Welcome!

CAREWare Quick Start guides will walk you through the basics of setting up, managing and using the main CAREWare functions. It is intended for non-technical users who just need to get basic information in and out of CAREWare.

About This Guide #9:
User and System Administration

PLEASE NOTE: The client data used in these manuals is purely fictional.

Guides in this series:

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 RSR)*
7. *Creating basic custom reports*
8. *Creating more advanced reports*
9. *User and System Administration*

For additional information:

Please refer to the **Frequently Asked Questions** page on the CAREWare programmers' website:

http://www.jprog.com/wiki/

Or contact the help desk at cwhelp@jprog.com.

Revision date: September 21, 2012

First Things First

What do I need to get started?

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

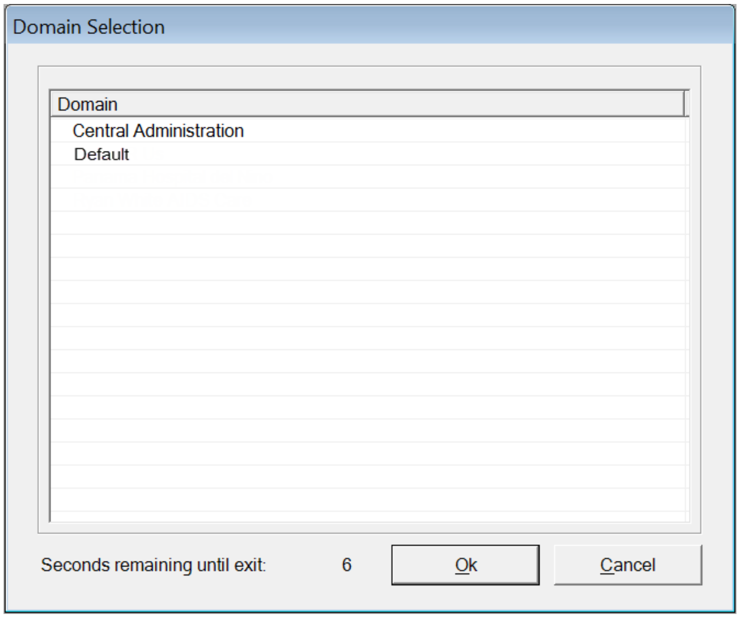
Creating new users

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@01,” you can’t type “connie@01” when you log in. User **cwtemp** comes with all system privileges, so you can create your real users and their system privileges.

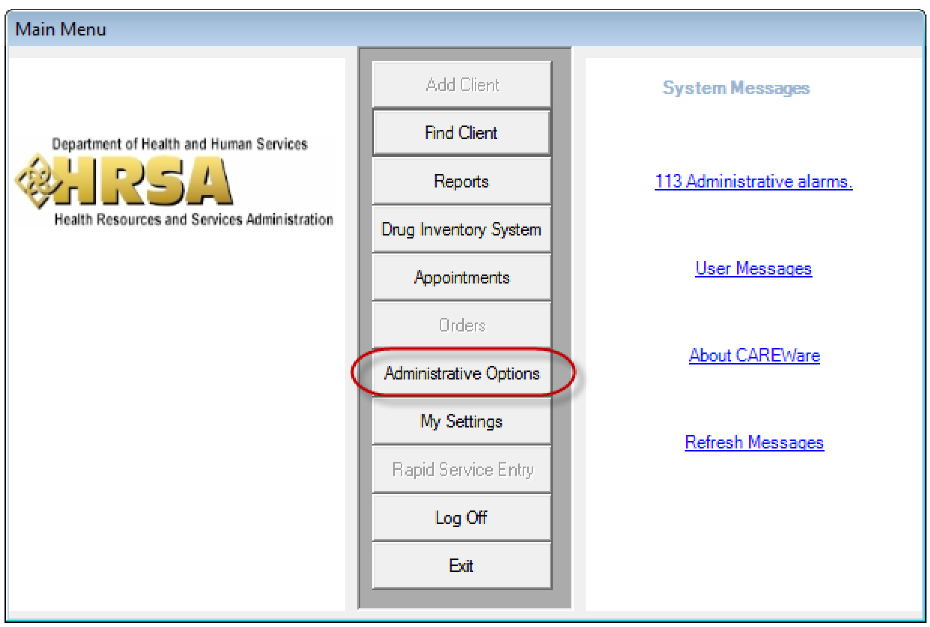
PLEASE NOTE: The Health Insurance Portability and Accountability Act (HIPAA) requires us to take certain steps to protect the privacy and security of our clients’ protected health care information. One of these steps includes deactivating the **cwtemp** user after you’ve set up your real users, as this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

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 (Domain) Name**, depending on how far your system has already been configured. Our sample database has already been configured, so its name appears here.

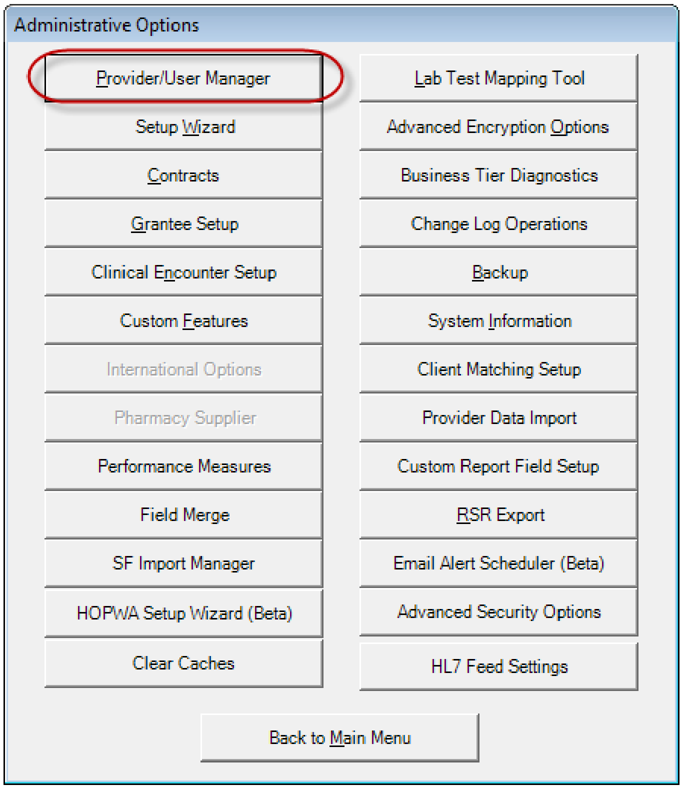
2. Choose **Central Administration.** For security reasons, you only have 20 seconds to choose one or the other.



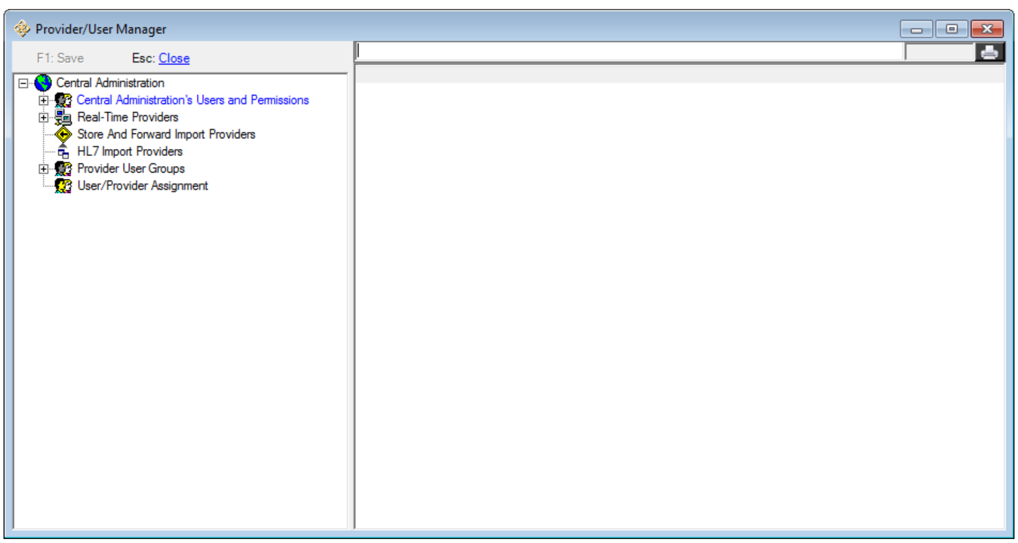
3. The main menu will appear. Select **Administrative Options**.



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



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



Users can be set up as either **Central Administration** users, who can:

Configure other central administrative users and their permissions

Configure provider domains and their permissions

Configure provider users and their permissions

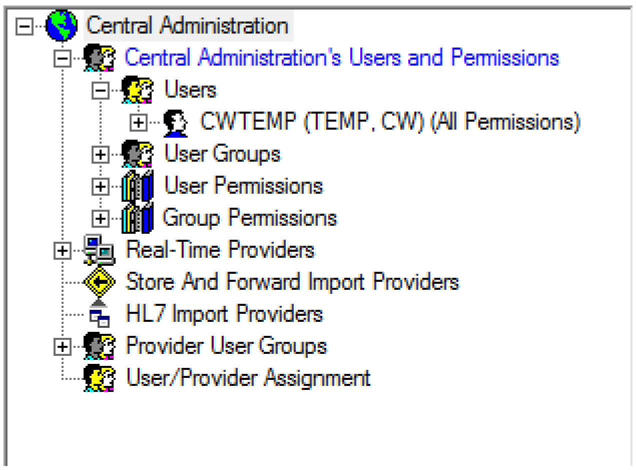
Or as **Provider Domain Users**. With these privileges you can:

Configure provider domains and their permissions

Configure provider users and their permissions.

Even if you are a stand-alone provider, you must use Central Administration to configure your agency's permissions.

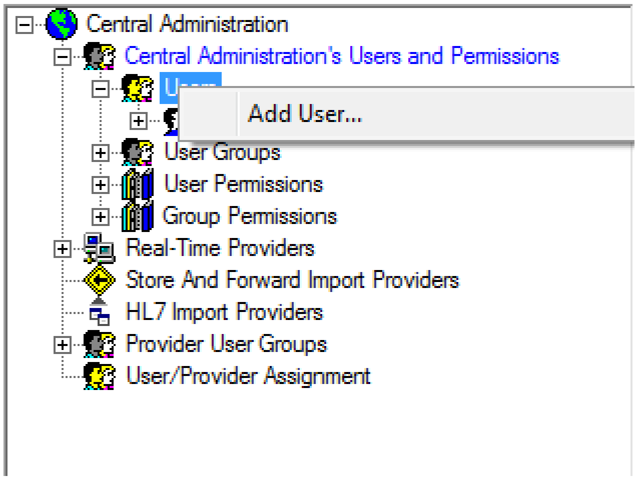
6. Click on the + sign next to **Central Administration's Users and Permissions**, then the + sign next to **Users**.



If you are configuring CAREWare for the first time, you'll only see the one user, **cwtemp**.

PLEASE NOTE: All user names appear in CAPS in the Provider/User Manager, but user names are not case-sensitive. Use caution when creating user names; once a user is created, the user name cannot be edited, and the account cannot be deleted (only deactivated).

7. Right click on **Users**, and click on the option presented to **Add User…**

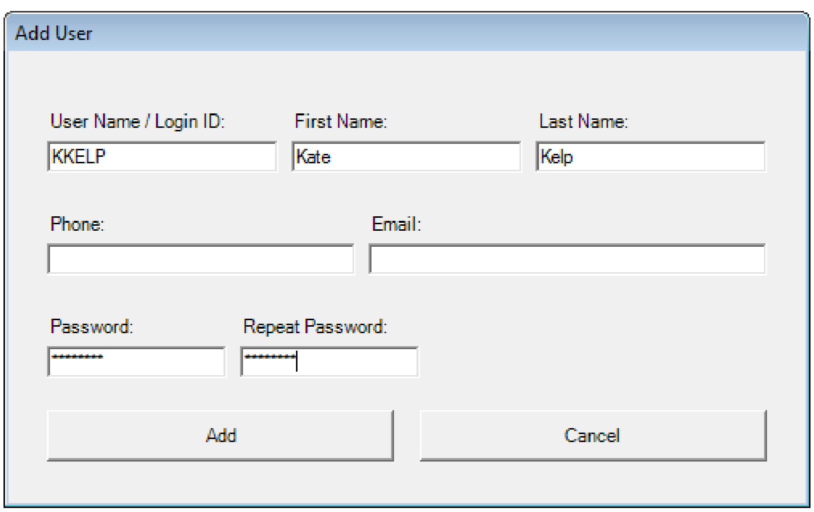


8. You'll see a menu similar to the one you use to enter new clients. You must enter a username (it will appear in all caps), first and last name, and a password of at least 8 characters, with two non-alpha characters – i.e., numbers or special characters. Passwords are case-sensitive. **HIPAA compliance** requires you to select a password that:

   a. Is not easy to guess (e.g. using "password1234")

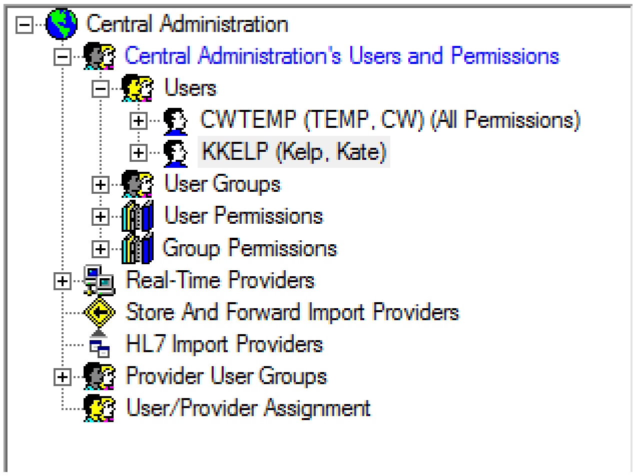
   b. Has an alphanumeric combination (i.e., you might want to select a word and replace its vowels with numbers and symbols, i.e., "d1d@ct1c" for "didactic")

   c. Is changed on a regular basis (every 90 days is typical in many corporate environments; check with your local IT department for company policy and standards if applicable).

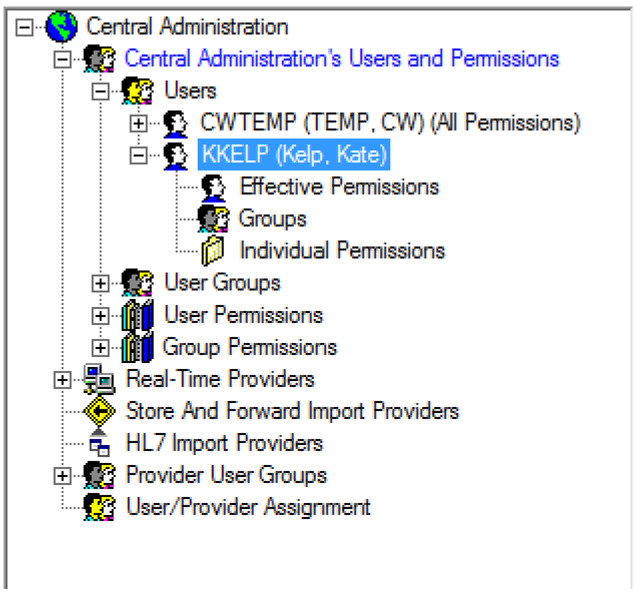


Phone and email are optional fields.

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



10. Click the + next to the new user.



Effective Permissions is a read-only list of all the permissions a user has been granted, either through the granting of **Individual Permissions**, or through their addition to a group via **Group Permissions**. Individual Permissions only lists those permissions granted directly to this user, outside the application of group permissions.

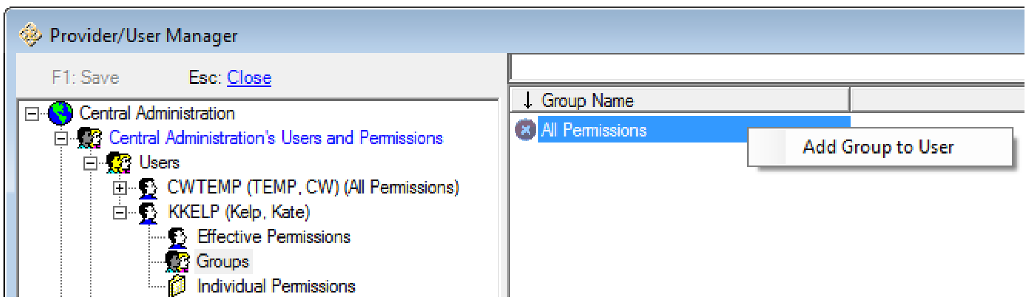
You may assign **Individual Permissions** to a user, but with 200 - 300 different permissions available in CAREWare, this can be time consuming and may lead to errors, especially if applied individually for numerous users.

Instead, you can create **Groups** and assign group permissions to users. This allows you to set up roles rather than people – i.e., a Receptionist who can only view basic demographic data, or a Nurse who has access to view and enter clinical results.

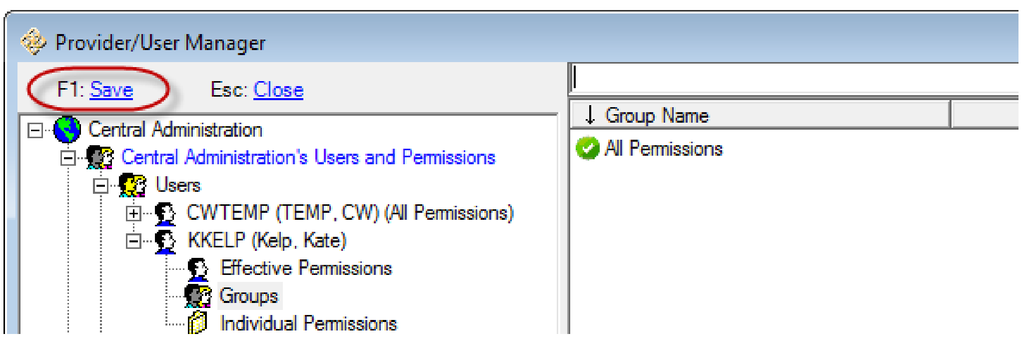
We will walk through the steps for creating Group permissions, but if you so choose, the process is the same for applying permissions to an individual user.

PLEASE NOTE: **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).

11. Click on **Groups** for the new user. You'll see a list of all currently created groups. CAREWare comes with no permissions groups by default. Groups which the user is NOT a member of have a red circle with an X.



12. Right click on the group and select the **Add Group to User** option.



The group now appears with a green circle and a check mark, and this user has been assigned the group permissions in CAREWare.

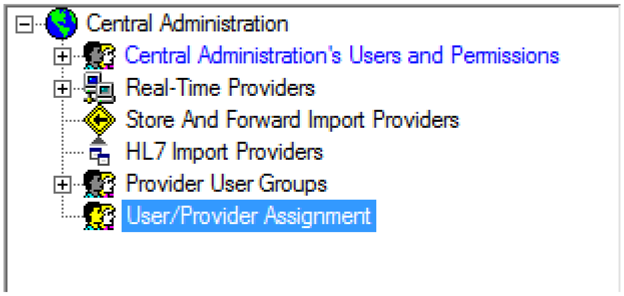
13. Click **F1: Save** (or press the F1 button) to save your changes.

14. Repeat this process for your users at the provider levels.

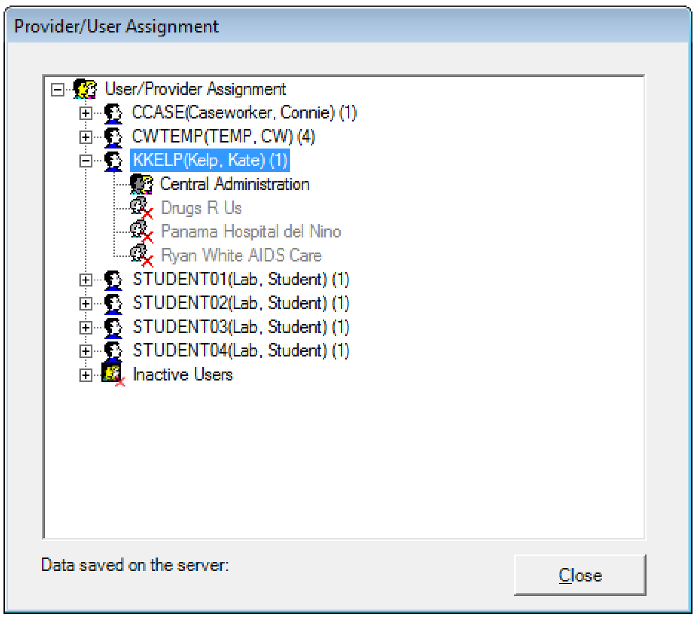
User/Provider Assignment

You can add provider domain access to users through the User/Provider Assignment tool. For instance, once you add yourself as a Central Admin user, you'll want to have permissions for all your provider domains to be able to log in, perform quality control, and assist users in identifying any questionable data, etc.

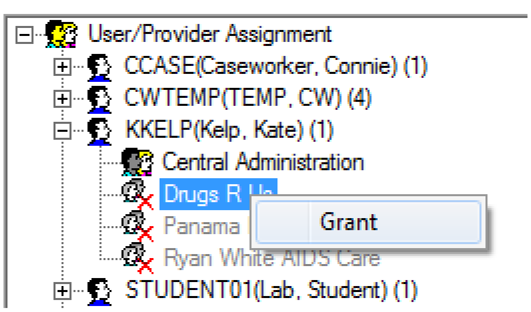
1. From within Central Admin, double click **User/Provider Assignment**.



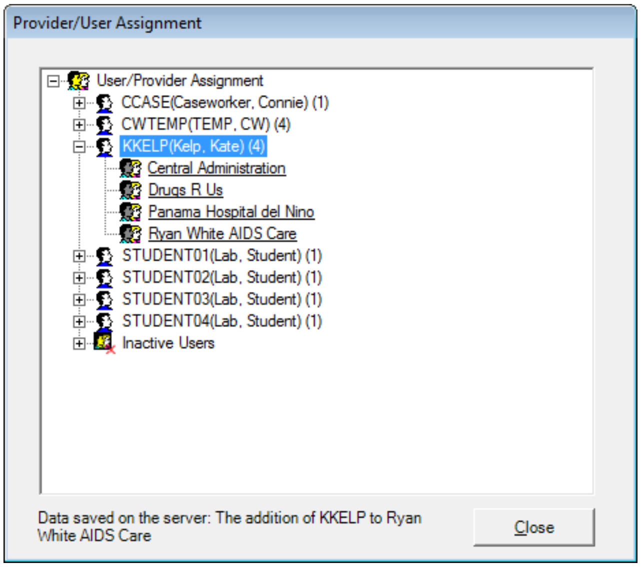
2. Expand the user you want to add to another provider. Above, we added "Kate Kelp" as a Central Admin user, so we'll now give her access to all providers as she is our system administrator.



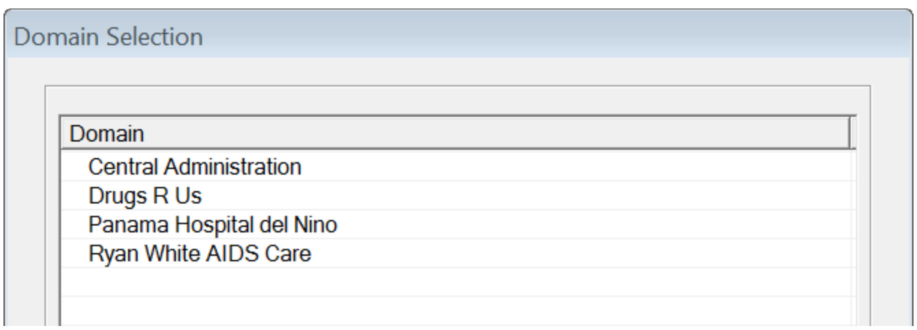
3. Providers marked with a red X and shaded out are providers she cannot access. Right click on the provider to add and select **Grant**. Do this for as many providers as you need to.



4. Access to all providers has now been granted. (Note: user permissions would still need to be configured within each provider domain.)



5. When Kate Kelp logged in before this, she would be logged directly into the Central Admin domain. Now she will get the menu you've seen at the beginning of all these manuals, giving her the choice of domain:



Creating Groups

Groups can be created from either the Central Admin or Provider domain. Since most Central Admin users will have all permissions, we will look at these at a Provider domain level.

PLEASE NOTE: Any group of permissions you assign a user at this group will be subsidiary/dependent to the allowed permissions of the provider. We will discuss provider permissions later. Permissions not available to a provider will show as **Locked** when you work with that provider's user permissions.

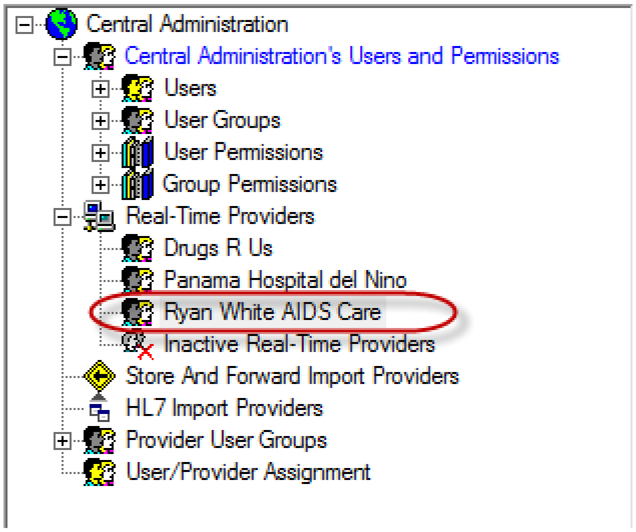
Permissions are divided into three **Permission Groups**: Data Access, Reports, and Administration**.**

- **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.

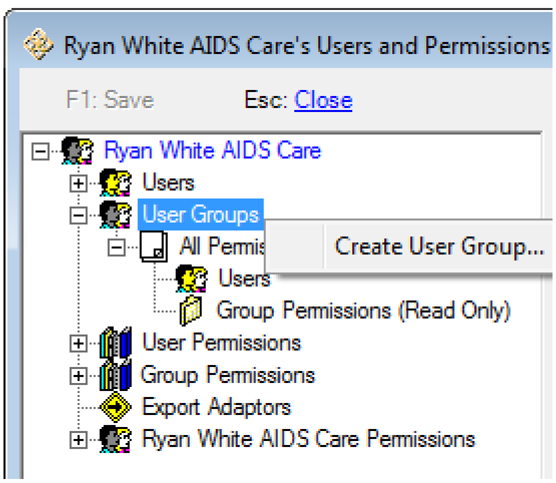
Within each Group are **Permission Sections**. For instance, under Data Access, there is a section for Annual Review information.

Permission	Permission Section	Permission Group
Change Business Tier Password	Advanced Encryption Options	Administration
Change Encryption Key	Advanced Encryption Options	Administration
Show/Hide Encrypted Fields in cw_client	Advanced Encryption Options	Administration
Global User	Advanced Security Options	Administration
Security Question Admin	Advanced Security Options	Administration
View Annual Custom	Annual	Data Access
View annual title III data	Annual	Data Access
View HIV Status	Annual	Data Access
View Insurance/Poverty	Annual	Data Access
View Quarterly Custom	Annual	Data Access
View Quarterly Data	Annual	Data Access
View Appointment/Order	Appointments/Orders	Data Access
View Client Use/Default Days	Appointments/Orders	Data Access

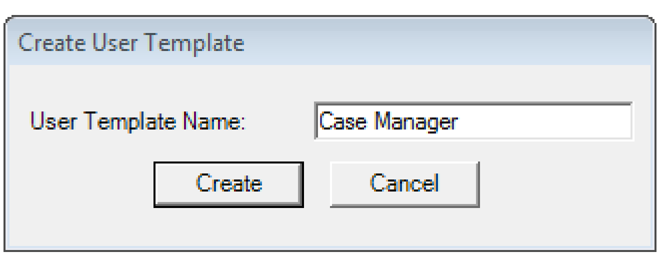
1. Double-click on the provider for whom you wish to create a group. In a new setup, this is still named "Default" – see the Setup Wizard later in this manual for information on renaming the provider.



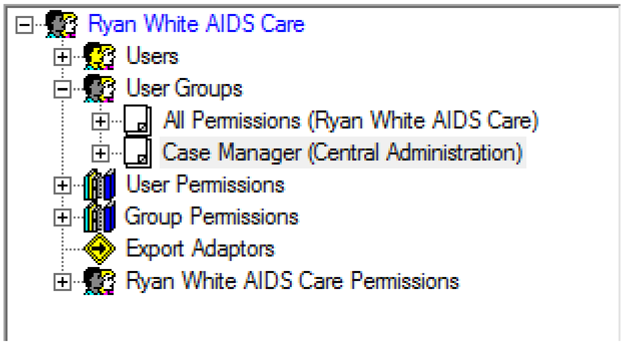
2. A new window will open for this provider. Click the + sign next to **User Groups** to see the existing groups. Right-click on User Groups and select **Create User Group…**



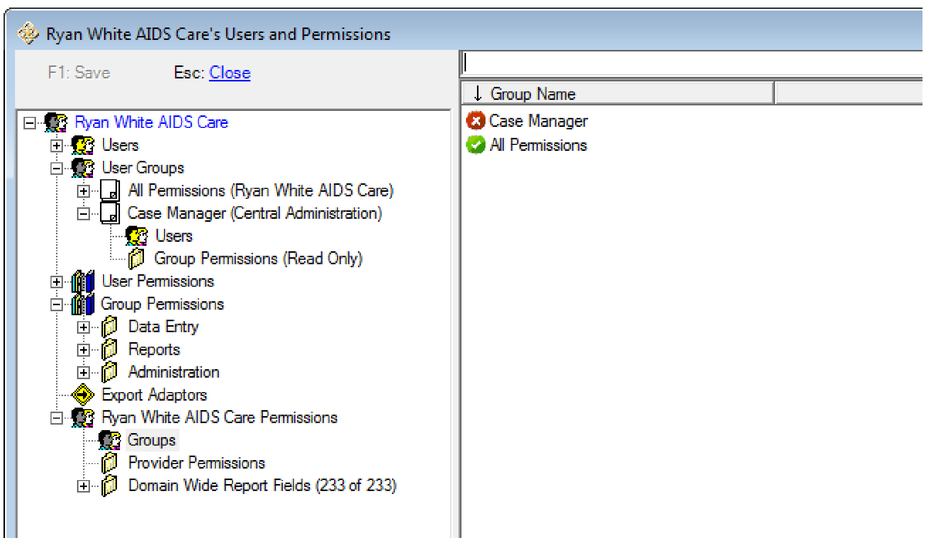
3. You'll be asked to name the user group. Enter a name that corresponds with the role you're working with and click **Create**.



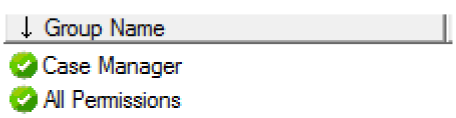
4. The user group will populate in the list. If the group is created at the Central Admin domain, (Central Administration) will appear after the name. This group's permissions will be "read only" to Provider users.



5. You'll then need to go to the provider's permissions. Click the + sign next to the provider name, then click on **Groups**.

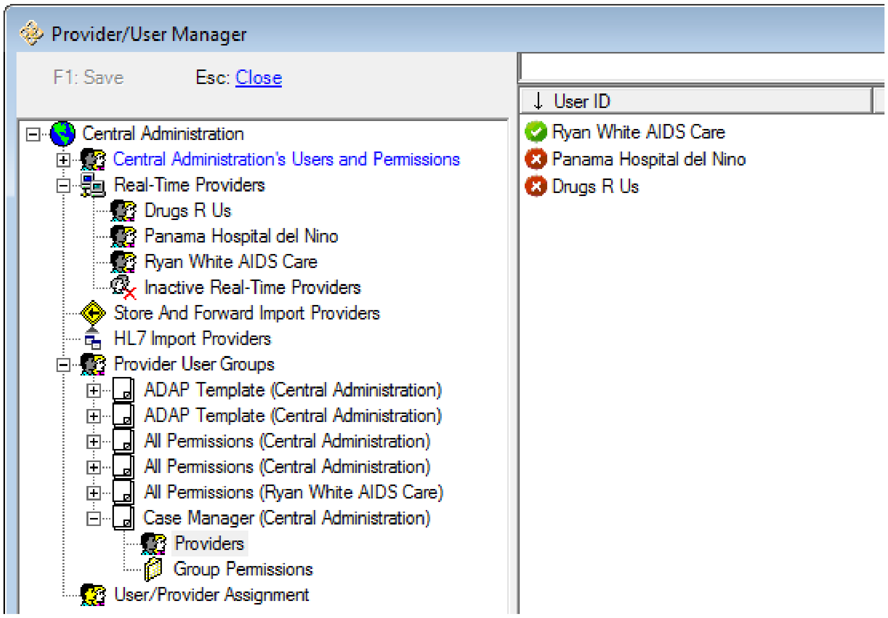


6. The group needs to be activated for this provider. Double click the Case Manager group name to activate.

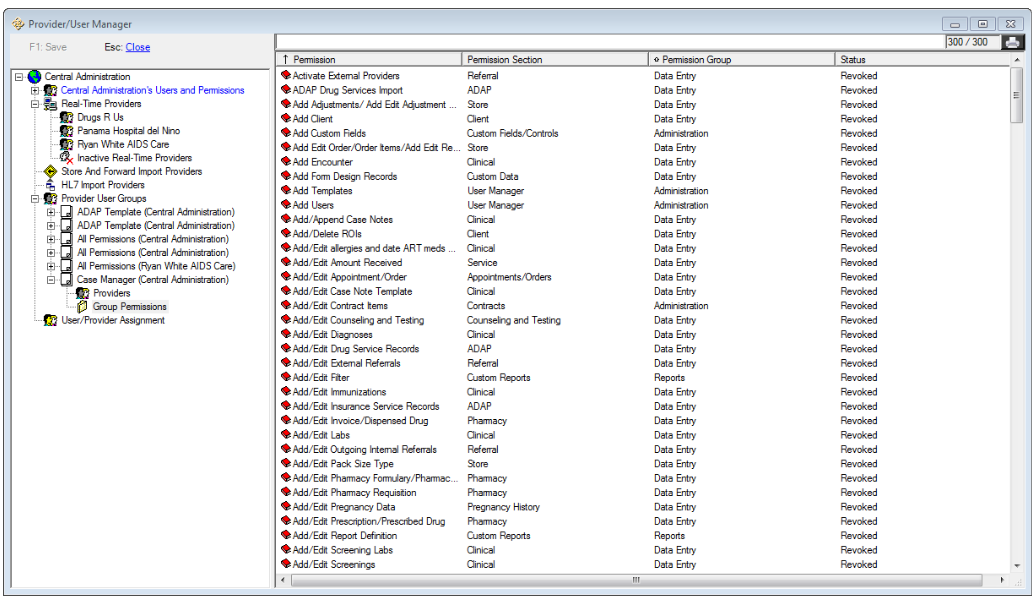


7. Now you'll need to return to the Central Admin window. Click **F1 Save** if necessary to leave the provider domain window.

8. Expand the **Provider/User Groups** section. Click on Providers to see the providers for whom this permissions group is activated. You can activate it for other providers in this window.



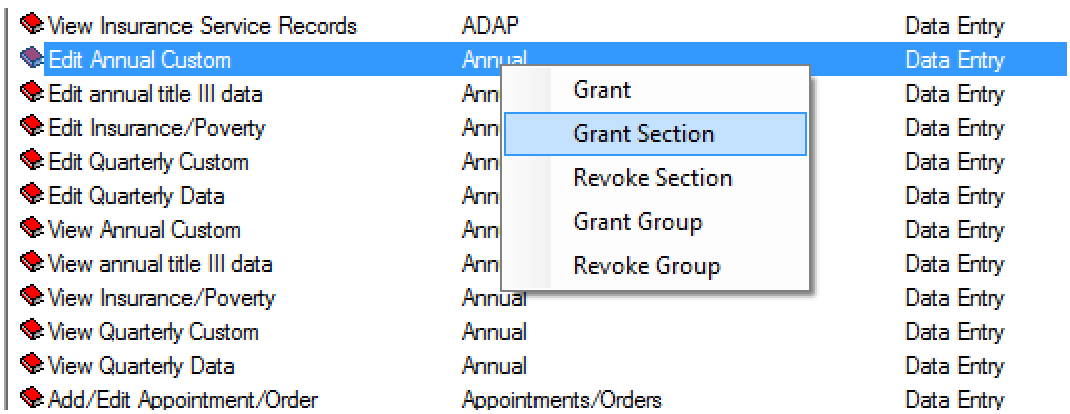
9. Click on **Group Permissions** to see the permissions list. All are "Revoked" by default in a new group. The red "closed book" icon indicates revoked permissions.



10. Permissions are sorted alphabetically by default. Click on the **Permission Section** or **Permission Group** column headers to sort them. Here we have sorted by Section, then again by Group (which alphabetizes sections within groups):

Permission	Permission Section	Permission Group	Status
Edit dispenser list	ADAP	Data Entry	Revoked
Edit formulary/drug list	ADAP	Data Entry	Revoked
Run ADAP Quarterly Report	ADAP	Data Entry	Revoked
View Drug Service Prices	ADAP	Data Entry	Revoked
View Drug Service Records	ADAP	Data Entry	Revoked
View Insurance Service Prices	ADAP	Data Entry	Revoked
View Insurance Service Records	ADAP	Data Entry	Revoked
Edit Annual Custom	Annual	Data Entry	Revoked
Edit annual title III data	Annual	Data Entry	Revoked
Edit Insurance/Poverty	Annual	Data Entry	Revoked
Edit Quarterly Custom	Annual	Data Entry	Revoked
Edit Quarterly Data	Annual	Data Entry	Revoked
View Annual Custom	Annual	Data Entry	Revoked
View annual title III data	Annual	Data Entry	Revoked
View Insurance/Poverty	Annual	Data Entry	Revoked
View Quarterly Custom	Annual	Data Entry	Revoked
View Quarterly Data	Annual	Data Entry	Revoked
Add/Edit Appointment/Order	Appointments/Orders	Data Entry	Revoked
Delete Appointment/Order	Appointments/Orders	Data Entry	Revoked
Set Client Use/Default Days	Appointments/Orders	Data Entry	Revoked
View Appointment/Order	Appointments/Orders	Data Entry	Revoked
View Client Use/Default Days	Appointments/Orders	Data Entry	Revoked

11. To add access to Annual fields, right click on any of the Annual fields listed and select **Grant** for an individual permission, or **Grant Section** for fields in a certain area – i.e., you would not generally grant access to a single demographics field, but to all the fields required. (You would select **Grant Group** to add access to ALL Data Entry fields, which we don't want to do for a case manager.)



12. The "book" icon changes to open/clear to indicated granted status.

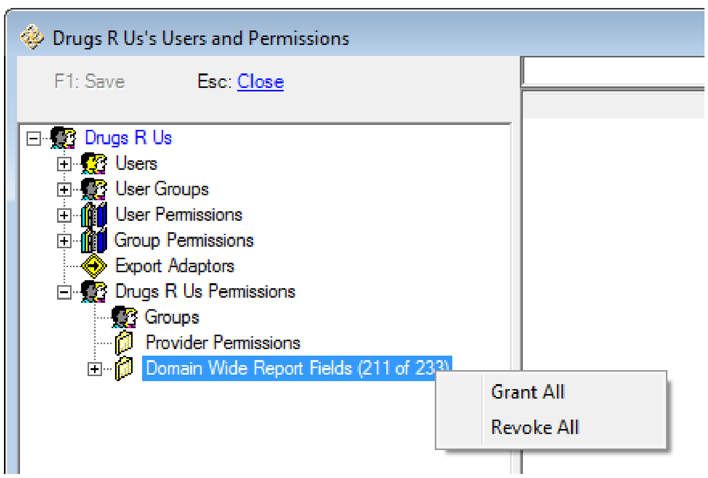
View Insurance Service Prices	ADAP	Data Entry	Revoked
View Insurance Service Records	ADAP	Data Entry	Revoked
Edit Annual Custom	Annual	Data Entry	Granted
Edit annual title III data	Annual	Data Entry	Granted
Edit Insurance/Poverty	Annual	Data Entry	Granted
Edit Quarterly Custom	Annual	Data Entry	Granted
Edit Quarterly Data	Annual	Data Entry	Granted
View Annual Custom	Annual	Data Entry	Granted
View annual title III data	Annual	Data Entry	Granted
View Insurance/Poverty	Annual	Data Entry	Granted
View Quarterly Custom	Annual	Data Entry	Granted
View Quarterly Data	Annual	Data Entry	Granted
Add/Edit Appointment/Order	Appointments/Orders	Data Entry	Revoked

13. Continue to select the permissions you want to grant for this user type. Some permissions will have to be granted individually; for instance, we want a case manager to be able to Find/View a client but not add or delete a client.

Add Client	Client	Data Entry	Revoked
Add/Delete ROIs	Client	Data Entry	Revoked
Delete Client	Client	Data Entry	Revoked
Find/View Client	Client	Data Entry	Granted
View Change Log	Client	Data Entry	Revoked
Request Client Clinical Data	Client-by-Client Sharing	Data Entry	Revoked

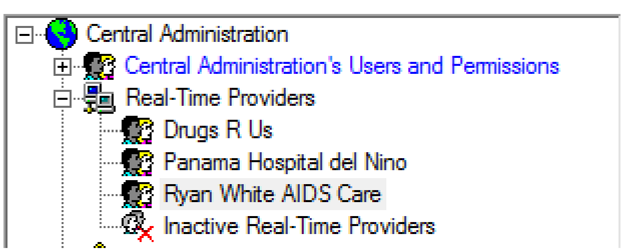
14. Click **F1: Save** when done.

PLEASE NOTE: Some CAREWare business tier upgrades will include new functionality, which by default will NOT be granted to your users or groups. You will need to update your provider permissions under **Domain Wide Report Fields** permissions to access any additional features.

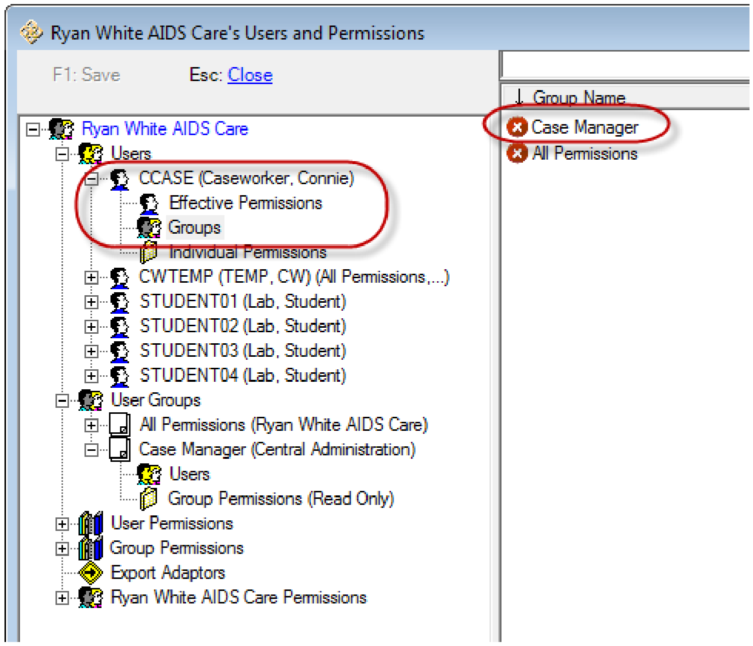


Assigning Users to Groups

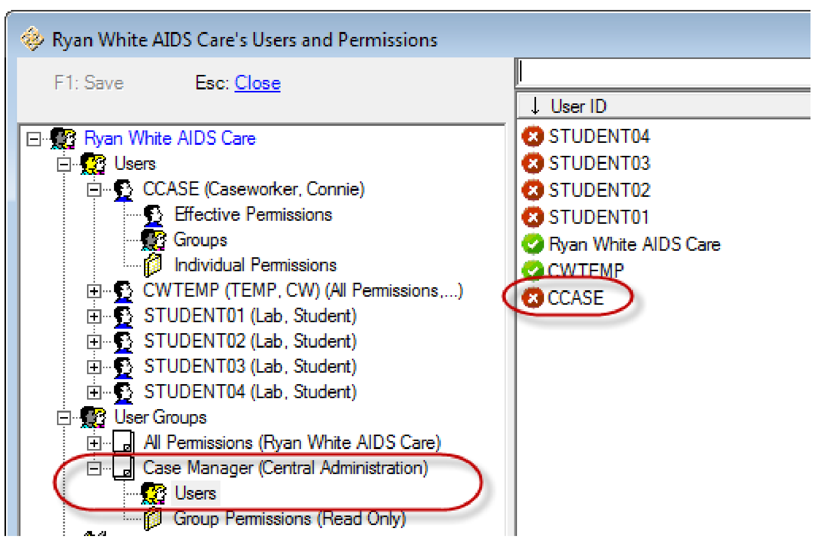
1. Now you can double-click on the provider name under the Real-Time Providers list.



2. You can assign a group to a user by expanding the user info and clicking on **Groups**, then double clicking the **Group Name**…



3. …or assign a user to a group by expanding the group information and clicking on **Users**, then double clicking the **Group** name.

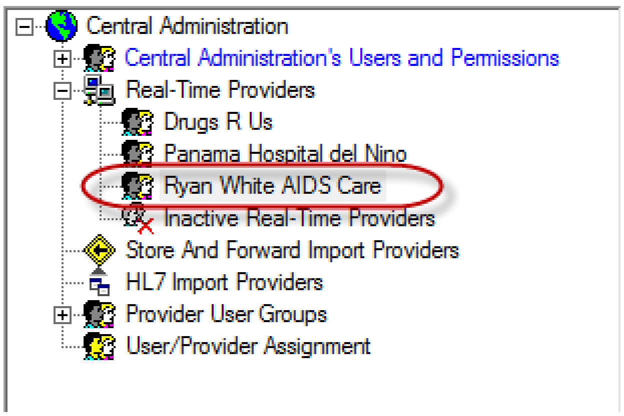


4. The Red X will change to Green check and this user will have the permissions assigned to this group.

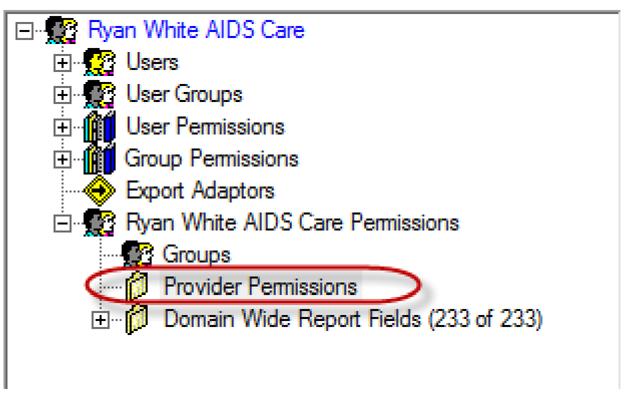
Configuring Provider Permissions

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 domain. For instance, as the central administrator, you may want to control whether or not 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 + sign next to **Real-time Providers.** If you only see "Default," don't worry; we'll change that later. Double-click the provider for whom you want to set permissions.

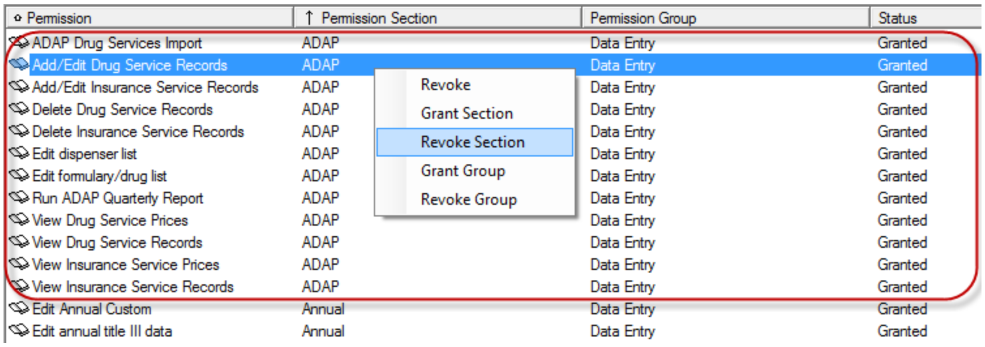


2. Click on the + sign to expand the provider's permissions, then double click **Provider Permissions**.



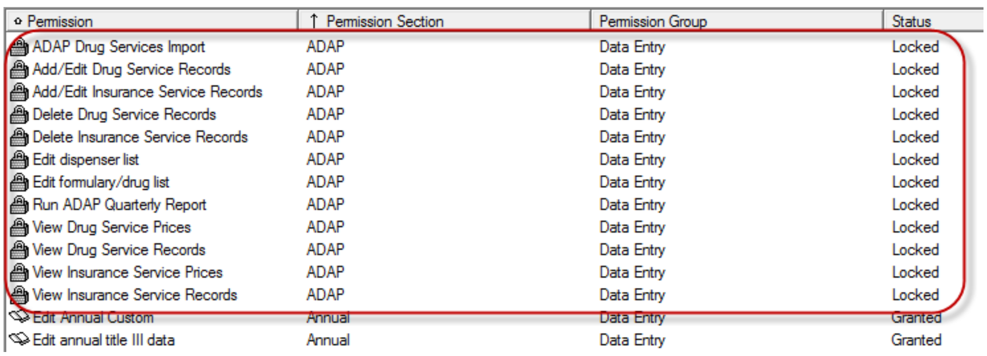
3. In this case, we will revoke ADAP permissions as this agency does not provide any ADAP services. Sort the **Permissions Section** by clicking on the column header.

4. Right-click one of the ADAP permissions and select **Revoke Section**.



5. You can now expand the **Users** list, then expand any user (CWTEMP in this case), and double click on **Effective Permissions** or **Individual Permissions**.

6. Click the Permission Section column header to alphabetize. You'll see that rather than **Granted** or **Revoked**, this user's permissions for the ADAP section are **Locked**, with a padlock next to the permission.

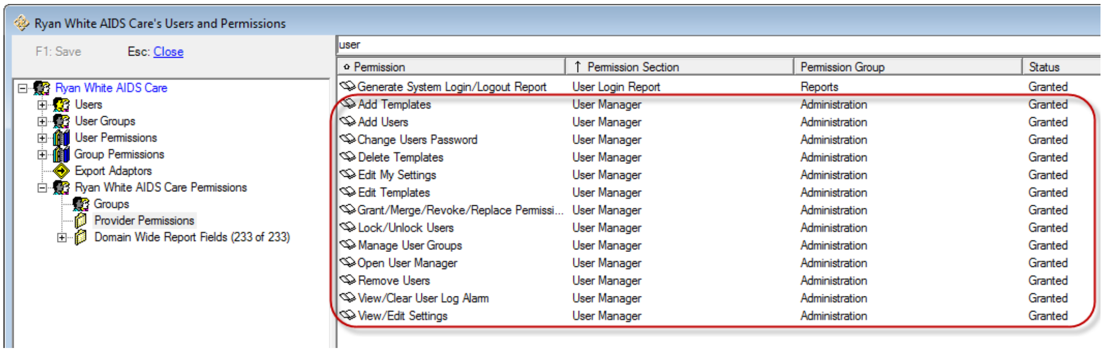


7. Click **F1: Save** to save your changes.

Now, regardless of group permissions applied, no user at this agency can access the locked section unless you unlock it from Central Administration.

User Management Permissions at Provider Domains

Depending on your staffing needs, the technical abilities of provider users, and/or HIPAA security requirements, you can elect to allow users at the provider domains to perform user administration for their own staff. The **User Manager** Permission Section under provider permissions will allow/disallow these features.

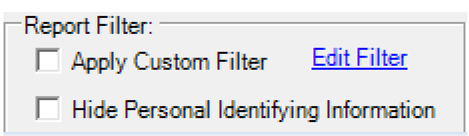


Restriction of PII in Reports

This feature allows administrators to restrict users' access to fields in custom reports on a field-by-field basis. It also adds the capability to restrict the Personal Identifying Information (PII) that is available in most of CAREWare's built-in reports.

Report restrictions are managed via permission groups configured via the **Advanced Security Options** menu and the **Provider/User Manager** at the Central Administration domain. They can be applied at the Central Admin domain, or through the **User Manager** button or **Provider/User Manager** at the provider domain level. We will show the Central Administration methods here.

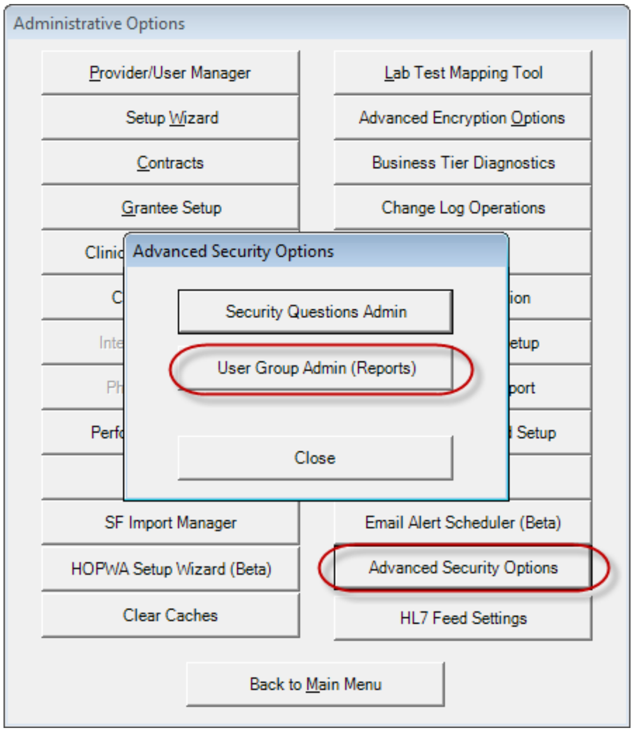
Each prebuilt report that shows PII has a new check box to "Hide Personal Identifying Information":



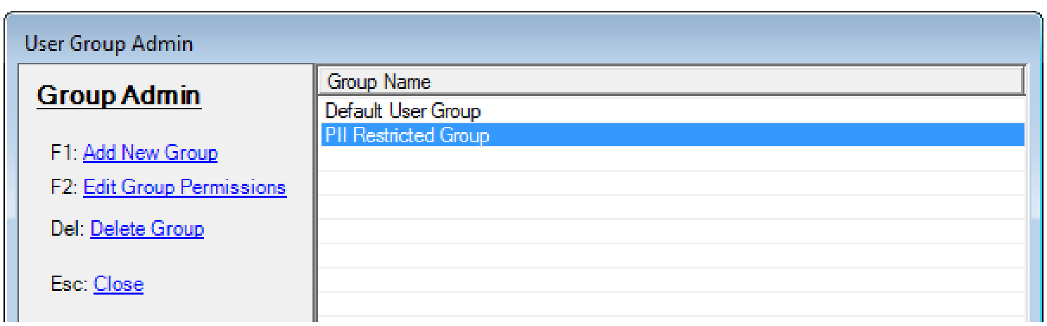
For users whose access to PII in reports has been restricted by administrators, this check box will be grayed out and cannot be unchecked. Users whose permissions allow PII to show in reports can elect to check this box before running a prebuilt report. When PII is hidden in prebuilt reports, fields that have been designated as PII, such as name or date of birth, will show as asterisks in the report. The encrypted URN will be added to these reports to provide a protected client identifier. Note that administrators define the set of fields that are considered PII for this purpose by modifying the PII Restricted Group as described below.

In custom reports, a user may add restricted PII fields to the field selections in a report. But when the report is run the PII fields will be replaced with asterisks if the user's report group assignment restricts those fields.

1. Choose **Advanced Security Options** from the **Administrative Options** menu, and then choose **User Group Admin (Reports)** from the **Advanced Security Options** menu.



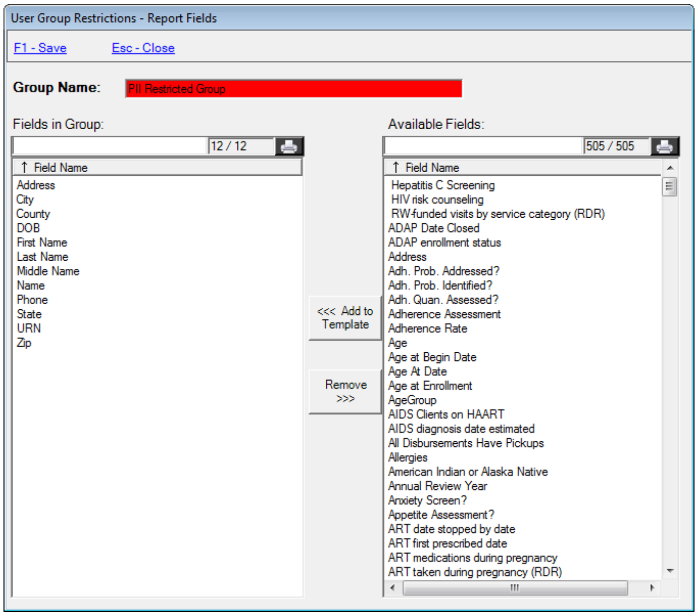
2. By default, there are two groups, **Default User Group** and **PII Restricted** group.



The **Default User Group** is automatically added to any new CAREWare user. This allows a provider to, by default, limit access to report data for all users. If your provider does not want default restrictions, add no fields to this group; no fields are restricted by default.

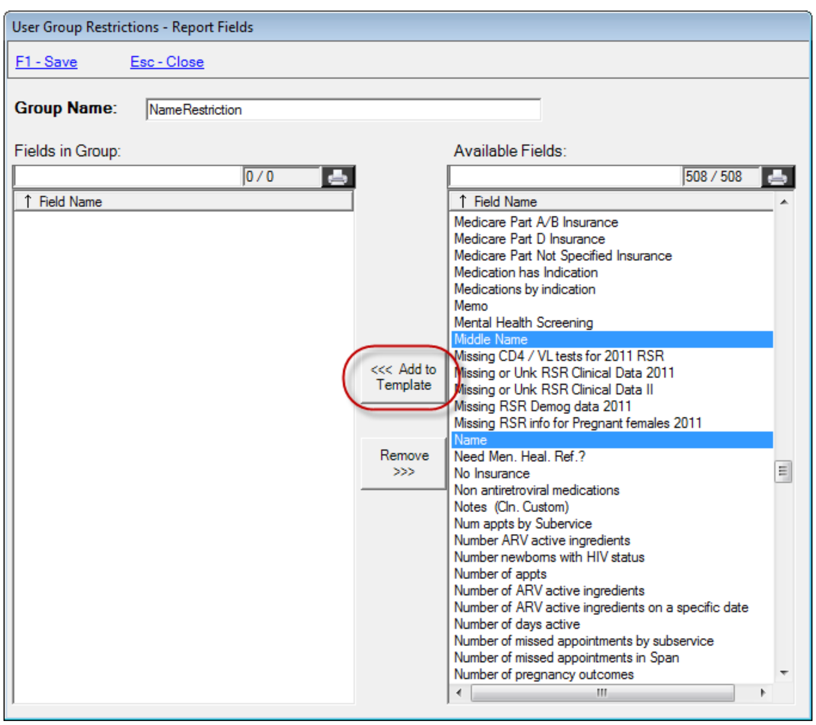
The **PII Restricted Group** defines what fields are hidden when **Hide PII Fields** is selected for prebuilt reports.

3. Highlight the **PII Restricted Group** and click **F2: Edit Group Permissions**.



The red Group Name indicates that this is a built-in Restriction Group. The Group Name cannot be changed for built-in groups, and the group cannot be deleted, but users are still allowed to define which fields are included in the group.

4. To add a new group, click **F1: Add New Group** from the menu. Name the group and begin selecting fields. Use Ctrl + Click to select more than one at a time.

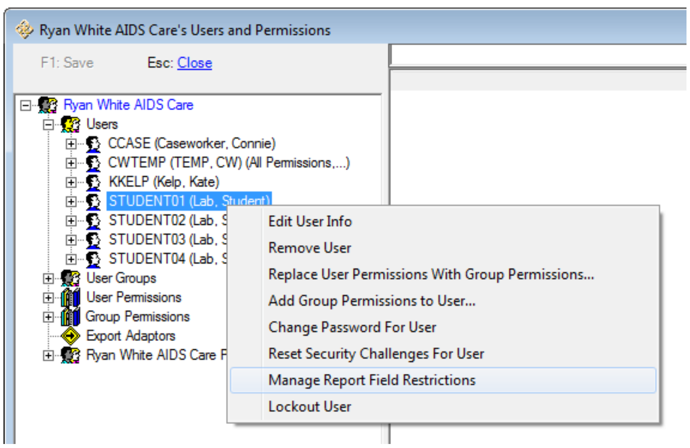


5. Click **Add to Template** to add the field(s).

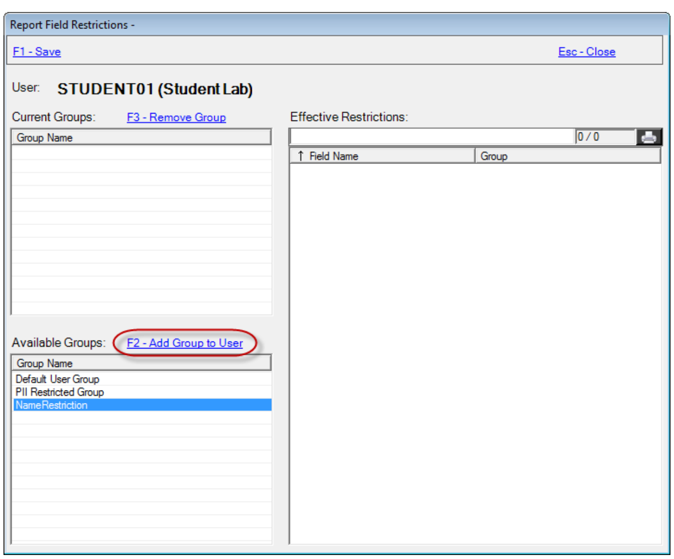
6. Click **F1: Save**.

7. Go to the **Provider/User Manager** and select the user to whom you want to apply these restrictions. Expand the Real Time Providers record if you need to apply to a provider user.

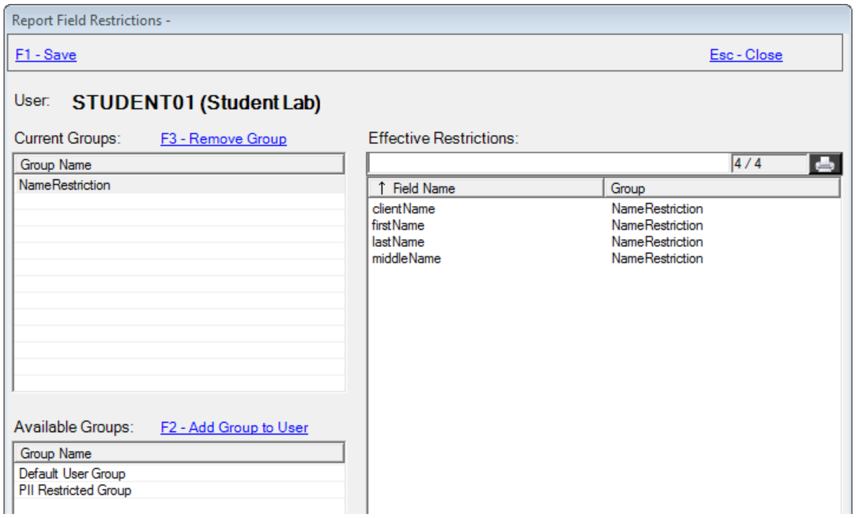
8. Right click the user and select **Manage Report Field Restrictions**.



9. Select the restriction set to be applied and click **F2 – Add Group to User**.

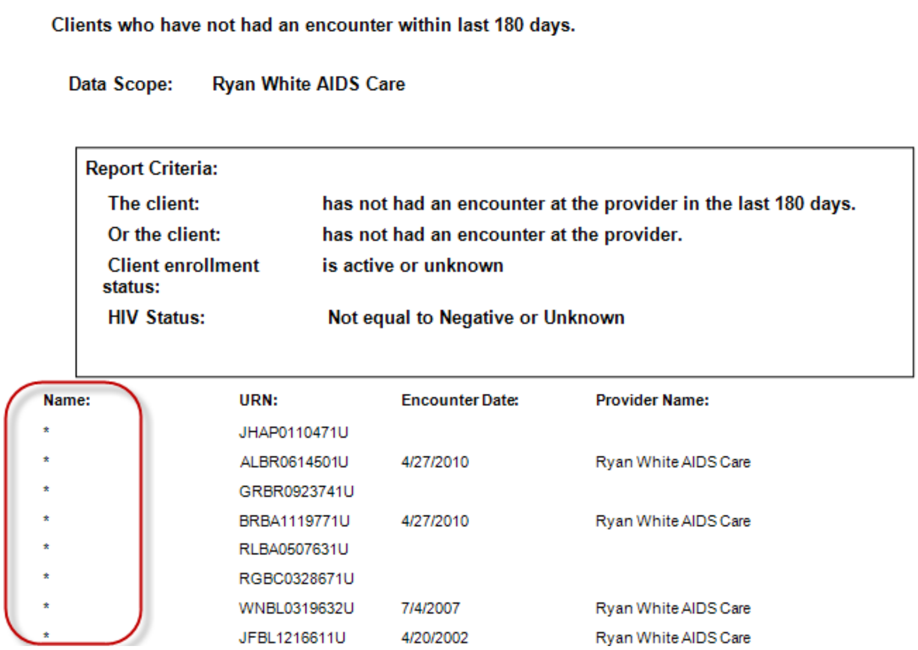


10. The list of effective restrictions populates on the right. Each group of restrictions added to this user will add to the fields listed.



11. Click **F1 – Save** to finish.

When this user runs a report, the information you designated will be masked:



Clients who have not had an encounter within last 180 days.

Data Scope: Ryan White AIDS Care

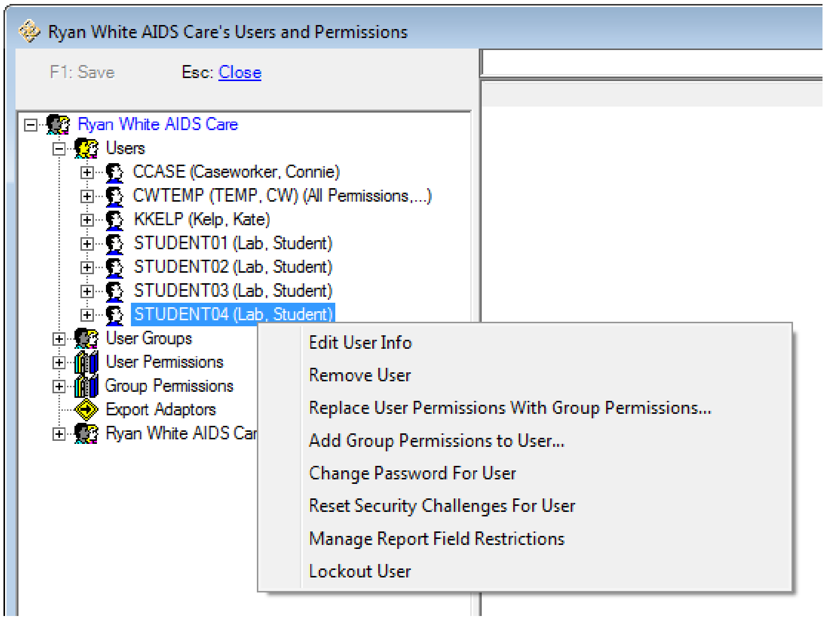
Report Criteria:

The client:	has not had an encounter at the provider in the last 180 days.
Or the client:	has not had an encounter at the provider.
Client enrollment status:	is active or unknown
HIV Status:	Not equal to Negative or Unknown

Name:	URN:	Encounter Date:	Provider Name:
*	JHAP0110471U		
*	ALBR0614501U	4/27/2010	Ryan White AIDS Care
*	GRBR0923741U		
*	BRBA1119771U	4/27/2010	Ryan White AIDS Care
*	RLBA0507631U		
*	RGBC0328671U		
*	WNBL0319632U	7/4/2007	Ryan White AIDS Care
*	JFBL1216611U	4/20/2002	Ryan White AIDS Care

Other User Management Options

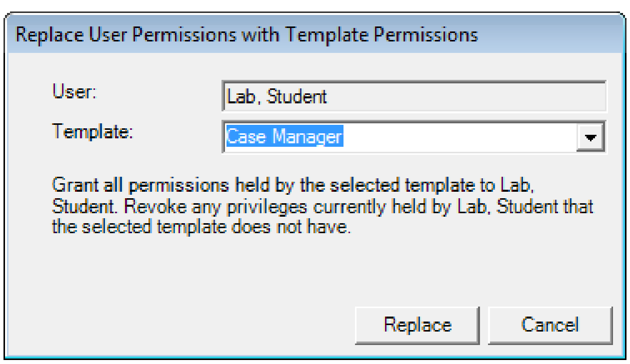
Right click on any user to access other user management options:



Edit User Info: Change the name or contact information for a user. (Caution: you cannot change a User Name / Login ID after it is has been added.)

Remove User: Remove a user's access to the database. This user's record is still available under "User/Provider Assignment / Inactive Users" for reactivation. For **HIPAA compliance**, you should immediately remove terminated employees' access. You may also wish to remove users while on extended leave. User permissions will need to be reassigned after reactivation.

Replace User Permissions with Group Permissions: This can be used to standardize users in the same role, or change the permissions of a user who transitions to a new role.



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

Reset Security Challenges for User: For users who have been locked out and unlocked (see below), resetting the security challenge questions will require them to create new challenge questions when they log in again.

Manage Report Field Restrictions: Use this tool to apply Report Field restrictions (see above) to a user.

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

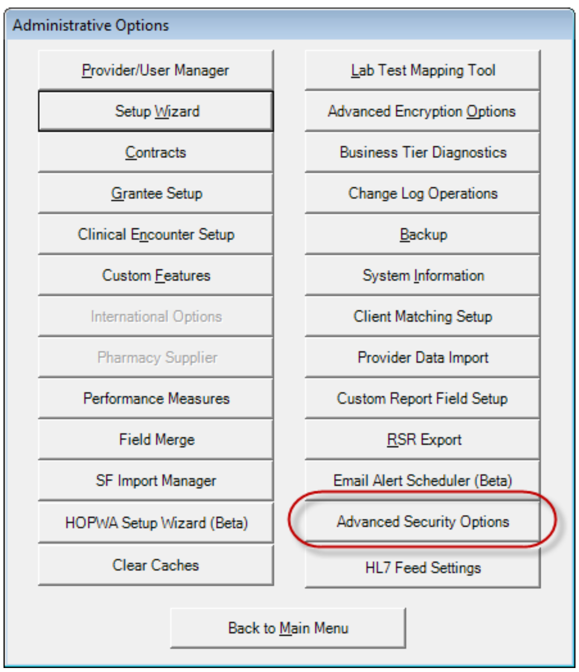
Setting up Security Questions

The (optional) Security Questions feature adds another layer of security to the CAREWare system. When a user's account has been unlocked and the password reset, the first login after the password reset will prompt the user to answer one (or more) of the Security Questions before access is restored. Failure to answer the questions correctly will relock the account.

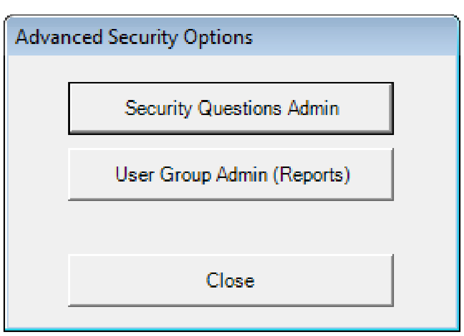
The Central Administrator sets up the pool of questions users can choose from, and sets the number of questions that must be answered correctly before login after a password reset is completed. The Central Administrator also sets the maximum number of attempts a user gets to answer a question correctly (1 or more).

Users are responsible for choosing which of the security questions they will use and for setting an answer to each. Each user must choose three security questions and give three answers.

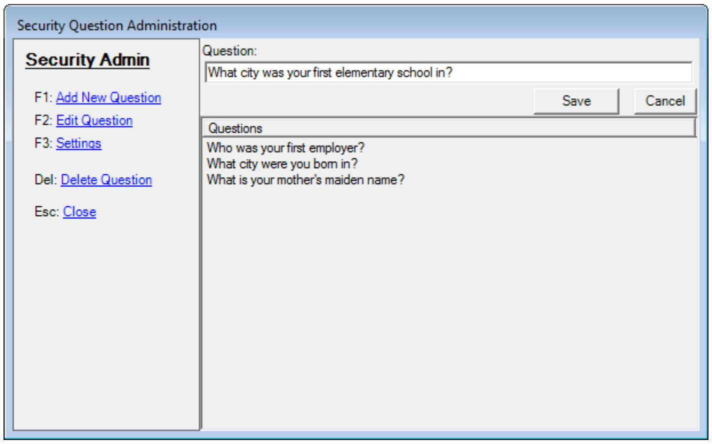
1. Choose **Advanced Security Options** from the **Administrative Options** menu.



2. Click the Security Questions Admin button.

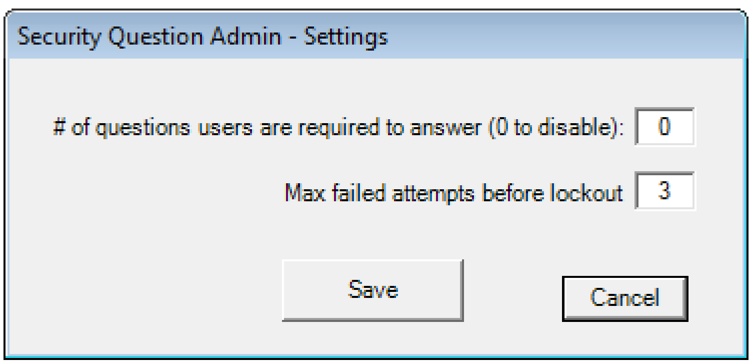


3. Click **F1: Add New Question** and type in the question. Standard security questions are seen here.



4. Click **Save** after each question.

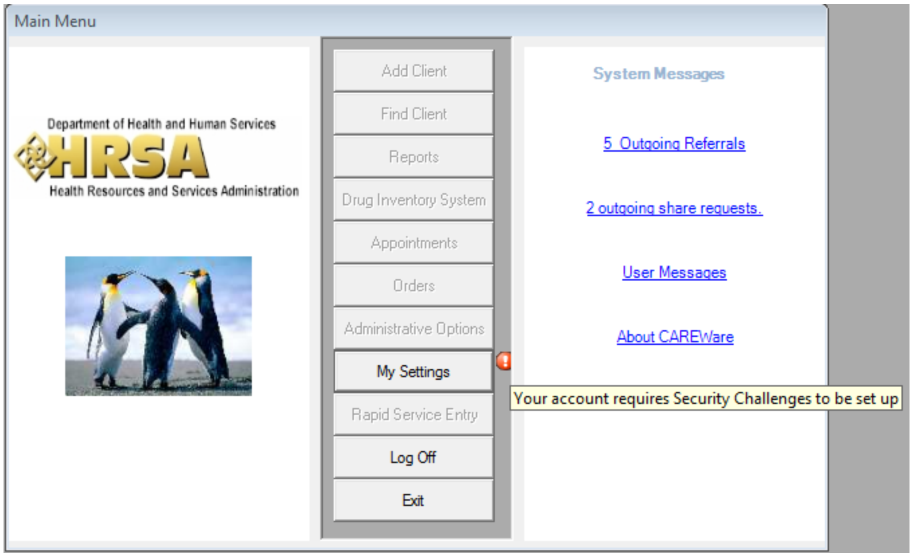
5. Click **F3: Settings.** Set the number of questions users must answer (0 disables the security questions feature) and the number of times a question can be answered incorrectly before the user's account is locked again.



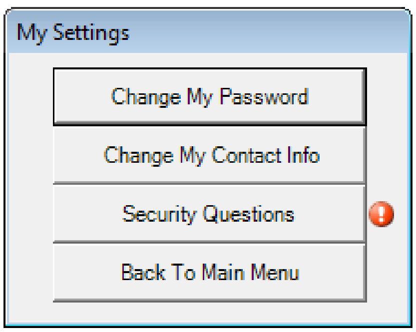
6. **Save** and **Close**.

After the Security Question feature has been activated by the Central Administrator, on their next login, users will be prompted to select Security Questions and enter answers.

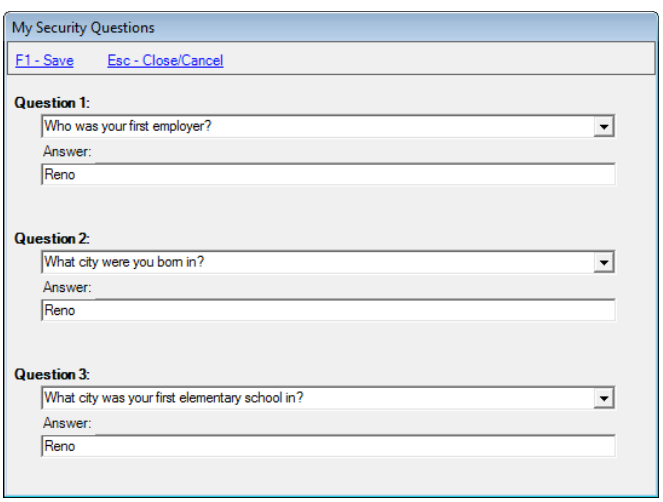
All Main Menu buttons except **My Settings, Log Off** and **Exit** will be grayed out (inactive). There will be a warning icon next to the **My Settings** button. Hovering over the icon will bring up a message box that says "Your account requires security questions to be set up."



7. Click on the **My Settings** button to proceed, then click **Security Questions**.



8. Select questions from the drop down menu, fill in the answers, and click **F1 - Save**.

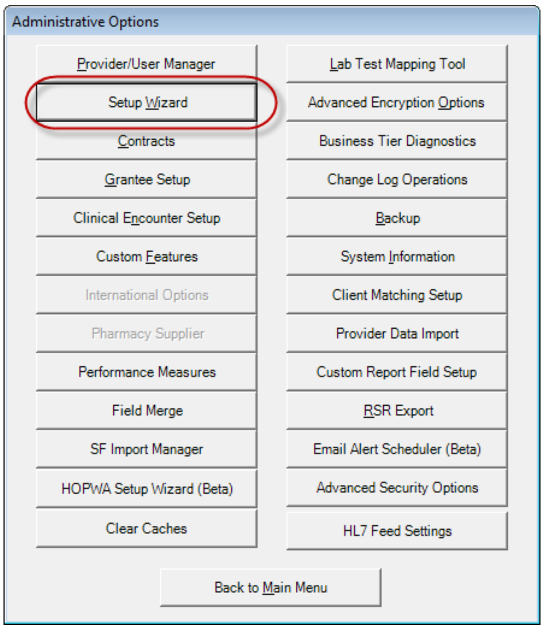


9. Users will only be asked to answer these questions after a lockout/reset.

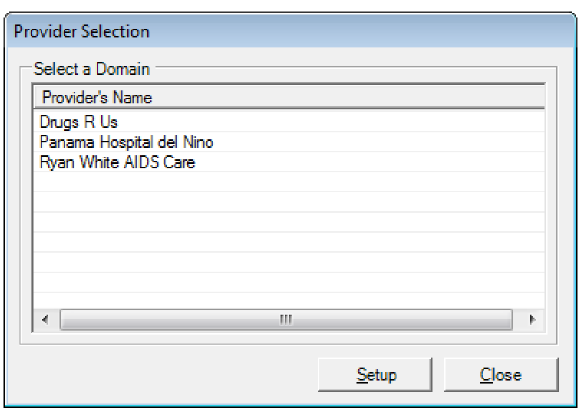
Using the Setup Wizard

Use the Setup Wizard to enter your agency's data for the RSR Provider Report. This is also where you would rename a new provider from "Default" to your agency's name.

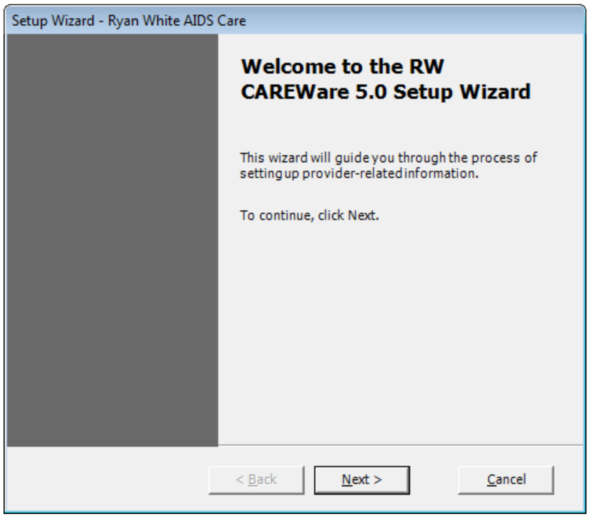
1. From Central Admin, you can set up all providers; or providers can set up or update their information individually (if granted the permissions). In either instance, from the **Administrative Options** screen, click the **Setup Wizard**.



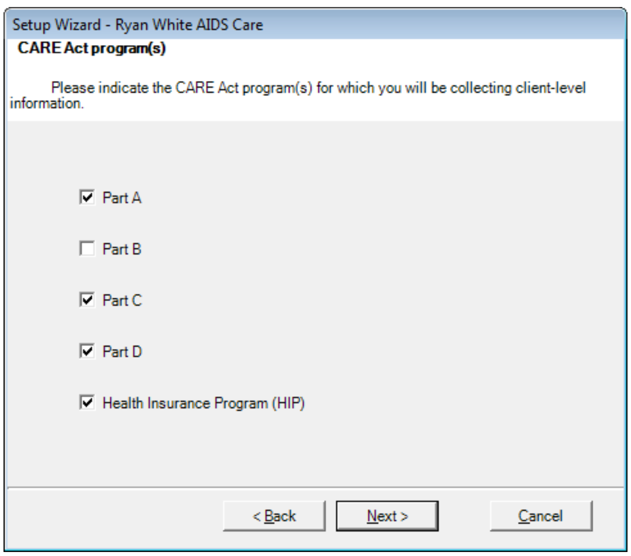
2. If you are doing this from the Central Admin domain, you'll be asked to pick a provider to set up.



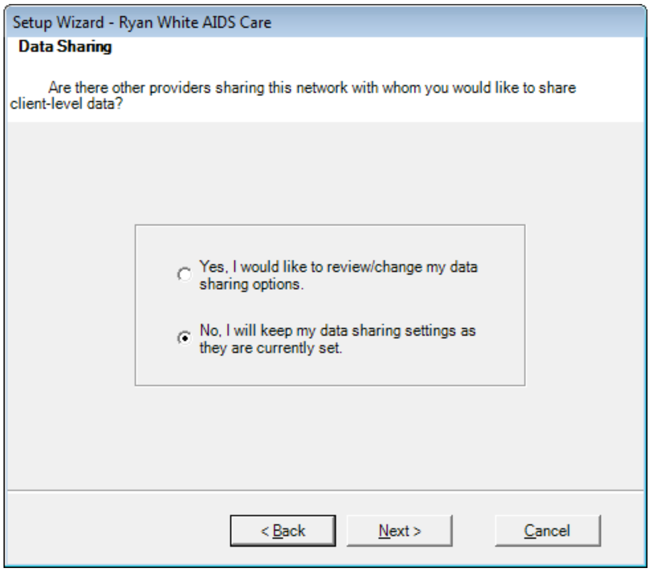
3. Click **Next** at the welcome screen.



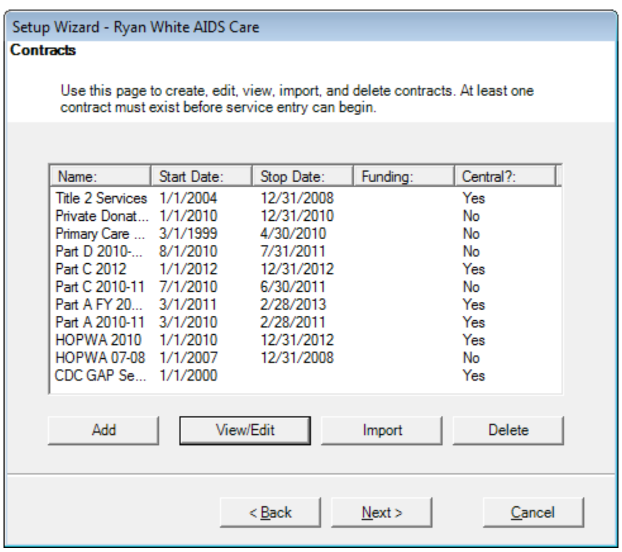
4. Check the Ryan White funding streams your agency receives.



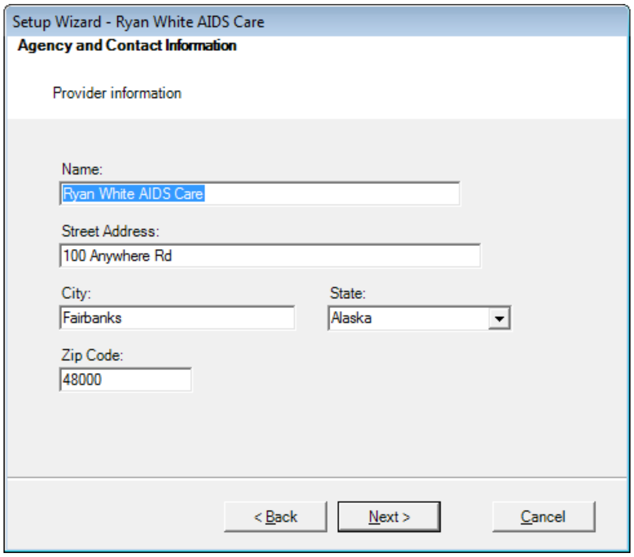
5. Click **Next** and select your data sharing options. If you are a stand-alone provider, this is not applicable; click “No, I will keep my data sharing settings.” For a complete discussion of multi-provider data sharing options, please see the complete user manual.



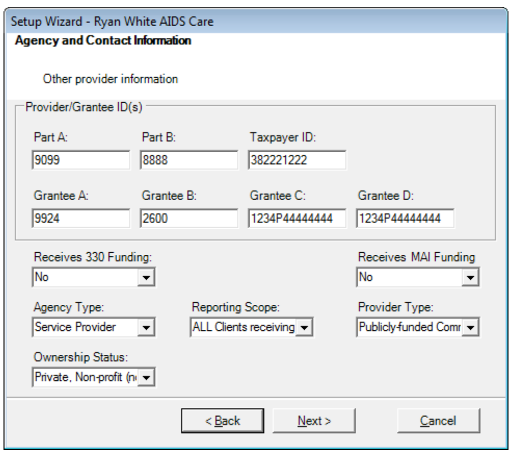
6. Click **Next** to go to the Contracts menu. You can add your contracts at this point, or go through the Administrative Options/Contracts menu later. For information on contracts, please see the guide, “Setting up contracts and services.” (This will be blank on a new install.)

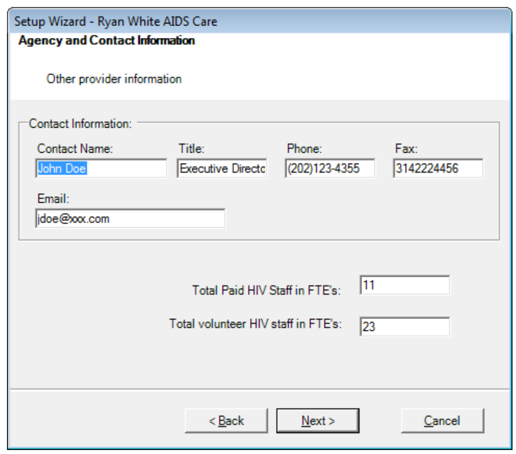


7. Click **Next** to enter your provider information (this is the information that will replace “Default” on your provider list in Provider/User Administration).

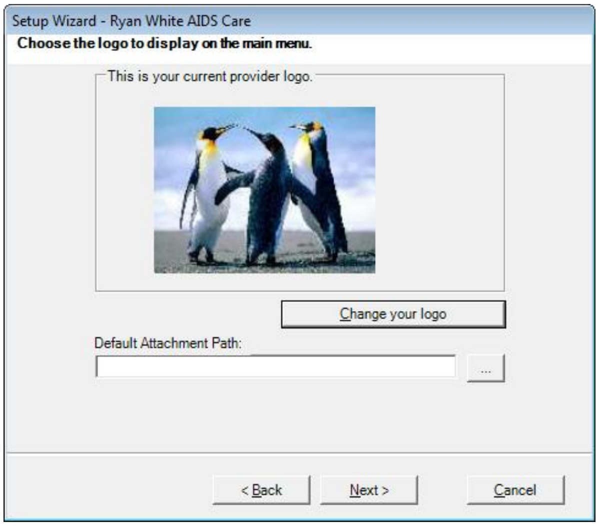


8. Click **Next** to enter additional provider information on the next two screens.

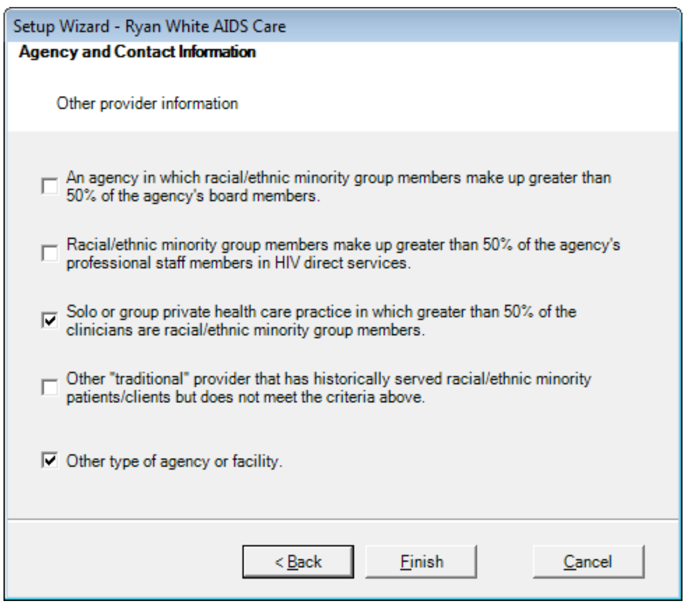




9. Click **Next** to change your provider logo. Click on **Change your logo** to select any bitmap, JPEG or GIF file. This file will then show up on the left hand side of your main menu.



10. Click **Next** to complete your provider information.

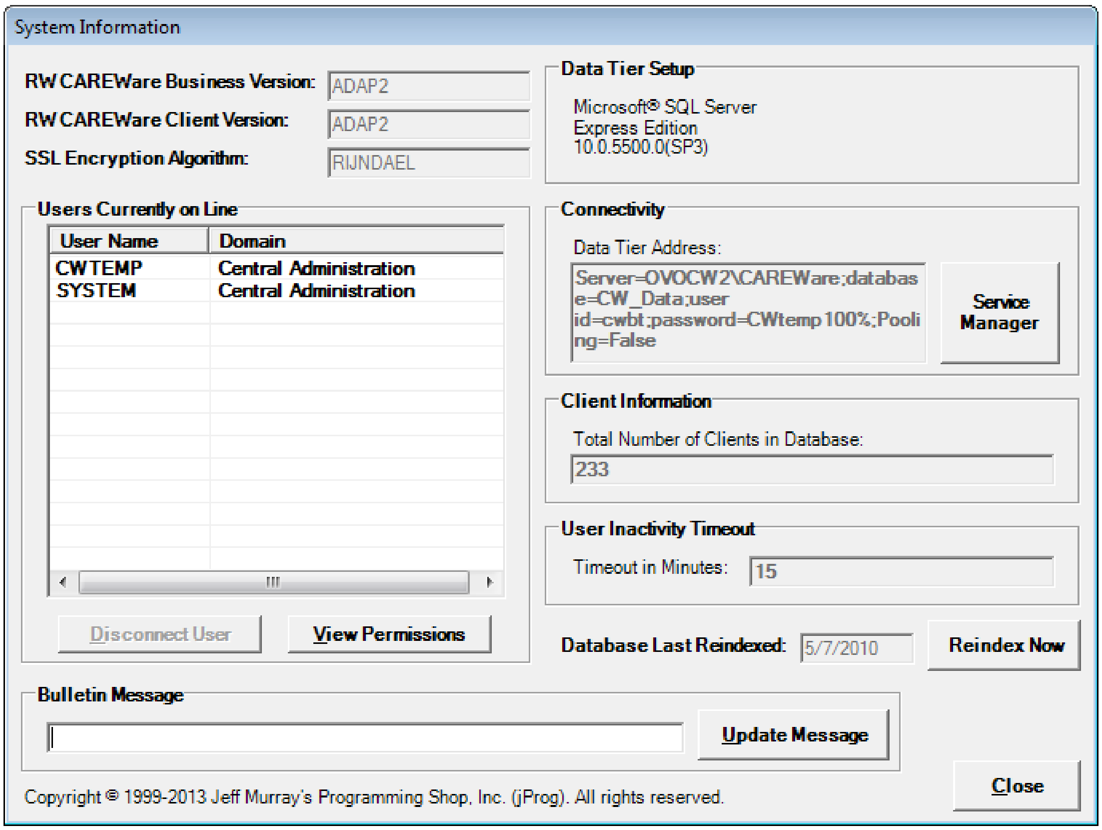


11. Click **Finish** to complete setup. (Note: you must click finish to save any changes.)

System Information

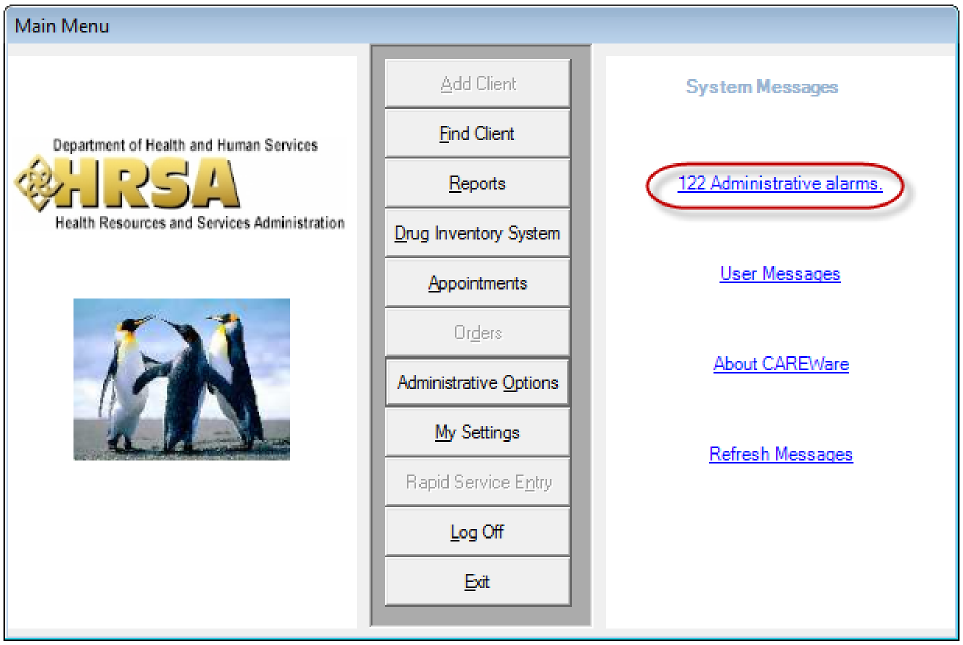
System information will give you information on your current business and client tier versions, the number of users currently online, the ability to view a user's permissions, disconnect a user, and the number of clients in the database.

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

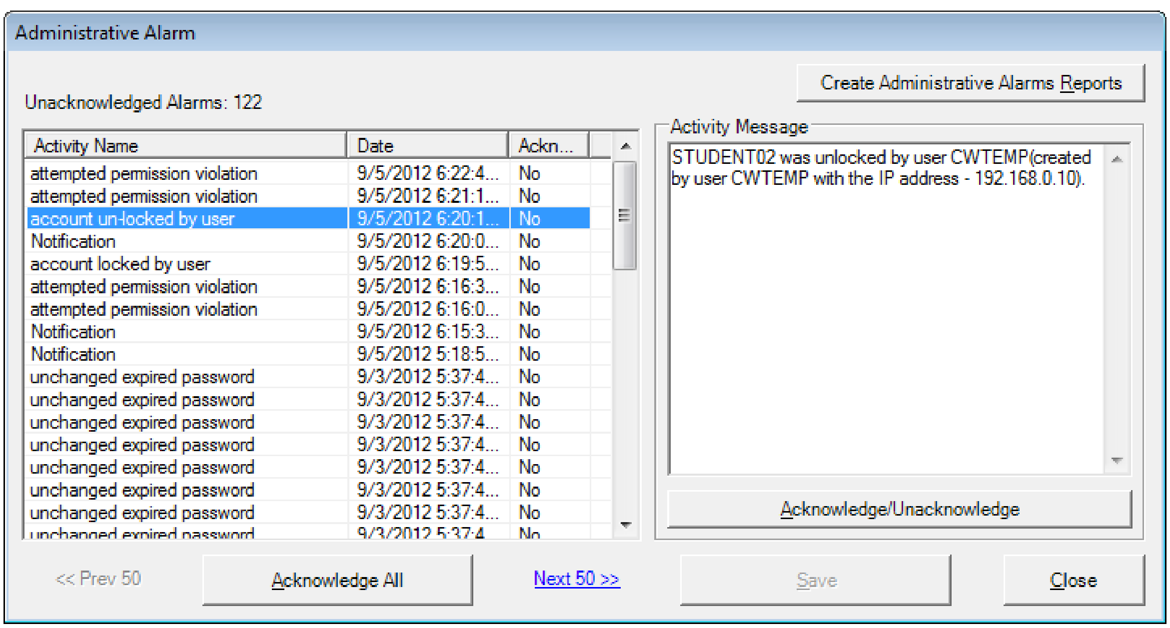


Administrative Alarms

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.



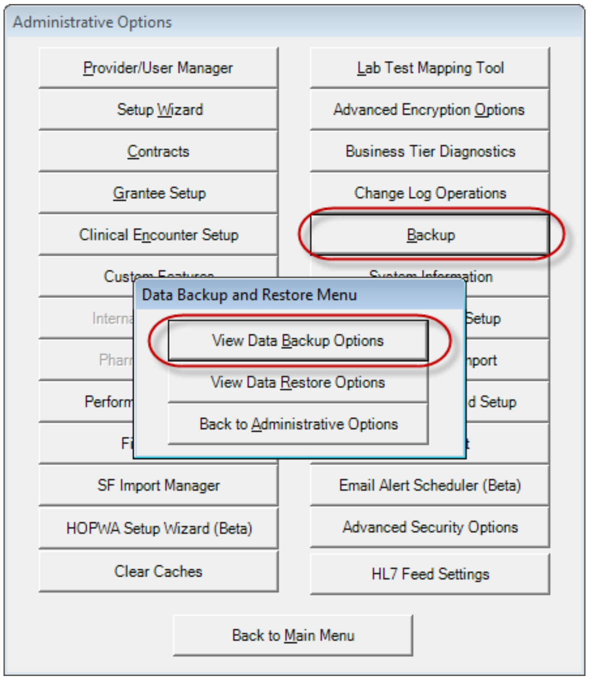
1. Click **Acknowledge All** to clear the alarms. You can click **Create Administrative Alarms Reports** to create paper trails if necessary.

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

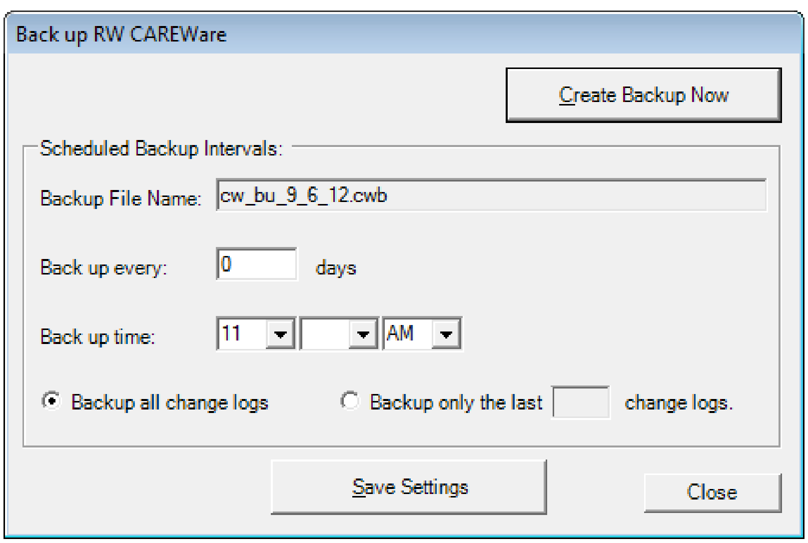
Backup and Restore

CAREWare has its own backup and restore function.

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



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



You can specify how many days between backups, or create a backup immediately (0 days). We recommend that you select **Backup all change logs** to retain complete audit trails. If you prefer, you can set **Backup only the last [number of] change logs.**

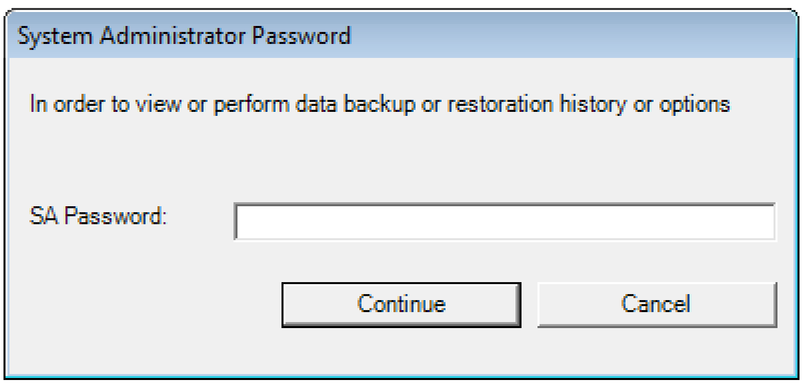
If you create a backup immediately, check your Administrative Alarms to see when it's completed.

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.

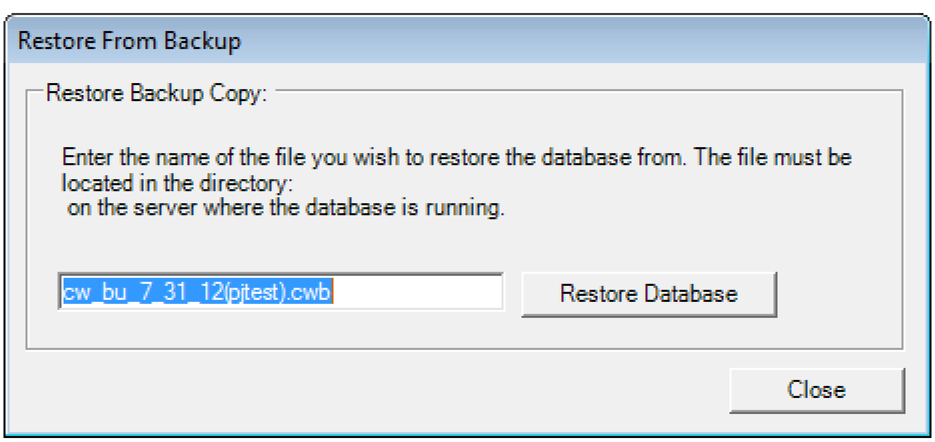
By default, CAREWare is NOT configured to make any backups. A daily backup is recommended.

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.

3. 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**.



4. 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.



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

Using SQL Management Studio Express for Restore

PLEASE NOTE: In order to **restore** a CAREWare backup (.cwb) file larger than a size of 1.5 GB, a user will need to **restore** the individual databases required for CAREWare using a SQL Manager such as Management Studio Express 2008. Please refer to the jProg website for more information.

System Optimization

RW CAREWare: Performance Checklist

Though most RW CAREWare users run the program without experiencing problems, some have reported that parts of the program respond slowly, particularly if configured in a network environment. Here are some TIPS to help those users improve the overall performance of their installation. It is not intended to replace or amend the system requirements to use RW CAREWare.

RW CAREWare Configuration:

There are several configuration changes that can be made to RW CAREWare that can improve performance.

- If the server is running a full version of SQL Server 2008 / R2 – be sure to have the latest Service Packs installed. These contain many optimizations that will have a dramatic effect on the performance of RW CAREWare, particularly when running reports.

- Install a dedicated server – if the server is running several applications, then SQL server resources will be split up among these and will usually decrease performance.

- Separate Business Tier and Data Tier – having the Business Tier and Data Tier on separate computers can have a big effect on performance in situations where there is a lot of user activity on the system. Note that both computers need to be on a very high speed connection (i.e. a LAN) and should not be separated by a firewall, which can severely degrade performance.

- Turn off service sharing – if you don't need to share services between providers, turning this feature off can significantly improve performance with all service-related processes.

- Turn off data encryption – this can boost performance in some installations, particularly on lower-end computers.

- Turn off change log audits – these logs contain all changes made to the database by users within the Client Tier. However, over time change log files can take up significant drive space and add to the overall size of CAREWare database and backup file(s).

System Hardware:

The recommended system requirements listed in the Sys-Admin document are taken from Microsoft's recommendations for the platforms on which RW CAREWare is run. Real world use has shown that using those recommendations will work, but may result in poor performance. For best performance, we recommend the following hardware specifications:

At least 2 GB of RAM, 30gb Hard-drive and a 2.00 GHz processor (Pentium 4).

General Computer Health:

The general health of the computers running RW CAREWare can have a huge impact on performance. For optimal performance, ensure that all computers:

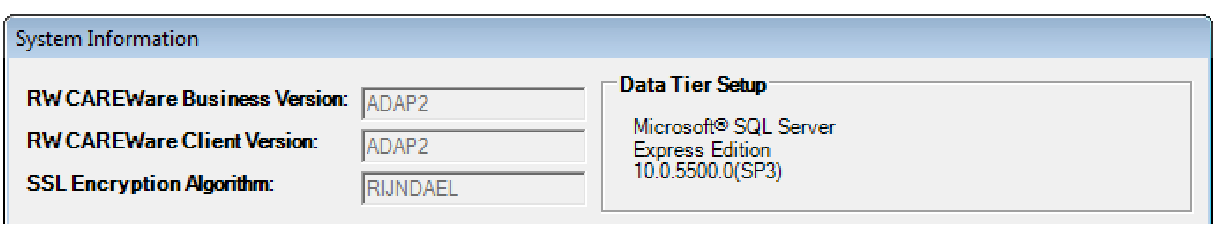
- Have the latest version of RW CAREWare
- Are free from Spyware and viruses
- Have the latest Windows Updates

SQL Server Version(s):

RW CAREWare is an enterprise level application built on MS SQL Server using the VB.Net development language. Thus, hardware configurations that can perform well with those applications should perform well with RW CAREWare.

How do I know what version of SQL Server I have?

The System Information link under Administrative Options will show your version of SQL Server on the top right, as indicated here:



Any number that begins with 8 is SQL Server 2000.

Any Number that begins with 9 is SQL Server 2005.

Any Number that begins with 10 is SQL Server 2008.

PLEASE NOTE: The free version of SQL 2008 'Express Edition' is distributed with the full version of CAREWare 5.0 and should be sufficient unless you experience lag due to heavy traffic or if your CW_Data.MDF file has exceeded or is pushing the maximum size of 4GB, in which case you should get the full version of SQL Server 2008.