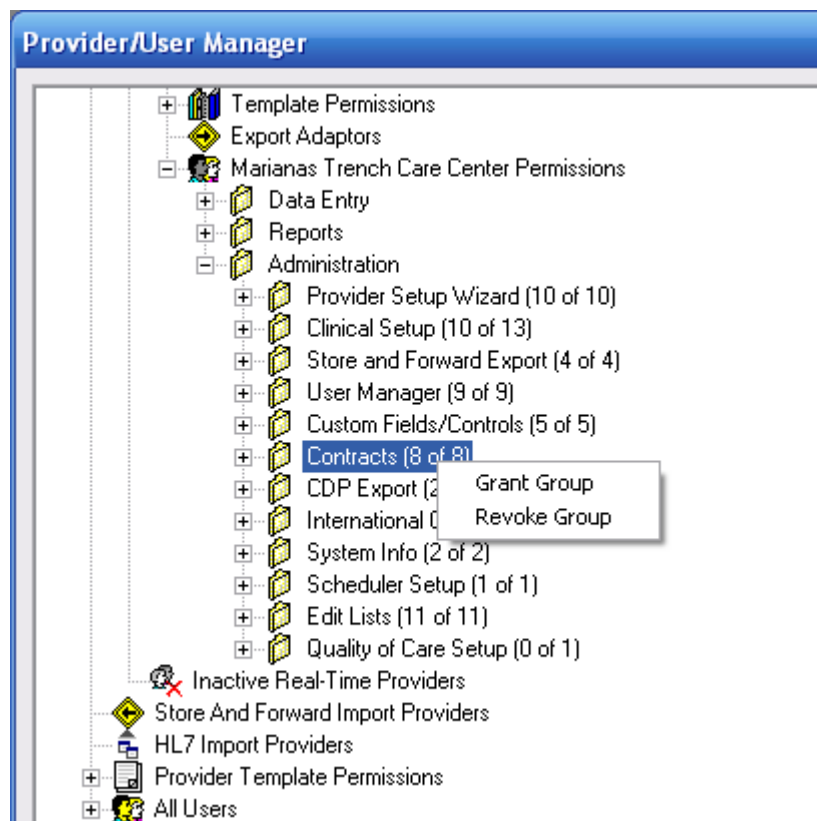
2. Click on the + sign to expand any permissions set. You'll see that when providers are created, they have almost all permissions by default.



You can add any remaining permissions (for instance, if you use the ADAP module) by right clicking each group or permissions within each group.



3. You can remove permissions from the provider the same way, by group or by permissions. For instance, to prevent the provider from modifying contracts, expand the **Administration** privileges, right click on **Contracts**, and select **Revoke Group**. No user at the provider level will be able to modify contracts.

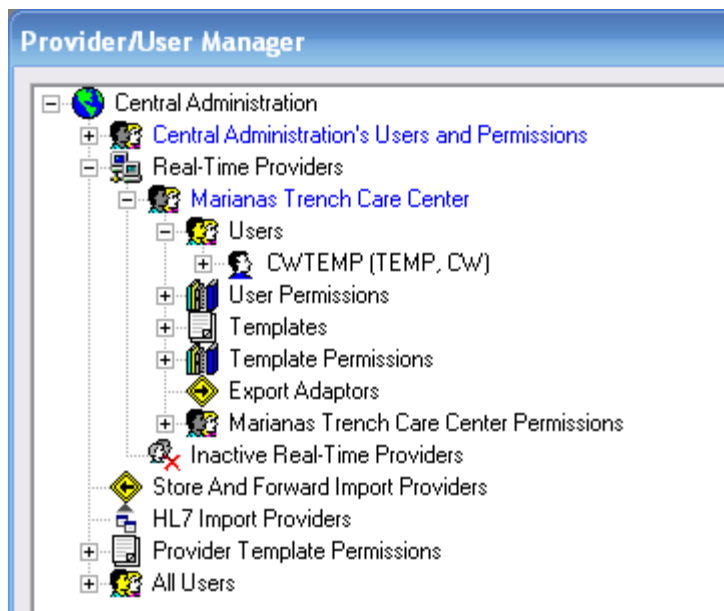


4. Click **Save** at the bottom of the window to save your changes.

Configuring Provider Users

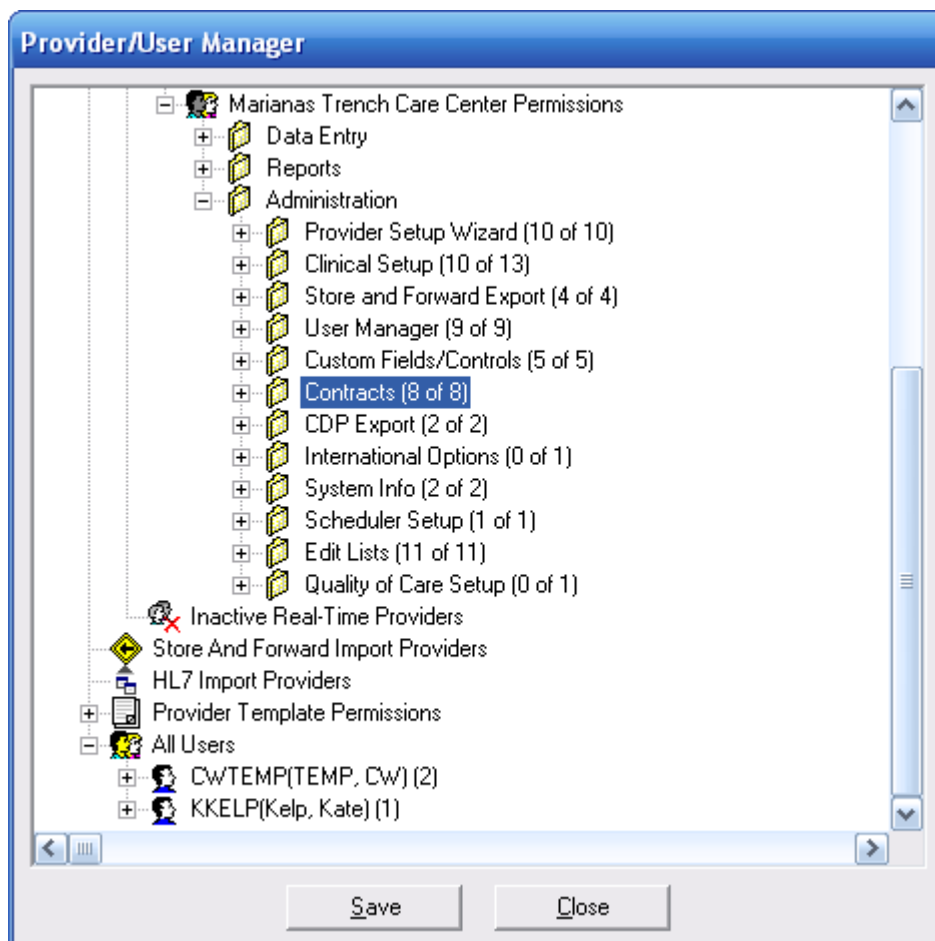
Now it's time to set up all the CAREWare users at your provider. Then we'll create templates for different user types so you don't have to configure each user's permissions every time an employee comes or goes.

1. Expand your list of Real-Time Providers using the + sign, then expand the list of users.



You'll see that only **cwtemp** is listed here, because the user we created was only added to Central Administration. You can add new users who only have provider level permissions, using the instructions above, or you can add the user you created at the administrative level to the provider level.

2. Scroll to the very bottom of the window and expand (+ sign) **All Users**.

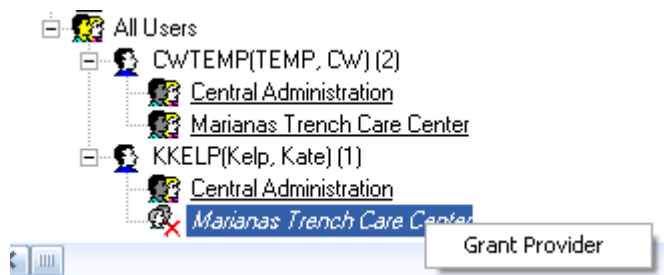


Here you'll see both **cwtemp** and **kkelp**. Expand (+ sign) both users.

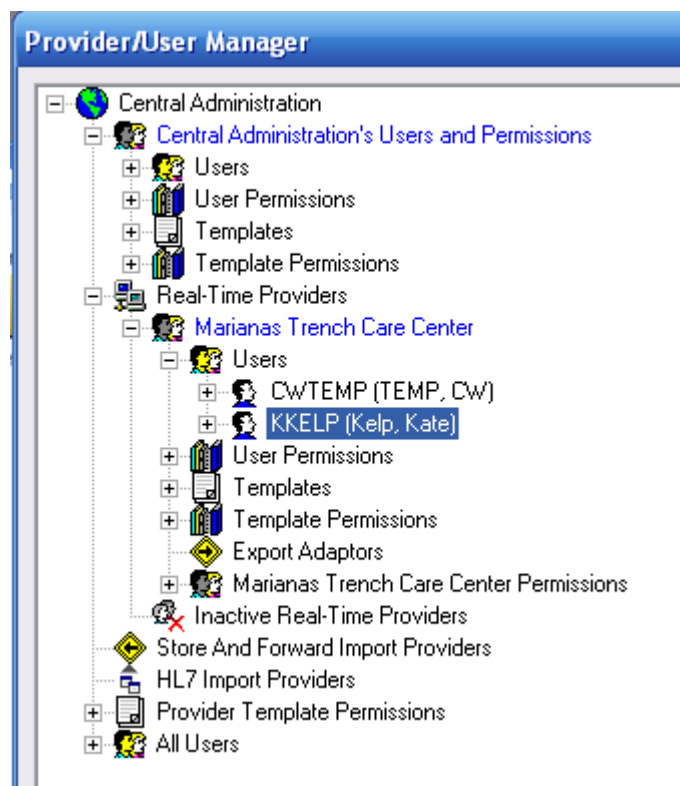


You'll see a (2) next to **cwtemp** and a (1) next to **kkelp**. This tells you **cwtemp** is a user both at the central administration and provider levels, while **kkelp** is only in the central domain.

3. Under your new user, right click on your provider's name (or "Default") and select **Grant Provider**.



4. Go back to the **Real-Time Providers** list, expand it, expand your provider/default, and expand **Users**. The user you added to Central Administration is now also added to your provider, with no permissions.

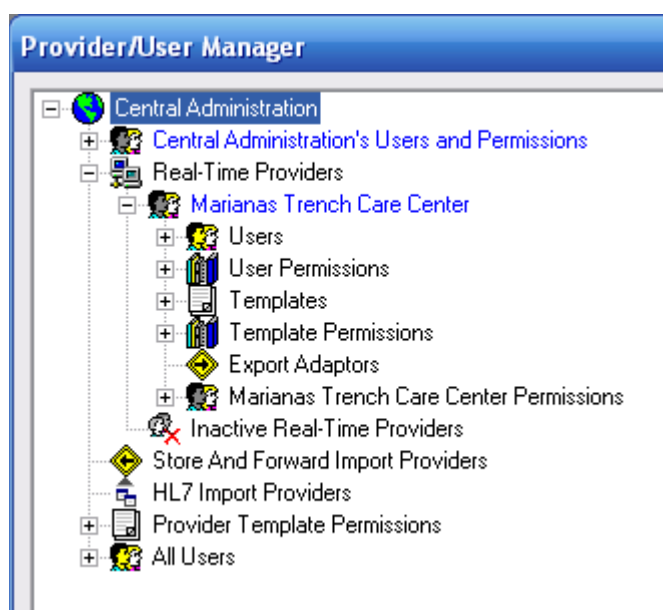


5. Right click on the new user and use the “All Permissions” template or another template to configure their permissions.

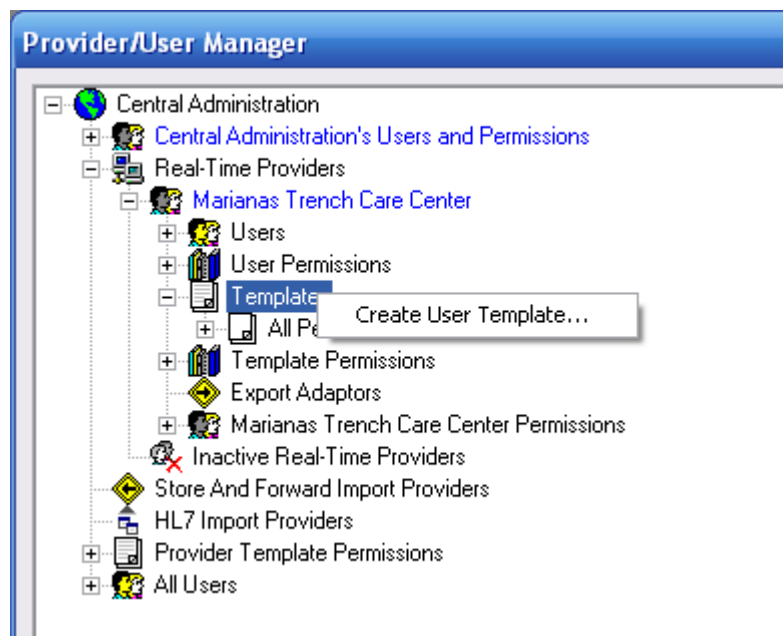
Configuring Templates

Now we'll create a typical template and apply it to a user. Your agency and your HIPAA compliance officer will have to sit down and review the available permissions and determine what type of user needs what permissions. In some agencies, a case manager may need to see medical information; in other agencies, there may be a nurse case manager who handles the client's medical needs. Remember that "need to know" is the rule of thumb in creating templates for each user type.

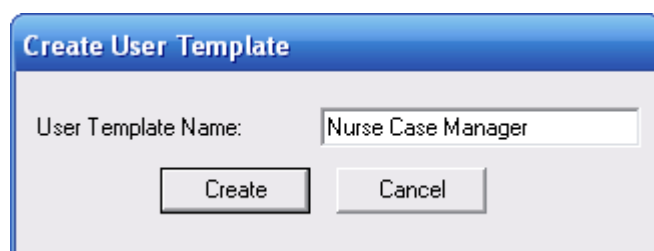
1. Open the **Provider/User Manager**, expand the list of **Real-Time Providers**, and expand **Default/Your Agency**.



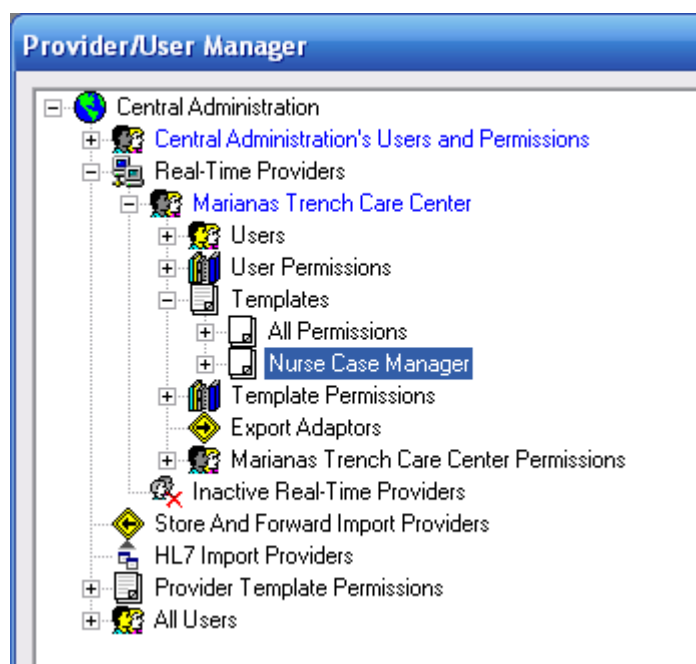
2. Right click on **Templates**, and select **Create User Template**.



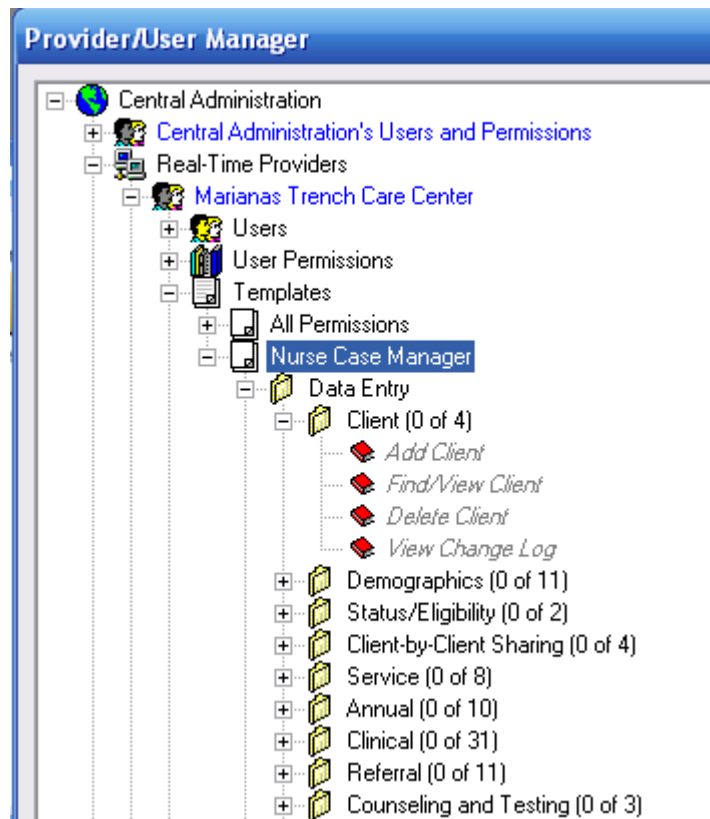
3. Name your template; choose the type of user you're configuring.



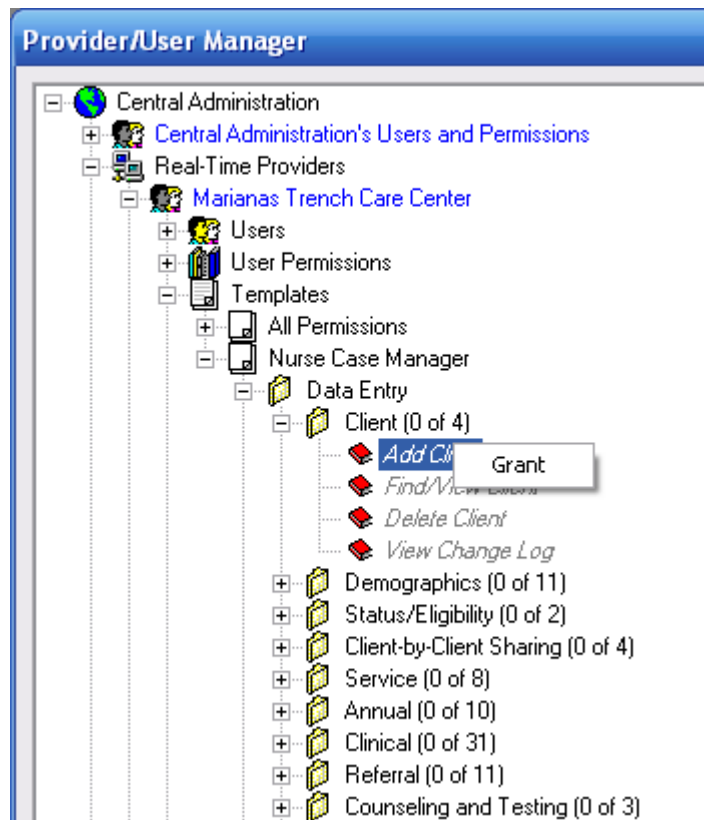
4. The template now appears beneath "All Permissions" in your list of templates.



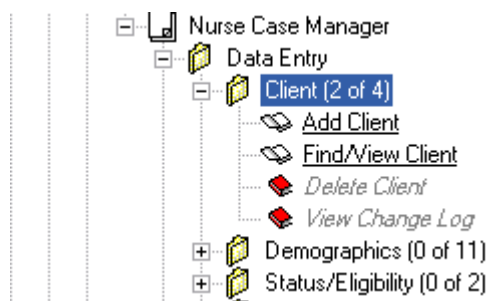
- Expand the new template and select the groups of permissions or individual permissions you want this user to have. For instance, a nurse case manager would need to be able to add clinical data, case notes, and services. Think carefully about what a person in this role needs to know. Let's look at the first set of **Data Entry** permissions.
- Click to expand the **Data Entry** permissions, then **Client** permissions.



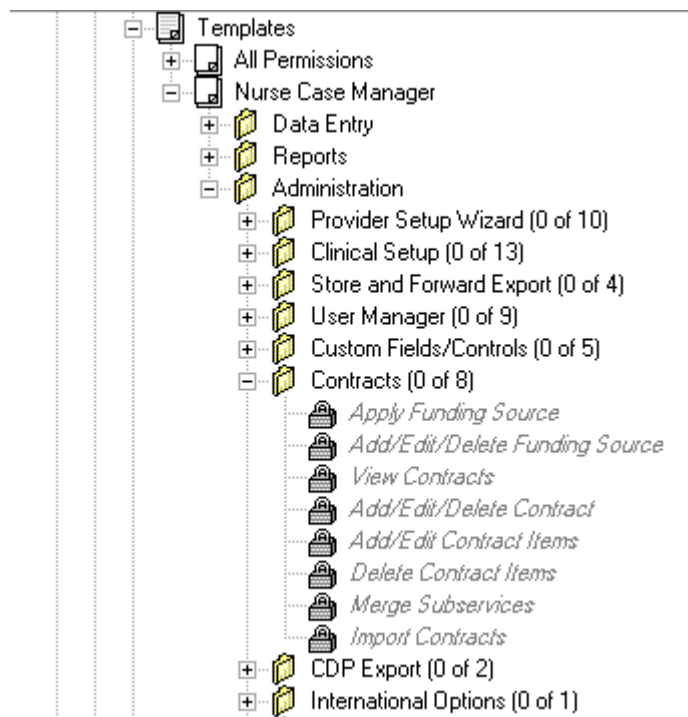
- Right click each permission and select **Grant**.



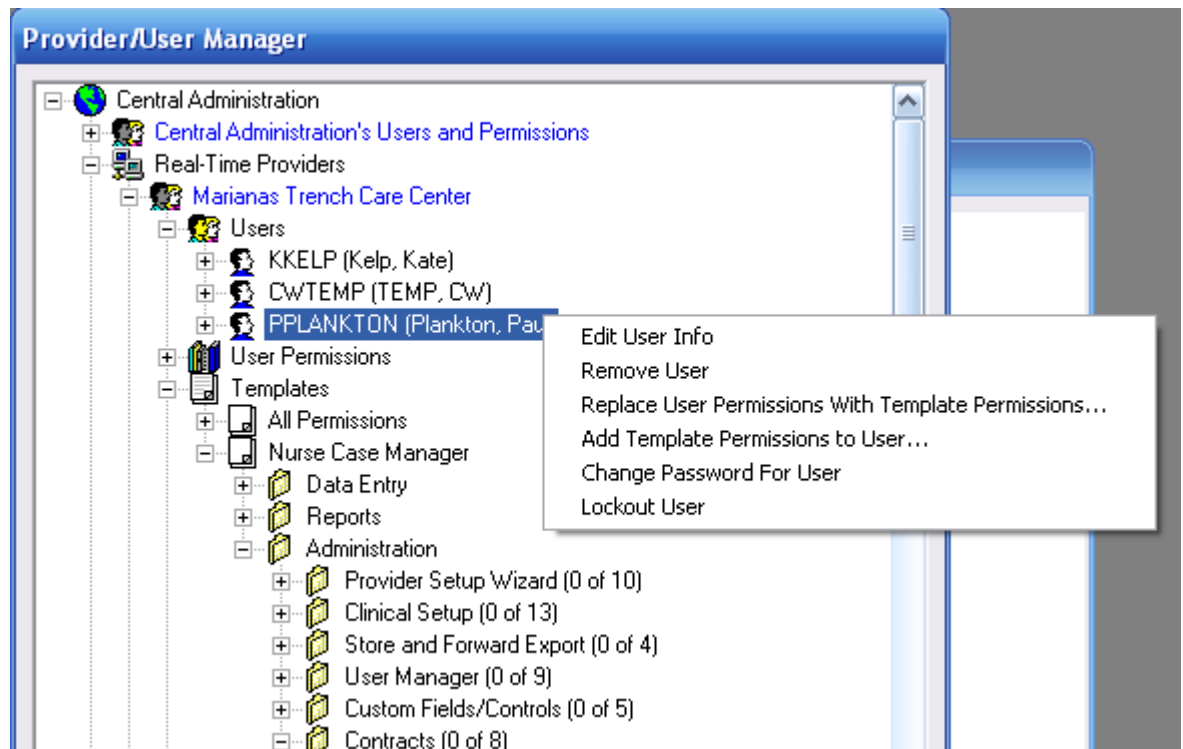
A nurse case manager may do an intake, so you might want them to be able to add a client. Everyone will need to be able to find/view a client. You would probably want to restrict the ability to delete a client to administrative personnel, as well as the ability to view the change log (an audit trail that indicates which user has made what changes to the client’s record). So your nurse case manager template’s Data Entry/Client permissions would look like this.



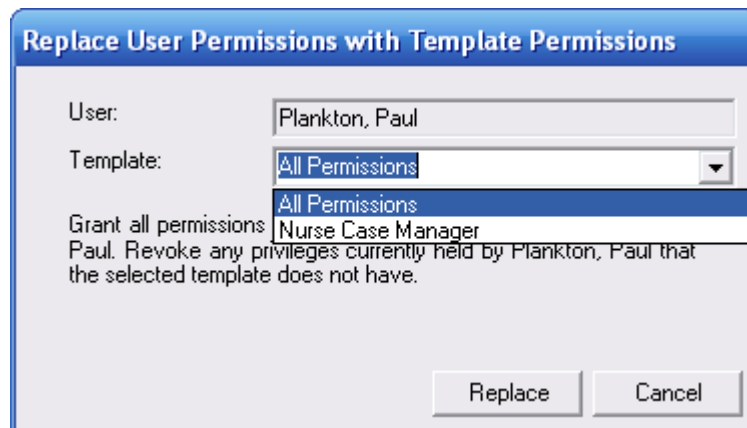
A white, open book indicates a permission that has been granted. A red, closed book, indicates a permission that has not been granted. A permission with a lock next to it indicates a permission that’s not available. For instance, when we configured the provider permissions, we might have locked our provider out of changing contracts, so if you tried to add contract permissions here, you’d see this:



8. Continue through the permissions until you've configured this template's role. Click **Save** at the bottom of the window to save your changes. You can now apply this template to a user.
9. Create a new user at the provider level using the steps above.
10. Right click on your new user and select one of the two template options. You can choose to **Replace User Permissions with Template Permissions**, which wipes out their existing permissions (if any) and replaces them with the permissions you specified when you created your template. Or you can **Add Template Permissions to User**, which will supplement existing permissions with those in the template you specify.



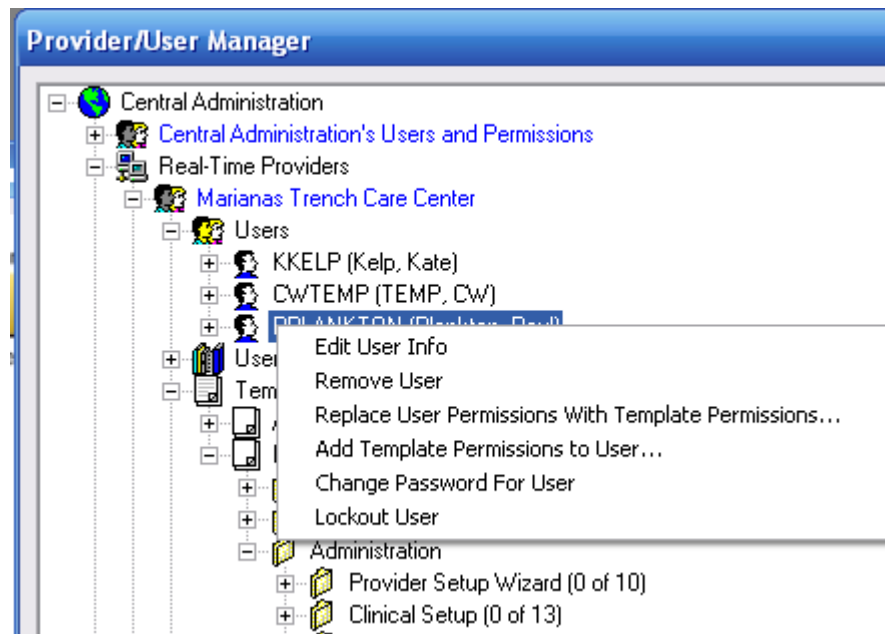
11. You'll be prompted to select a template from the list.



12. Select a template and click **Replace** (or **Add** if you selected add). Your user will now be able to access CAREWare with the permissions you've specified for their role.

Other User Management Options

Right click on any user to access other user management options:



Edit User Info: Change the name or contact info for a user. You cannot change a user's user name.

Remove User: Remove a user's access to the database. This user's record is still available under "All Users" for reinstatement. For **HIPAA compliance**, you should immediately remove terminated employees' access. You may also wish to remove users while they are on extended leave and reinstate them from the "All Users" menu when they return.

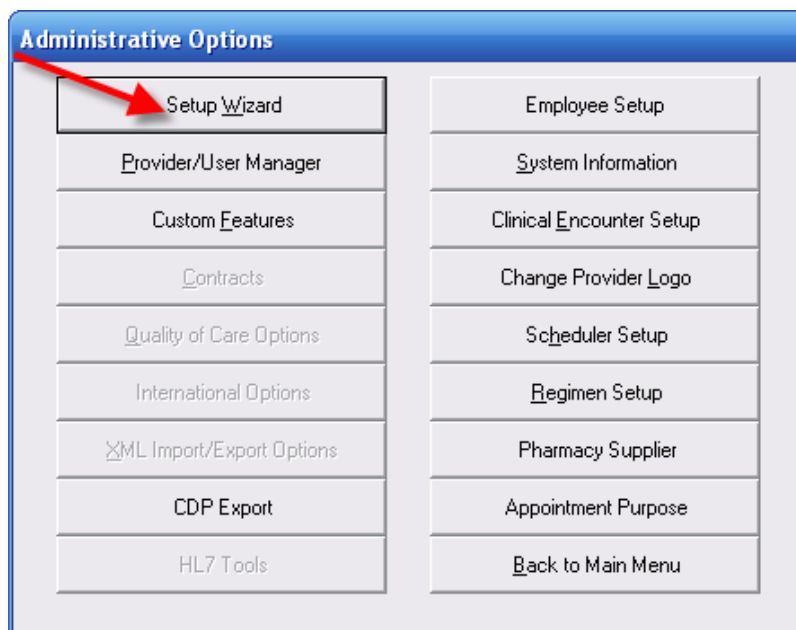
Change Password for User: Change a user's password.

Lockout User/Unlock User: Mostly you will use Unlock User; users who enter their password incorrectly more than twice will be locked out of CAREWare until unlocked.

Using the Setup Wizard

Use the Setup Wizard to enter your agency's data for the Ryan White Annual Data Report (RDR).

1. From the **Administrative Options** screen in your provider domain (NOT from within Central Administration), click the **Setup Wizard**.



2. Click **Next** at the welcome screen.
3. Check the Ryan White funding streams your agency receives.

Setup Wizard - Central Administration

CARE Act program(s)

Please indicate the CARE Act program(s) for which you will be collecting client-level information.

Part A

Part B

Part C

Part D

Health Insurance Program (HIP)

< Back Next > Cancel

4. Click **Next** and select your data sharing options. If you are a stand-alone provider, this is not applicable; click “No, I will keep my data sharing settings.” For a complete discussion of multi-provider data sharing options, please see the complete user manual.

Setup Wizard - Central Administration

Data Sharing

Are there other providers sharing this network with whom you would like to share client-level data?

Yes, I would like to review/change my data sharing options.

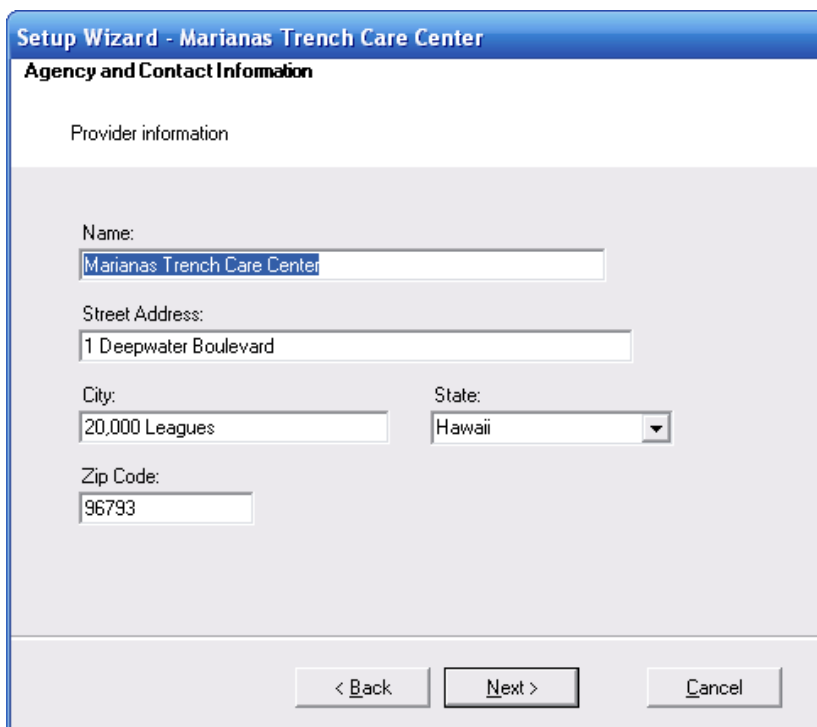
No, I will keep my data sharing settings as they are currently set.

< Back Next > Cancel

5. Click **Next** to go to the Contracts menu. For information on contracts, please see the quick reference guide, “Setting up contracts and services.”



6. Click **Next** to enter your provider information (this is the information that will replace “Default” on your provider list in Provider/User Administration).



7. Click **Next** to enter additional provider information on the next two screens.

Setup Wizard - Marianas Trench Care Center

Agency and Contact Information

Other provider information

Provider/Grantee ID(s)

Part A:	Part B:	Taxpayer ID:	
1	1	382221222	
Grantee A:	Grantee B:	Grantee C:	Grantee D:
9924	2600	1234P44444444	1234P44444444

Agency Type: Service Provider
 Reporting Scope: ALL Clients receivin
 Provider Type: Publicly-funded Com
 Ownership Status: Private, Non-profit (n)

< Back Next > Cancel

Setup Wizard - Marianas Trench Care Center

Agency and Contact Information

Other provider information

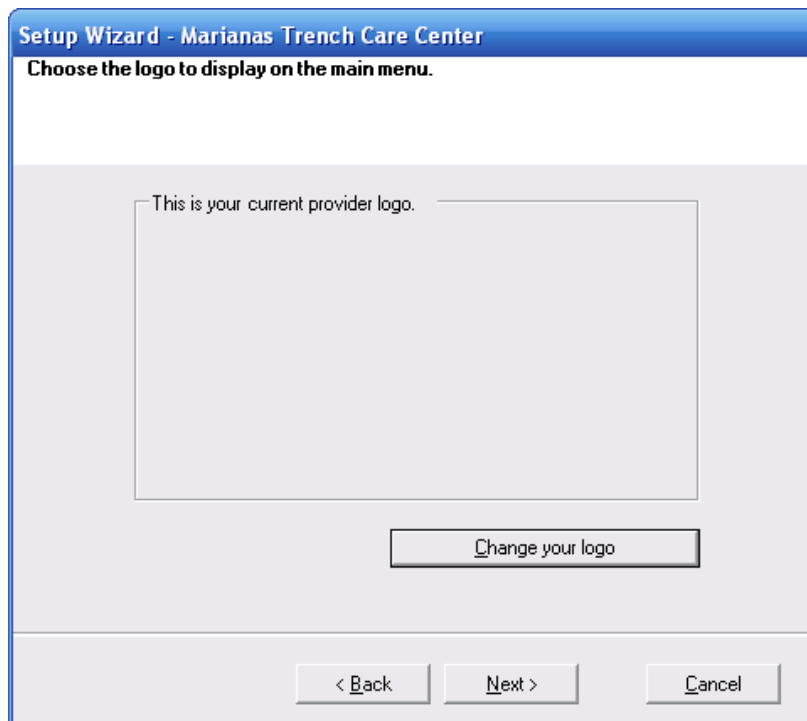
Contact Information:

Contact Name:	Part:	Phone:	Fax:
John Doe	Executive Direct	3132224455	3142224456
Email: jdoe@xxx.com			

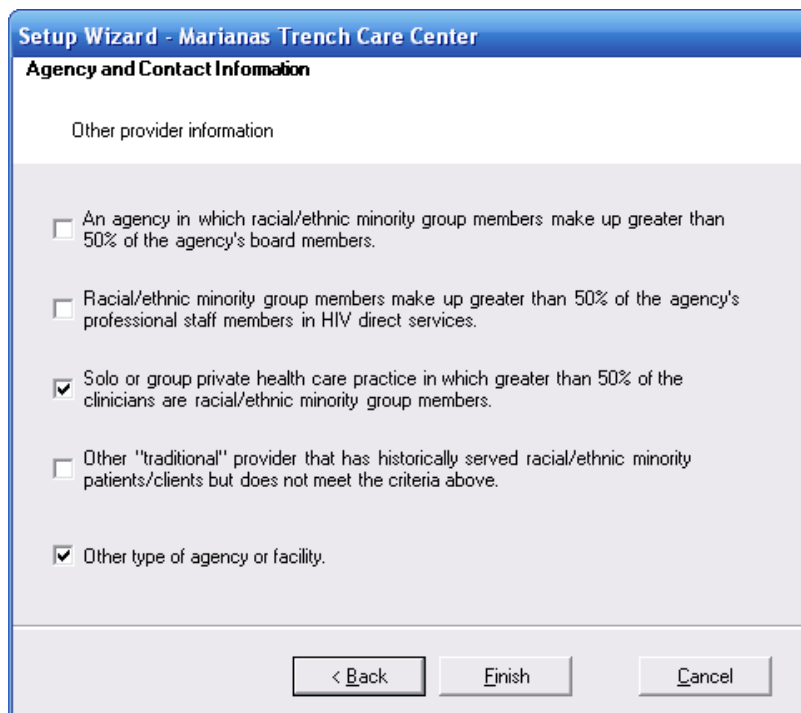
Total Paid HIV Staff in FTE's: 11
 Total volunteer HIV staff in FTE's: 23

< Back Next > Cancel

- Click **Next** to change your provider logo. Click on **Change your logo** to select any bitmap, JPEG or GIF file. This file will then show up on the left hand side of your main menu.



9. Click **Next** to enter additional provider information that will appear on your CADR.

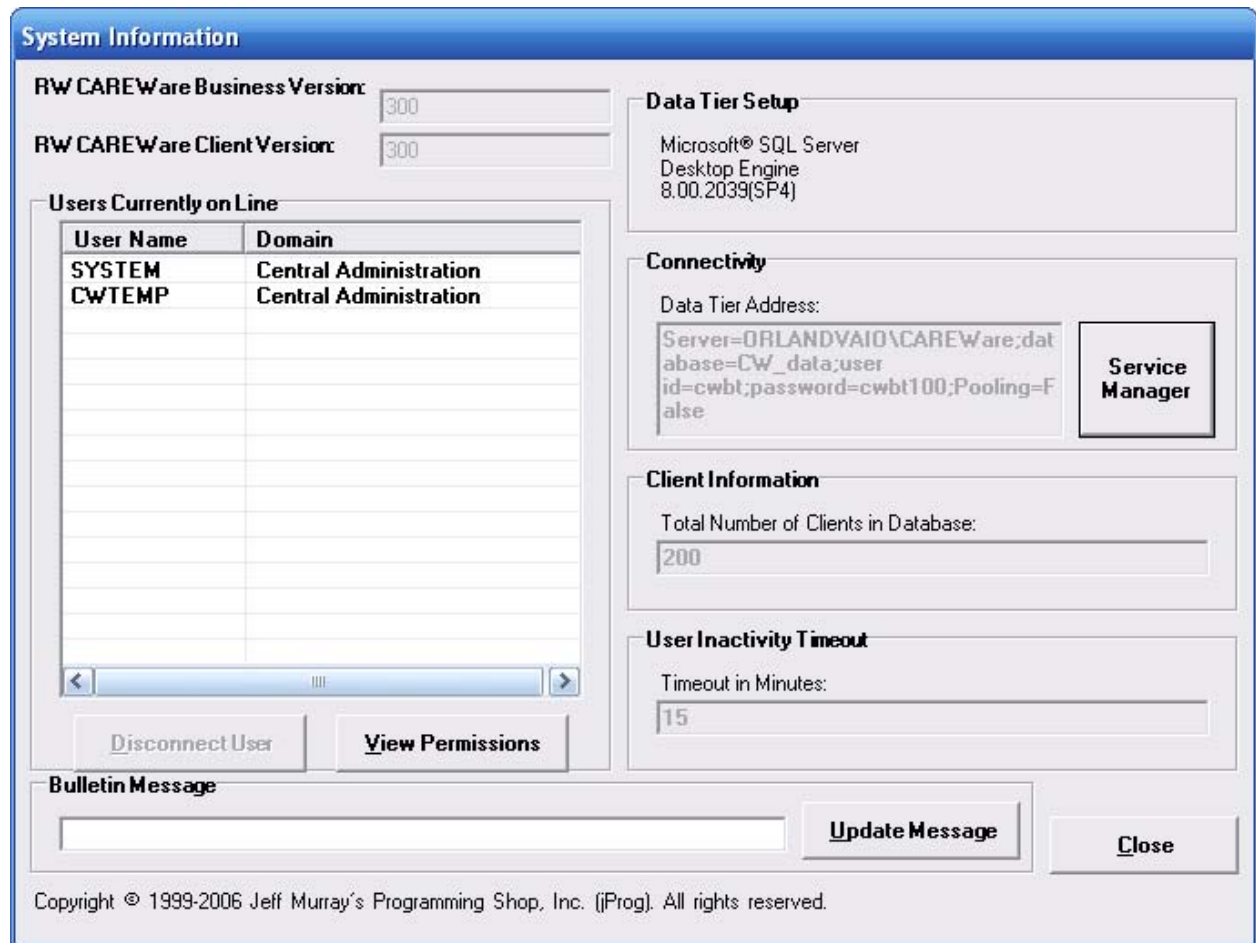


10. Click **Finish** to complete setup.

System Information

System information will give you information on your current business and client tier versions, the number of users currently online, the ability to view a user’s permissions, disconnect a user, and the number of clients in the database.

You can also publish a “bulletin message” that will appear on all users’ screens, such as “System will be down for maintenance Sunday.”



System Information

RW CAREWare Business Version:

RW CAREWare Client Version:

Users Currently on Line

User Name	Domain
SYSTEM	Central Administration
CWTEMP	Central Administration

Data Tier Setup

Microsoft® SQL Server
Desktop Engine
8.00.2039(SP4)

Connectivity

Data Tier Address:

Client Information

Total Number of Clients in Database:

User Inactivity Timeout

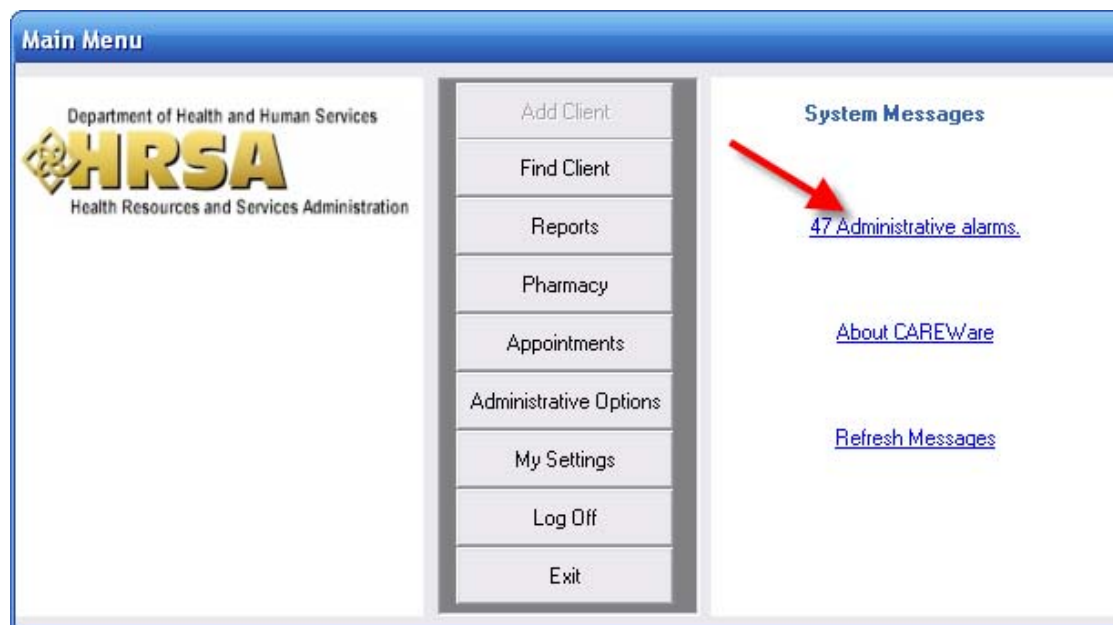
Timeout in Minutes:

Bulletin Message

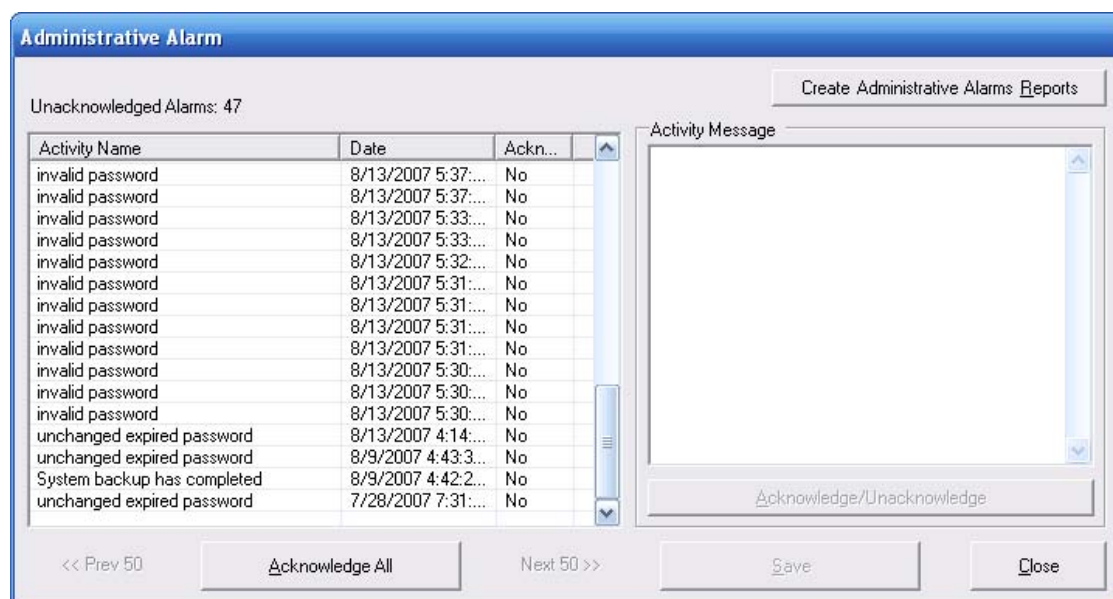
Copyright © 1999-2006 Jeff Murray’s Programming Shop, Inc. (jProg). All rights reserved.

Administrative Alarms

When you are logged into CAREWare as Central Administrator, you'll see a notice about "Administrative Alarms" on the right hand side of the screen. Click on this link to see the administrative alarms.

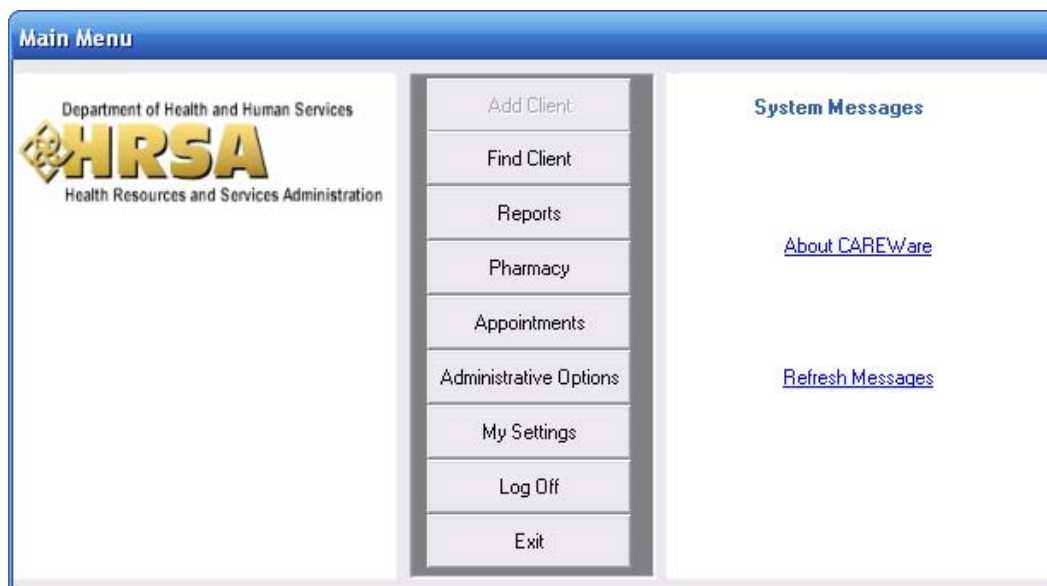


Administrative alarms are usually password-related – a user is overdue for a password change, or has been locked out for incorrectly entering a password too many times.



1. Click **Acknowledge All** to clear the alarms. You can click **Create Administrative Alarms Reports** to create paper trails if necessary.

2. Click **Close**. On the main screen, click **Refresh Messages** to update your display.



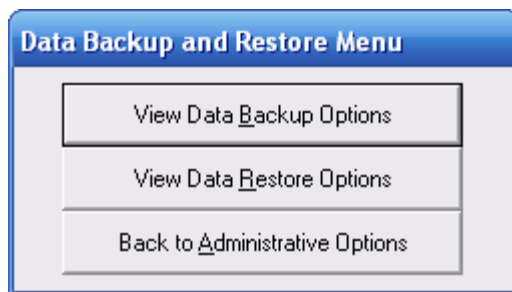
Backup and Restore

CAREWare has its own backup and restore function.

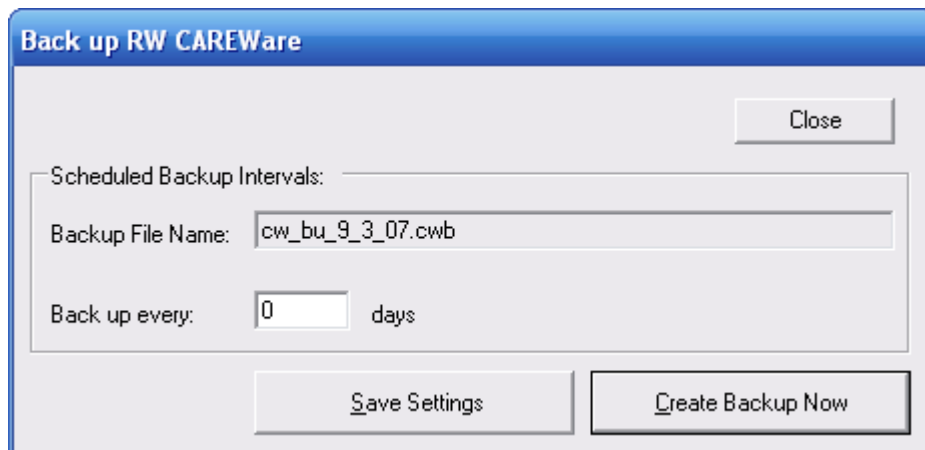
1. From the **Administrative Options** menu, click **Backup**.



2. Choose between Backup and Restore options.



3. For backup, select **View Data Backup Options**.



You can specify how many days between backups, or create a backup immediately. If you create one immediately, check your Administrative Alarms to see when it's completed.

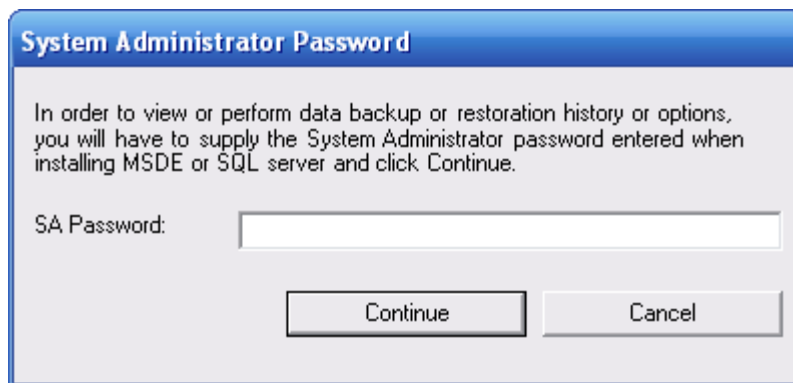
REMEMBER: Backing up from within CAREWare is only the first step to ensuring you have access to your data in event of a problem. You must also copy the associated backup files to a disk or other media.

By default on a stand-alone system, CAREWare backs up to C:\Program Files\Microsoft SQL Server\MSSQL\$CAREWARE\Data. For network users, it will default to the folder where your CW_Data.MDF file resides. There are three files there you must copy to another media:

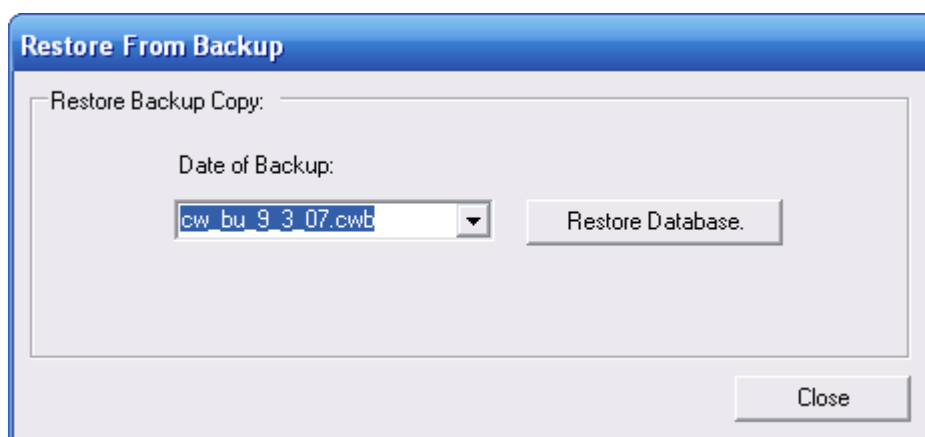
1. The .cwb file with the latest date (for instance, cw_bu_9_3_07.cwb)
2. CW_CHANGE_LOG_0000_Log.LDF
3. CW_CHANGE_LOG_0000.MDF

You will need all these files restored to your data folder to perform a backup.

4. For restore, choose **View Data Restore Options**. You will need to enter the SA (System Administrator) password chosen when you first installed CAREWare. If you used a blank SA password, click **Continue**.



5. Select the date of the backup to be restored; generally the latest but if you've encounter data corruption issues it may be an earlier one.



6. Click **Restore Database** to complete the restore process.