CAREWare Quick Start Guide #9
User and System Administration

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 need to get basic information in and out of CAREWare.

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

Getting Started

- You must have the appropriate user privileges to run reports.

Creating New Users

CAREWare comes with a single, default 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, to allow setup of real users and assign their system privileges.

PLEASE NOTE: The Health Insurance Portability and Accountability Act (HIPAA) requires certain steps to protect the privacy and security of client protected health information (PHI).

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 could be used for unauthorized access to your database if you haven’t changed it. If you choose to keep the cwtemp user active, change the password as soon as possible.

1. If you are setting up CAREWare for the first time, 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. From the Login menu, choose **Central Administration**. For security reasons, you only have 20 seconds to choose one or the other domains.

3. Select **Administrative Options** from the **Main Menu**.
4. Select **Provider User Manager** from the links menu.

5. From the Provider User Manager menu, select **Manage Users** from the links menu.
6. You are now on the Manage Users menu. If you are configuring CAREWare for the first time, you'll only see the one user, CWTEMP. Select **New User** from the action bar.

7. Enter in the following information (as applicable) and click **Save**.
   - Username / Login ID
   - First Name
   - Last Name
   - Phone
   - Email
   - Password (repeat)
   - Title
   - Force Password Reset on first login (checkbox)

**TIP:** You may want to standardize how new username formats are created. For example; the full Last name, and first initial of the First name or vice-versa.
The **Force Password Reset on first login** checkbox can be useful for network CAREWare administrators. A “default” password can be assigned to the user for the initial login. Users will then be required to change their password to continue.

The CAREWare password must be 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:

- Is not easy to guess (e.g. not using “password1234”)
- 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”)
- 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 fields are optional. (* Note: if using the **Password Reset Manager**, a feature that allows users to unlock their own accounts; a valid email address is required in user information, to receive a password reset token via email.

It is generally recommended to complete all user contact information fields.

**User/Provider Assignment**

1. From the Manage Users Menu, select the desired user and click **Manage**.
2. Select **Manage Permissions** from the links menu.

By default, new users have no permissions. They will be unable to complete any tasks, including adding, finding clients, or editing client information.

User permissions can be Granted Individually or Granted via Groups. Final Permission Status are the combination of both individual and group permissions granted.

3. From the Permissions for User menu, highlight the permission you would like to add for the user (in this example we are adding the permission “Add Client”) and select **Grant Individual Permission** from the action bar.

With over 350 other user permissions however, adding additional user permissions in this manner would be time-consuming and make it difficult to be consistent for a large number of users. To resolve this issue, we can utilize User Groups.
Creating User Groups

Groups can be created from either the Central Administration or Provider domain. We will create a new user group for a Provider domain.

1. From the Provider User Manager menu (return to pages 1-3 for directions on accessing this menu), select Manage User Groups from the links menu.

2. Select New Group from the action bar.
3. Enter a **User Template Name** and click **Save**. You will now be on the new group’s link menu.

4. From the group’s links menu (in this example, the group’s name is Read-only), select **Change Permissions**.

5. Enter “view” in the Search box. User permissions related to “view” are displayed.
6. Select desired permissions for the Read-only user group by using the check boxes in the Select column. Note: to narrow the search results, enter additional criteria in the Search field. Once all desired permissions are selected, click **Grant Selected Permissions**.

![Permissions for Group: Read-only](image)

**NOTE:** The **Select All** can be used from the action bar (see previous screenshot). However, using this method may grant unintended user permissions. It should be used with caution. By clicking at the top of the **Status** column, the Granted permissions will be sorted before the Denied permissions.

7. Note that the Status column for the previously selected permissions have changed to Granted. Click **Back** to return to the group’s links menu.
8. Note that 5 out of 350 permissions are now granted to the **Read-only** group.

---

**Assigning Users to User Groups**

1. From the user group’s links menu, click **Assign Users**.

---

![Assigning Users to User Groups](image-url)
2. Use the Search box field to search for the desired user (in this example, we are searching for user “kkelp”). Use the checkbox to select the user and click **Save**.

3. After clicking save, you will return to the user group’s links menu. User “KKelp” has been assigned to the user group, Read-only, which has been granted five (5) permissions.
Other User Management Options

It is recommended to manage user accounts from the Central Administration domain to access the full menu of user options.

1. From the Provider User Manager menu (return to pages 1-3 for directions on accessing this menu), select **Manage Users** from the links menu.

2. From the Manage Users Menu, select the desired user and click **Manage**.
3. You are now on the user’s menu:

4. Select a desired link menu to complete/edit the following:
   - User Info
   - Assign Providers
   - Assign Provider Groups
   - Change Password
   - Change Username
   - Reset Security Challenges
   - Undo Password Lockout
   - Reset Internal 2 Factor Key
   - User Notices
   - **Undo Password Lockout** – When users enter their password incorrectly more than three times, you must Undo Password Lockout. By default, the user account will be automatically locked out of CAREWare, until unlocked.
There are several other (optional) user account security settings available in CAREWare, including:

- **Reset Security Challenges** – For users who have been locked out and unlocked, resetting the security challenge questions will require them to create new challenge questions when they log in again.
- **Email Password Reset** – Enabling this feature will allow users who are locked out to reset their own password using a token sent to the email address in their user settings.

A user account cannot be Deleted, only the username can be changed. Users can be assigned and reassigned to multiple providers.

If a user is not assigned to any provider, the user account will automatically change to **User retired**. (Note: when a user account is “retired”, all previously assigned individual and group permissions will automatically be revoked.)

### Restriction of PII in Reports

This feature allows administrators to restrict users’ access to Personal Identifying Information (PII) that is available in most CAREWare built-in reports on a field-by-field basis. With sufficient permissions, a user may select the **Hide Personally Identifying Information** box to conceal certain field selections in prebuilt reports.

When reports are run, PII fields will be replaced with asterisks in the restricted fields:

Report restrictions can also be managed via permission groups configured within the **User Group Admin (Reports)** menu in the **Central Administration** domain.
1. From Administrative Options on the **Main Menu**, select the **Advanced Security Setup** link.
2. Select the **User Group Admin (Reports)** link.

3. Select the PII Restricted Group from the User Group column. Note the number five (5) under the Restrictions column. Click **Manage** from the action bar.
4. On the Manage menu, select **Edit Group Restrictions**.

5. By default, five (5) PII Restricted fields are preselected: Name, Last Name, First Name, Middle Name, and URN. These are the fields that will be hidden when the **Hide Personally Identifying Information** box is selected for prebuilt reports. To edit restrictions, check/uncheck the boxes in the Granted column and click **Save**.
6. On the User Group Admin (Reports) menu (see steps 1-3), new User Group(s) with customized restricted fields can also be created. To do so, click **Add** from the action bar.

7. Enter in the **Group Name** and click **Save**.

8. To apply the restrictions, go to the Manage Users menu (see pages 1-3) and select the desired user. Click **Manage**.

10. From the Report Field Restrictions for User menu, select **Manage Restrictions**.

11. Select the desired Group name by placing a check in the Granted column. Click **Save**.
12. The Report Field Restrictions are now displayed for the selected user.

**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 within 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 certain providers' 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. Log in to the **Central Administration** domain.
2. Select **Administrative Options** from the **Main Menu**.

3. Select **Provider User Manager** from the links menu.
4. From the Provider User Manager menu, select **Manage Providers** from the links menu.

5. Select the relevant provider and click **Manage** from the action bar.
6. Select **Manage Permissions** from the link menu.

7. In this example, we will revoke some ADAP drug permissions as this agency does not provide any ADAP services. Enter “ADAP drug” in the Search box. Select one of the ADAP permissions and select **Revoke Individual Permission** from the action bar. Continue until the remaining ADAP drug permissions are revoked.
8. Now, once we switch providers and log into the Ryan White AIDS Care and Treatment Clinic provider domain, the “ADAP drug” permissions are listed as “No (Locked for Provider)” under the Granted via Groups column.

Now, regardless of group permissions applied, no user at this agency can access the locked section unless you unlock the Permissions for Provider or change Provider Permissions Group from the Central Administration domain.

Other Provider Management Options

Deleting Providers

WARNING: Deleting a Provider will PERMANENTLY remove the provider, including all records (tests, services, referrals, etc.) associated with this provider. Additionally, any clients that are ONLY associated with this provider will also be deleted. Once these records are deleted, there is NO WAY TO RESTORE the data.

Instead, it is recommended to Deactivate a Provider, which will retain provider settings and save client data, should the provider be reactivated in the future. Please refer to the next section for further instructions.

To delete a provider:

1. From the Manage Providers menu, highlight the desired provider by clicking on the provider’s name, and click Delete from the action bar.
2. A Delete Confirm box will appear. To confirm, you must type in the word “DELETE” into the text box and click Confirm.

Deactivating Providers

1. From the Manage Providers menu, highlight the desired provider by clicking on the provider’s name, and click Manage from the action bar.
2. Select the **Deactivate Provider** link.

3. The link will change to **Reactive Provider**. To reactivate the provider, select the **Reactivate Provider** link.
Using the Provider Setup

Provider Setup is used to edit an agency’s name, information, contact information, or add a provider logo. This is also where you would rename the “Default” provider to your agency’s name, in a new installation of CAREWare.

From Central Administration, you can set up all providers.

1. Log in to the **Central Administration** domain.

2. Select **Administrative Options** from the **Main Menu**.
3. Select **Provider Management** from the links menu.

4. Select **Provider Setup**.
5. Select “Default” provider, then click **Manage Selected Provider** from the action bar.

Using the Provider Setup, CAREWare administrators can set up sharing for services, clinical data, case notes, appointments, custom subforms, and the form designer.

As a stand-alone provider, this is not applicable and will not be covered here. (For further information regarding multiple provider and network data sharing options, please refer to the CAREWare developer website: https://www.jprog.com/)

6. Once you click **Manage Selected Provider**, you will be at the provider’s Provider Setup menu.
7. Select CARE Act Program(s). Click Edit. Check the Ryan White funding sources your agency receives. Click Save.

8. Select Agency Information. Enter your provider information (this is the information that will replace the “Default” provider), in a new installation of CAREWare. Click Save.
9. Select **Additional Agency Information**. Enter your provider information. It is recommended to use the ID’s applicable on the RSR report for easy cross reference. Click **Save**.

**TIP:** The agency DUNS number can be entered in the **Other Provider Type** field.
10. Select **Contact Information**. Enter the primary contact information for your agency. Click **Save**.

11. Select **Agency Type**. Enter all that apply for your agency. Click **Save**.
12. Select **Provider Logo**, to add or change your agency logo. Select **Browse** to upload any .BMP, .GIF, .JPG, or JPEG file format. This file will then be displayed on your agency’s title page in CAREWare.

![Provider Logo](image)

**System Information and Messages**

**System Information**

System Information will provide CAREWare administrators the current CAREWare Business Tier version, the number of clients in your agency database, currently connected users, etc.

1. Select System Information from the Main Menu.
2. Select **Bulletin Message**.

3. Here, you can publish a “bulletin message” that will appear on all users’ screens. Enter a message into the text box and click **Save**.
System Messages

System Messages provide CAREWare administrators information regarding Administrative Alarms and allow them to send User Messages.

1. Select **System Messages** from the **Main Menu**.

2. Select **Administrative Alarms**. Administrative alarms are system notifications and are typically user-related, regarding attempted permission violations or account locks or unlocks.
3. After review, Administrative alarms can be cleared/acknowledged, by selecting one or more notifications. Click **Acknowledge** on the action bar.

4. Administrative alarms can also be sorted and printed like other reports in CAREWare. Select **Setup Parameters** from the **Administrative Alarms** link menu.
5. Click **Edit** and enter the report specifications. Once complete, click **Save** (this option will take the place of Edit within the action bar). Then, click **Run Report**.

6. Administrative alarms can ALL be cleared or acknowledged automatically. Select **Acknowledge Alarms** from the **Administrative Alarms** link menu. (Note: all alerts will be deleted so should be used with caution.)