

CAREWare 6

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.

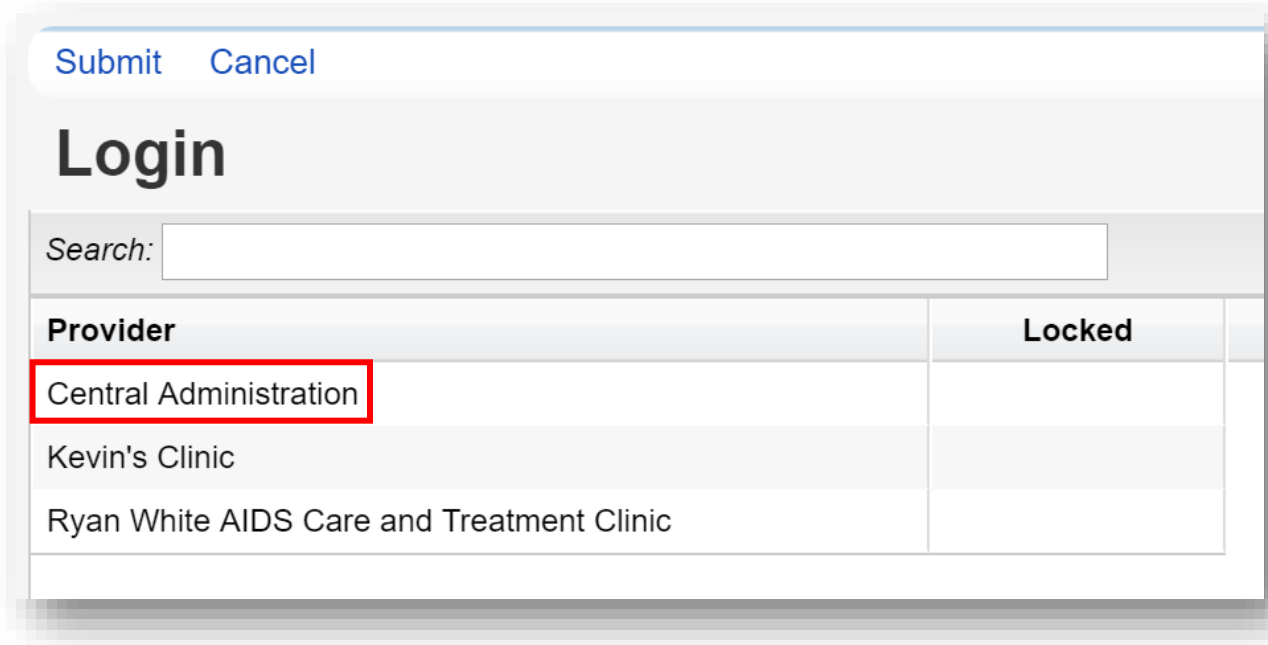
Submit

Login

Enter your CAREWare Username

Username:

- From the **Login** menu, choose **Central Administration**. For security reasons, you only have 20 seconds to choose one or the other domains.



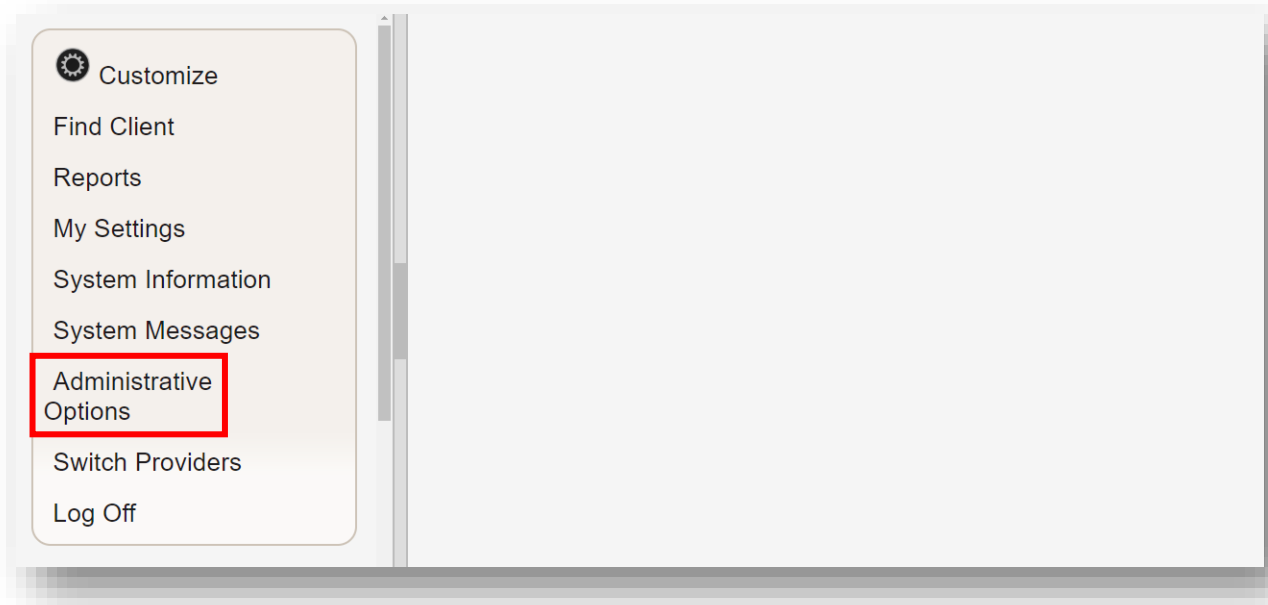
Submit Cancel

Login

Search:

Provider	Locked
Central Administration	
Kevin's Clinic	
Ryan White AIDS Care and Treatment Clinic	

- Select **Administrative Options** from the **Main Menu**.



- Customize
- Find Client
- Reports
- My Settings
- System Information
- System Messages
- Administrative Options
- Switch Providers
- Log Off

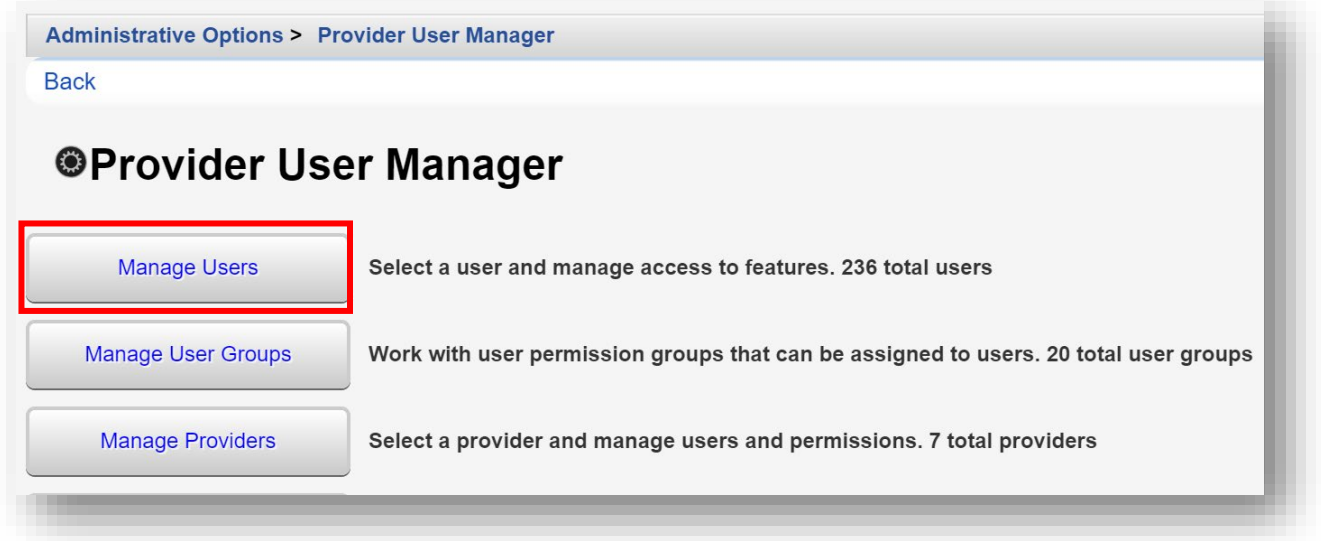
- 4. Select **Provider User Manager** from the links menu.



The screenshot shows a web interface titled "Administrative Options" with a gear icon. Below the title, there are four menu items, each in a rounded rectangular button. The first item, "Provider User Manager", is highlighted with a red border. To the right of each button is a brief description of its function.

Menu Item	Description
Provider User Manager	Manage Provider and User Permissions
Custom Features	Manage Custom Fields
Advanced Security Setup	Manage Advanced Security Setup
Data Import and Export Features	(PDI, PDE, HL7)

- 5. From the Provider User Manager menu, select **Manage Users** from the links menu.



The screenshot shows a web interface titled "Provider User Manager" with a gear icon. At the top, there is a breadcrumb trail "Administrative Options > Provider User Manager" and a "Back" link. Below the title, there are three menu items, each in a rounded rectangular button. The first item, "Manage Users", is highlighted with a red border. To the right of each button is a brief description of its function and the number of items it manages.

Menu Item	Description
Manage Users	Select a user and manage access to features. 236 total users
Manage User Groups	Work with user permission groups that can be assigned to users. 20 total user groups
Manage Providers	Select a provider and manage users and permissions. 7 total providers

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.

Administrative Options > Provider User Manager > Manage Users

Manage **New User** Back Print or Export

Manage Users

Search: CWTEMP

Username	First Name	Last Name	Status	Realtime	Central User
CWTEMP	CW	TEMP	Active	6	X

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)

Administrative Options > Provider User Manager > Manage Users > New User

Save Back

New User

Username / Login ID:

First Name:

Last Name:

Phone:

Email:

Password:

Repeat Password:

Title:

Force Password Reset on first login:



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**.

Administrative Options > Provider User Manager > Manage Users

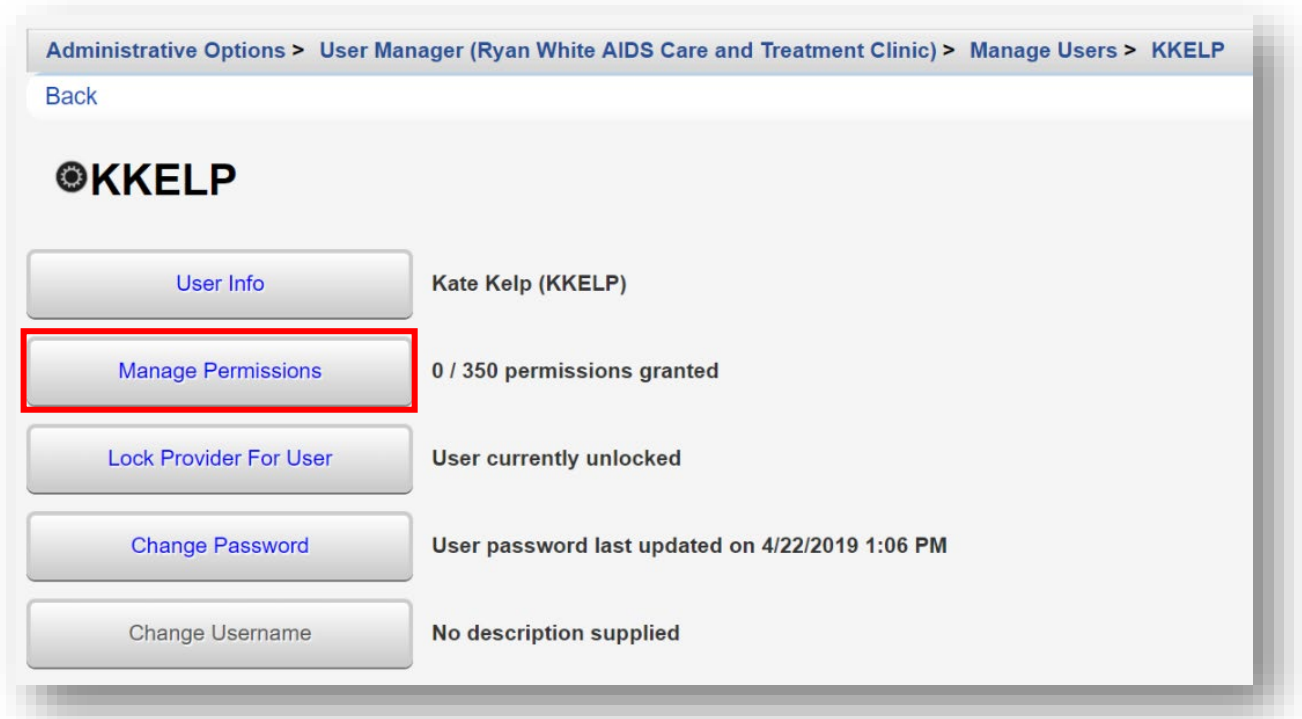
Manage New User Back Print or Export

Manage Users

Search: Kelp

Username	First Name	Last Name	Status	Realtime	Central User	Global
KKELP	Kate	Kelp	Active	1		

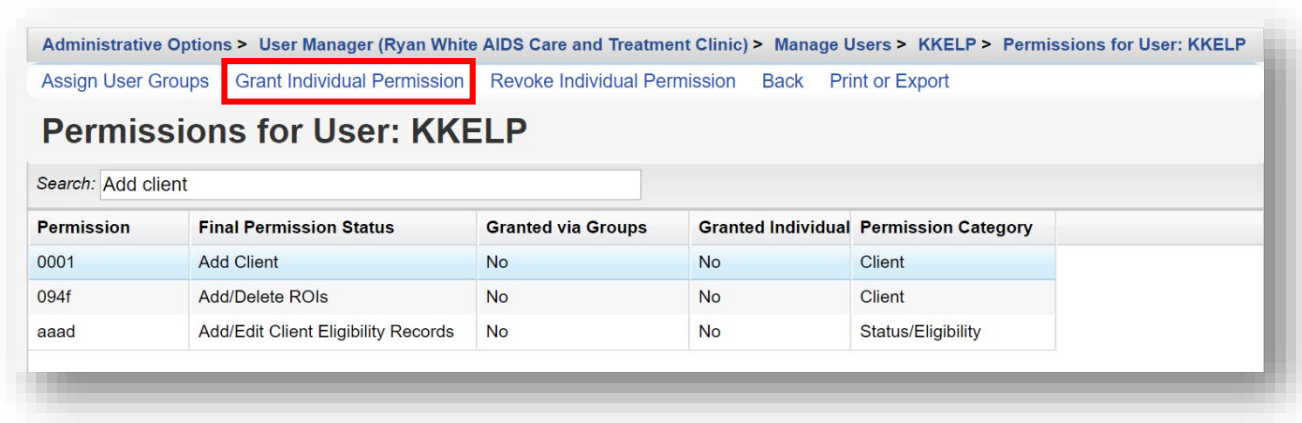
2. Select **Manage Permissions** from the links menu.



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.

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic)

Cancel

Provider User Manager

- [Manage Users](#) Select a user and manage access to features within the provider. 32 total users
- [Manage User Groups](#)** Work with user permission groups that can be assigned to users. 14 total user groups
- [Manage Permissions](#) 332 / 350 permissions granted

2. Select **New Group** from the action bar.

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Manage User Groups

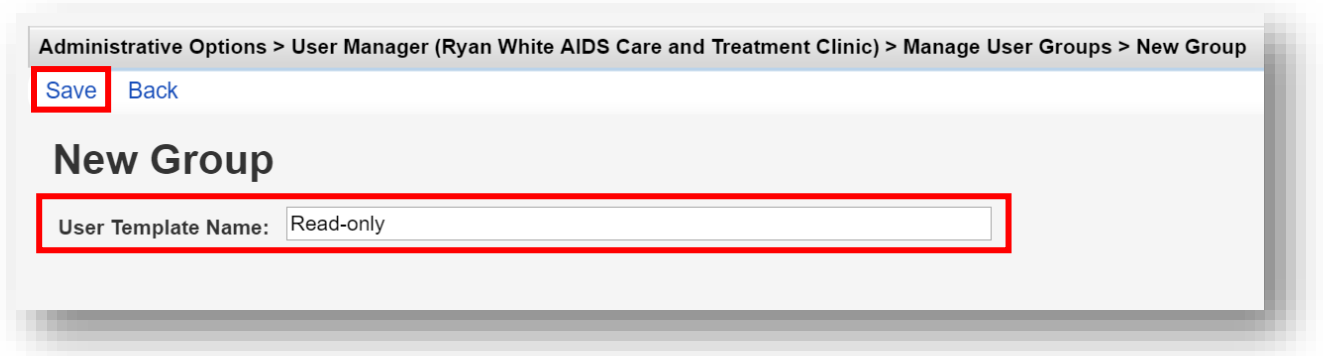
Manage **New Group** Delete Back Print or Export

Manage User Groups

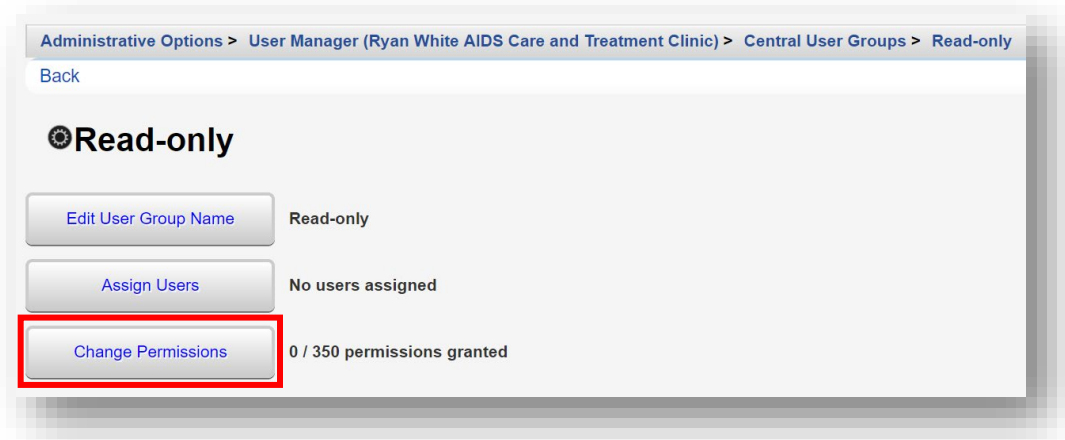
Search:

User Group Name	Created By	Number Users Assigned
All Permissions	Central Administration	2
Some Permissions	Central Administration	6
SF_template	Central Administration	2
ADAP Template 1	Central Administration	2
39573957	Ryan White AIDS Care and Treatment Clinic	3

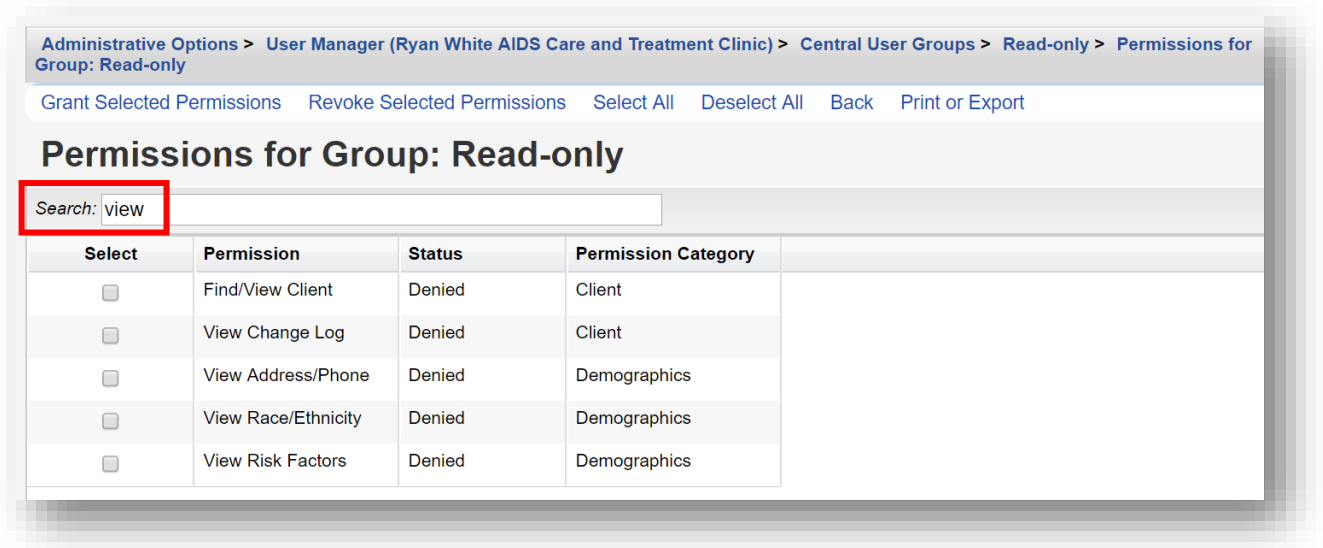
3. Enter a **User Template Name** and click **Save**. You will now be on the new group’s link menu.



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**.


Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Central User Groups > Read-only > Permissions for Group: Read-only

Grant Selected Permissions Revoke Selected Permissions Select All Deselect All Back Print or Export

Permissions for Group: Read-only

Search: view

Select	Permission	Status	Permission Category
<input checked="" type="checkbox"/>	Find/View Client	Denied	Client
<input checked="" type="checkbox"/>	View Change Log	Denied	Client
<input checked="" type="checkbox"/>	View Address/Phone	Denied	Demographics
<input checked="" type="checkbox"/>	View Race/Ethnicity	Denied	Demographics
<input checked="" type="checkbox"/>	View Risk Factors	Denied	Demographics

 **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.

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Central User Groups > Read-only > Permissions for Group: Read-only

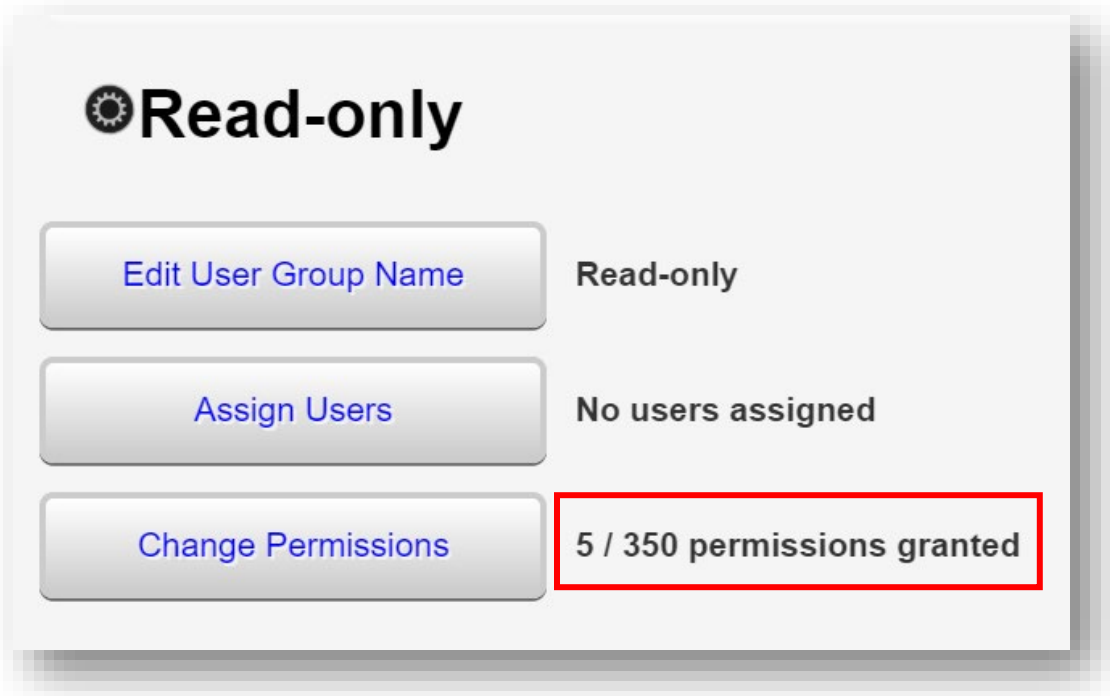
Grant Selected Permissions Revoke Selected Permissions Select All Deselect All Back Print or Export

Permissions for Group: Read-only

Search: view

Select	Permission	Status	Permission Category
<input type="checkbox"/>	Find/View Client	Granted	Client
<input type="checkbox"/>	View Change Log	Granted	Client
<input type="checkbox"/>	View Address/Phone	Granted	Demographics
<input type="checkbox"/>	View Race/Ethnicity	Granted	Demographics
<input type="checkbox"/>	View Risk Factors	Granted	Demographics

- Note that 5 out of 350 permissions are now granted to the **Read-only** group.

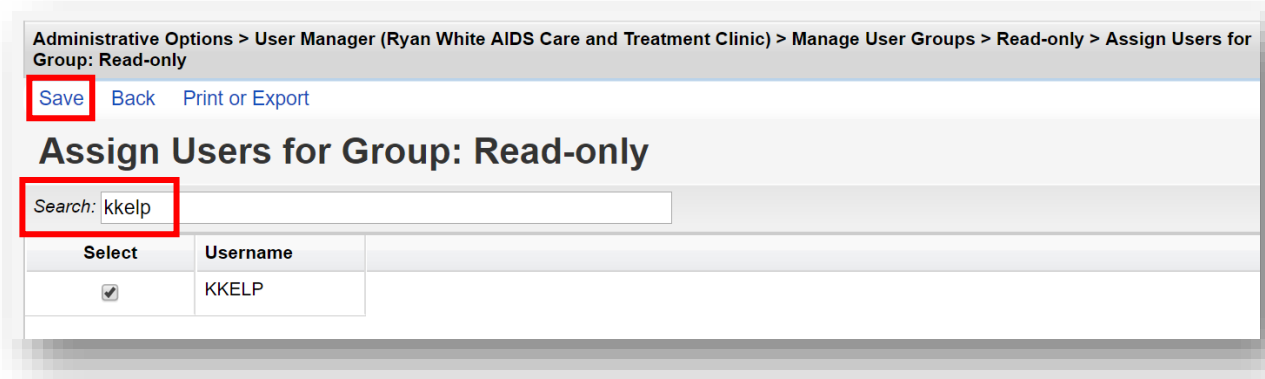


Assigning Users to User Groups

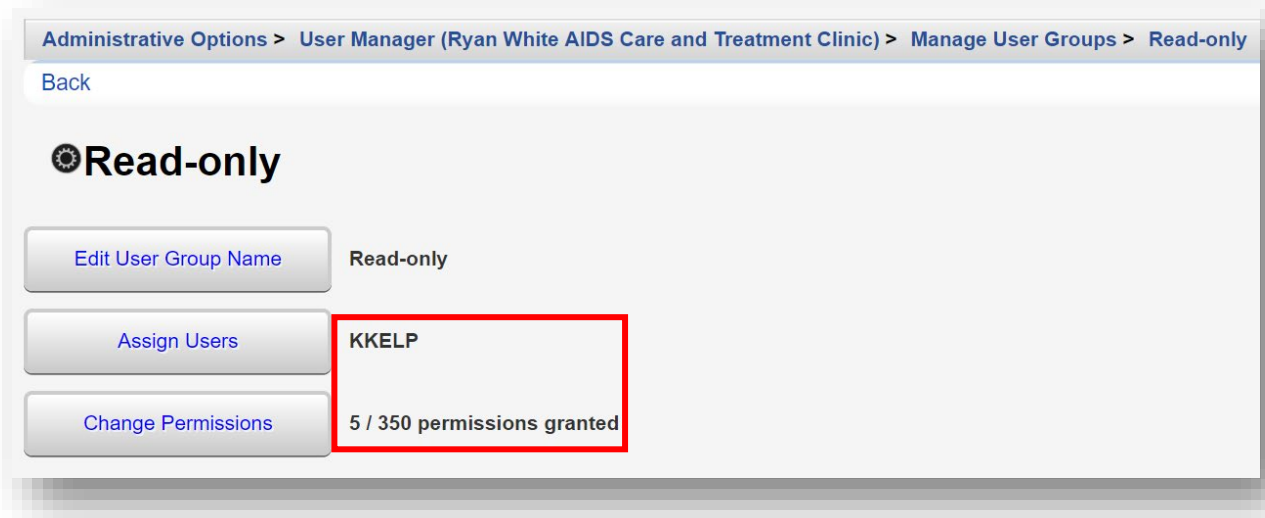
- From the user group’s links menu, click **Assign Users**.



- 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**.



- 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.

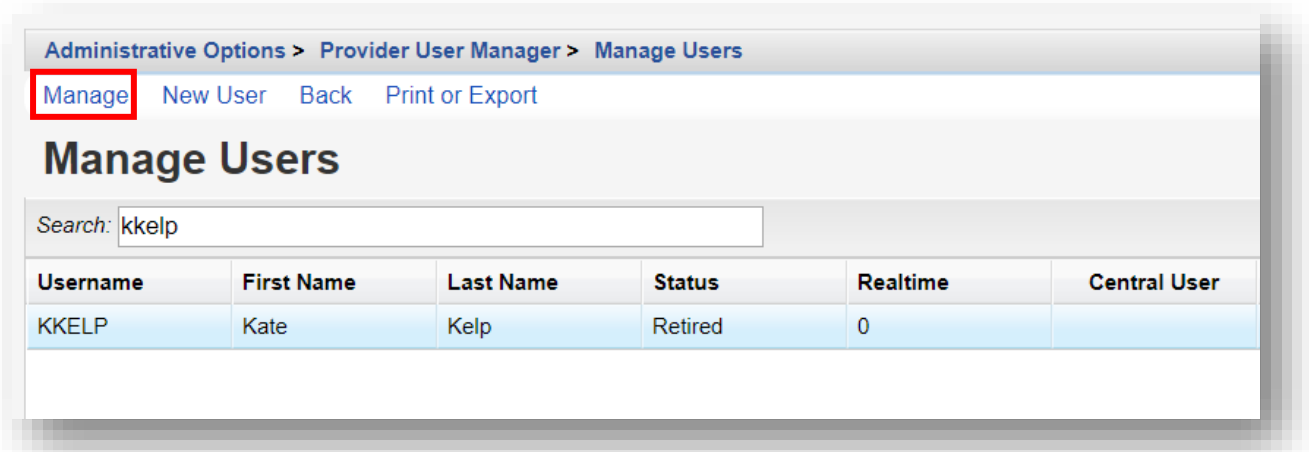
1. From the Provider User Manager menu (return to pages 1-3 for directions on accessing this menu), select **Manage Users** from the links menu.



The screenshot shows the 'Provider User Manager' interface. At the top, there is a breadcrumb trail: 'Administrative Options > Provider User Manager'. Below this is a 'Back' link. The main heading is 'Provider User Manager' with a gear icon. There are four main menu items, each with a button and a description:

- Manage Users** (highlighted with a red box): Select a user and manage access to features. 237 total users
- Manage User Groups**: Work with user permission groups that can be assigned to users. 21 total user groups
- Manage Providers**: Select a provider and manage users and permissions. 7 total providers
- User Notices**: Manage user notices

2. From the Manage Users Menu, select the desired user and click **Manage**.



The screenshot shows the 'Manage Users' interface. At the top, there is a breadcrumb trail: 'Administrative Options > Provider User Manager > Manage Users'. Below this is a 'Manage' button (highlighted with a red box), followed by 'New User', 'Back', and 'Print or Export' links. The main heading is 'Manage Users'. There is a search field with the text 'kkelp' entered. Below the search field is a table with the following data:

Username	First Name	Last Name	Status	Realtime	Central User
KKELP	Kate	Kelp	Retired	0	

3. You are now on the user's menu:

The screenshot displays the 'Manage Users' page for user 'KKELP'. The breadcrumb trail is 'Administrative Options > Provider User Manager > Manage Users > KKELP'. A 'Back' link is visible. The user's name 'Kate Kelp (KKELP)' is shown at the top. Below this, a list of management actions is provided, each with a button and a description of the action's effect.

Action	Description
User Info	Kate Kelp (KKELP)
Assign Providers	Ryan White AIDS Care and Treatment Clinic
Assign Provider Groups	Read-only
Change Password	User password last updated on 4/22/2019 1:06 PM
Change Username	Change this user's Username
Reset Security Challenges	Reset will force the user to setup Security Challenges upon next login
Undo Password Lockout	Not Locked Out
Reset Internal 2 Factor Key	Server is not set up for 2 factor auth
User Notices	View acknowledged user notices

4. Select a desired link menu to complete/edit the following:

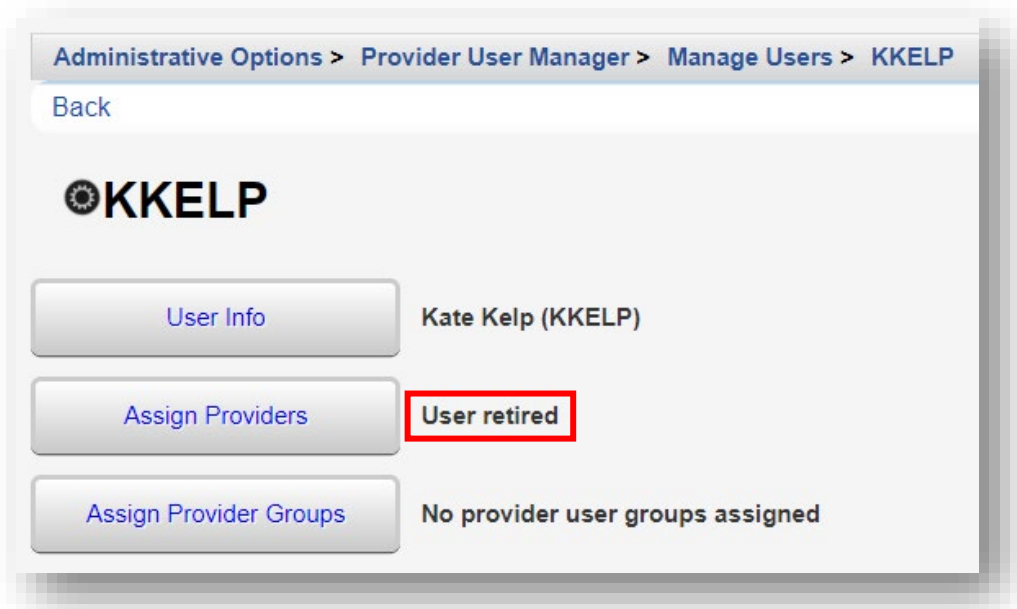
- **User Info**
- **Assign Providers**
- **Assign Provider Groups**
- **Change Password**
- **Change Username**
- **Reset Security Challenges**
- **Undo Password Lockout**
- **Reset Internal 2 Factor Key**
- **User Notices**
- **Undo Password Lockout** – When users enter their password incorrectly more 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

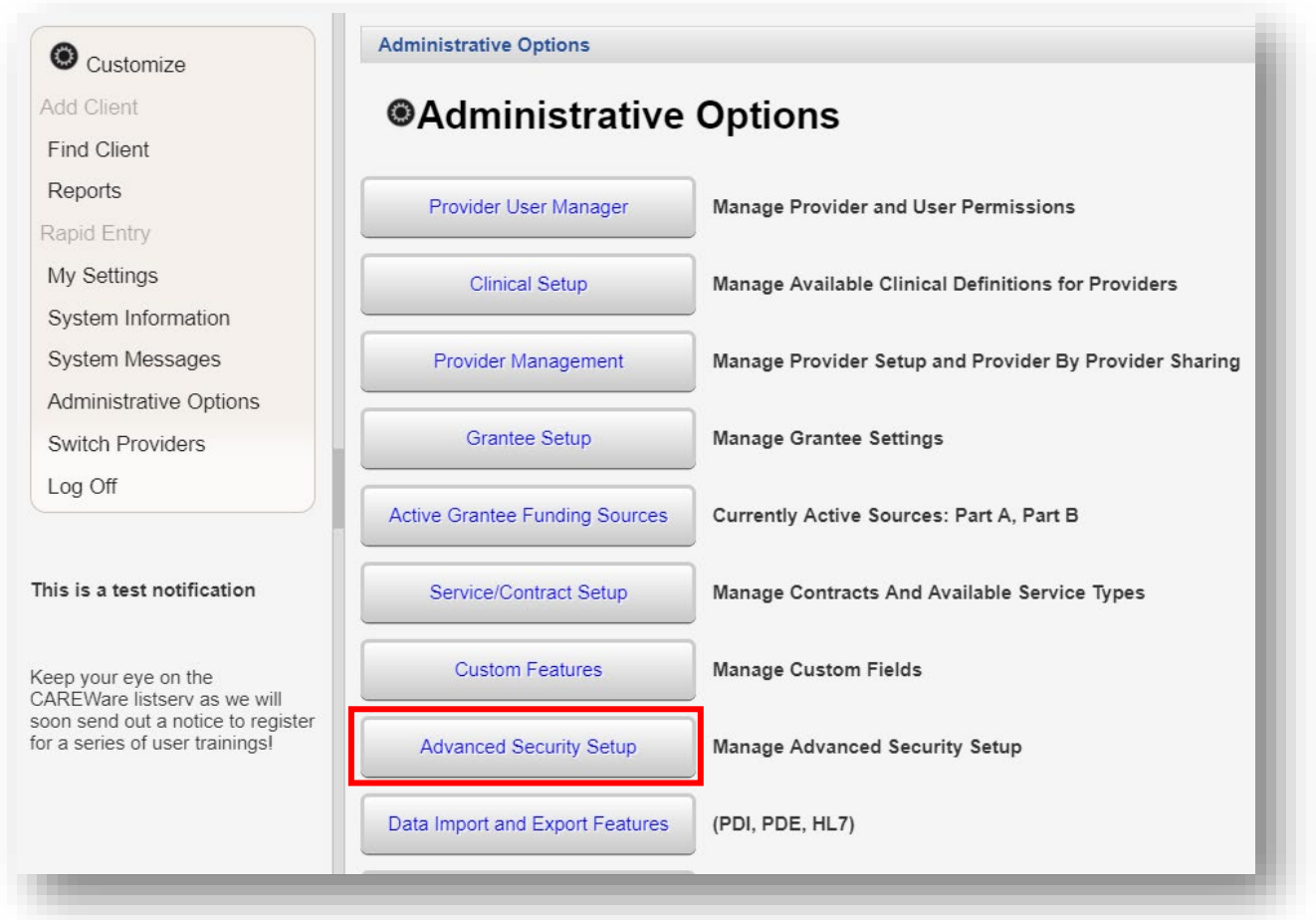
This feature allows administrators to restrict users’ access to Personal Identifying Information (PII) that is available in most CAREWare built-in reports on a field-by-field basis. With sufficient permissions, a user may select the **Hide Personally Identifying Information** box to conceal certain field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

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

Name:	URN:	eURN:	Last Service Date:	Provider:
*	*	+fAOgPpbm		
*	*	+fjZ4UmQF	1/12/2009 12:00:00 AM	Ryan White AIDS ...
*	*	+jFNvVlsw		

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.



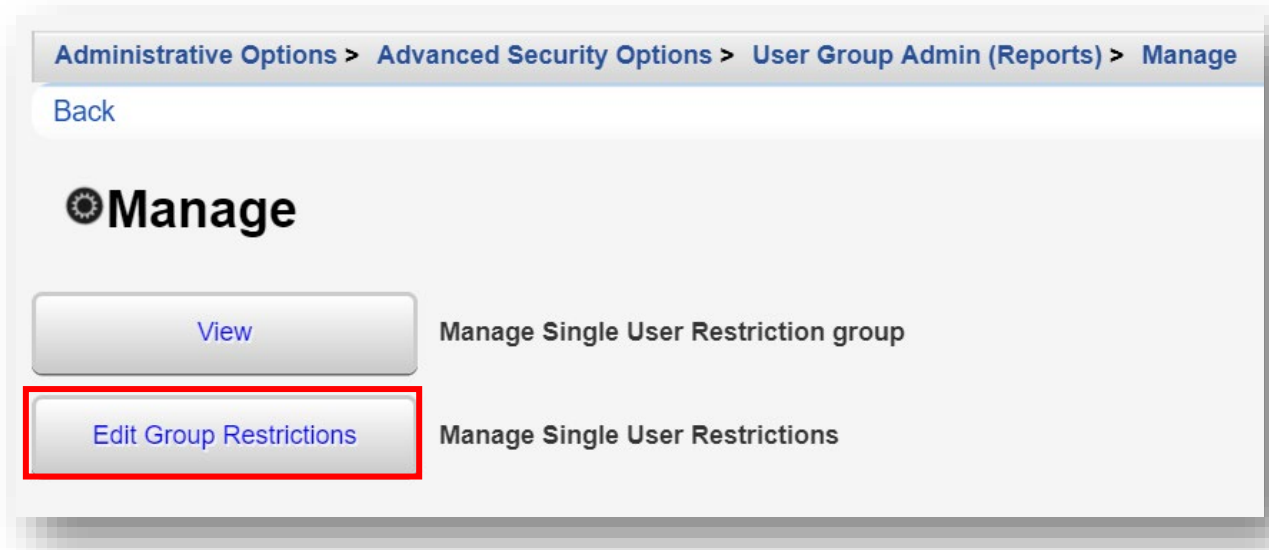
2. Select the **User Group Admin (Reports)** link.



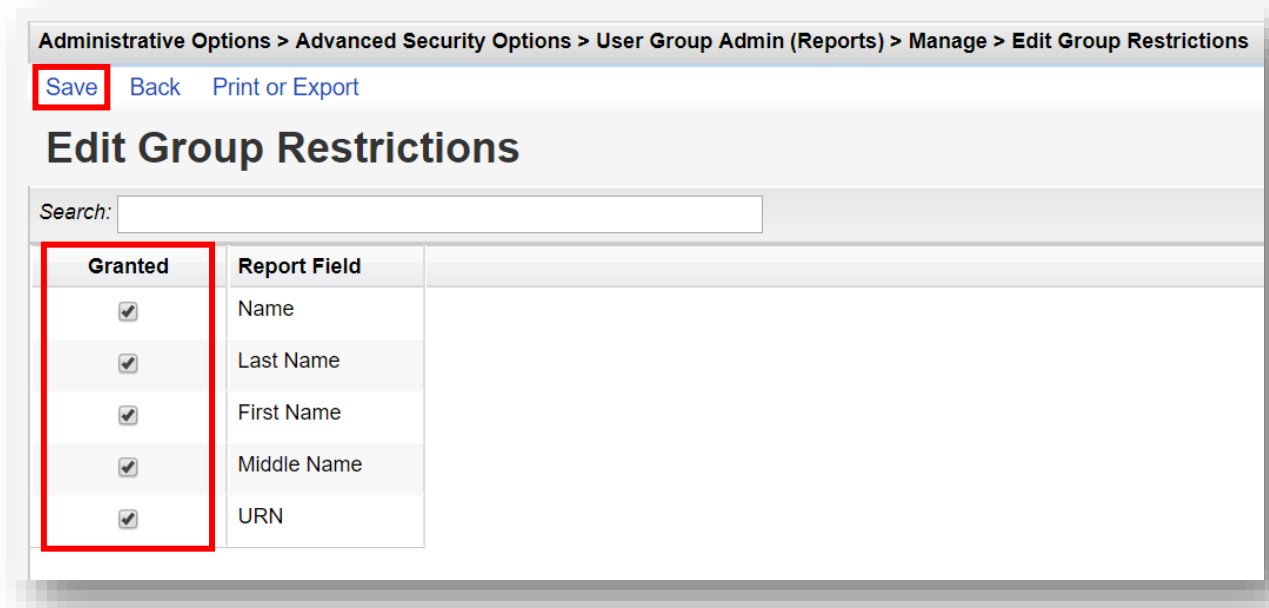
3. Select the PII Restricted Group from the User Group column. Note the number five (5) under the Restrictions column. Click **Manage** from the action bar.



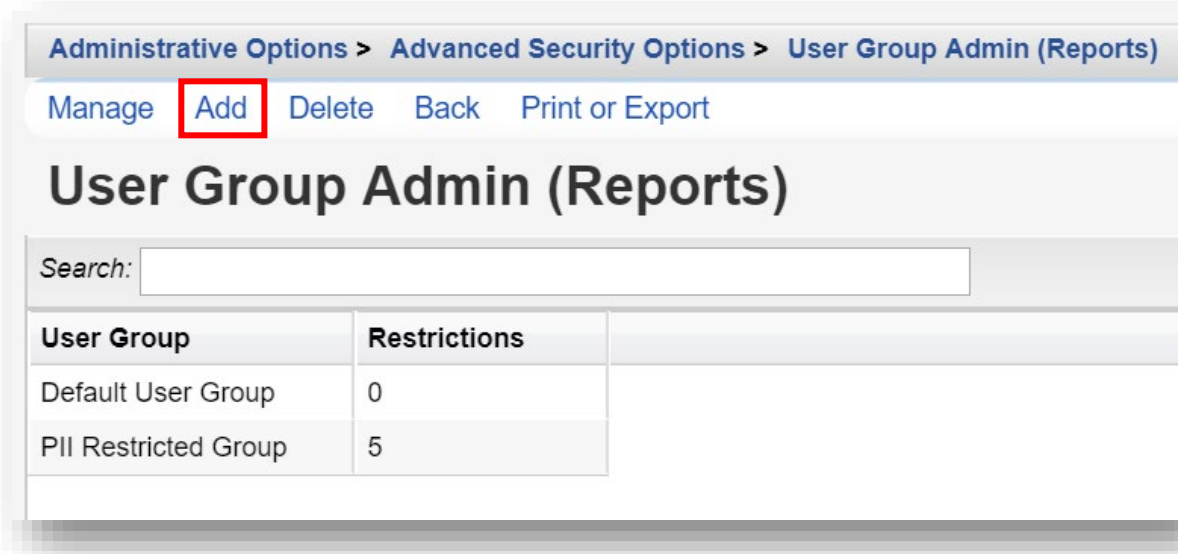
- On the Manage menu, select **Edit Group Restrictions**.



- 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**.



- 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.



Administrative Options > Advanced Security Options > User Group Admin (Reports)

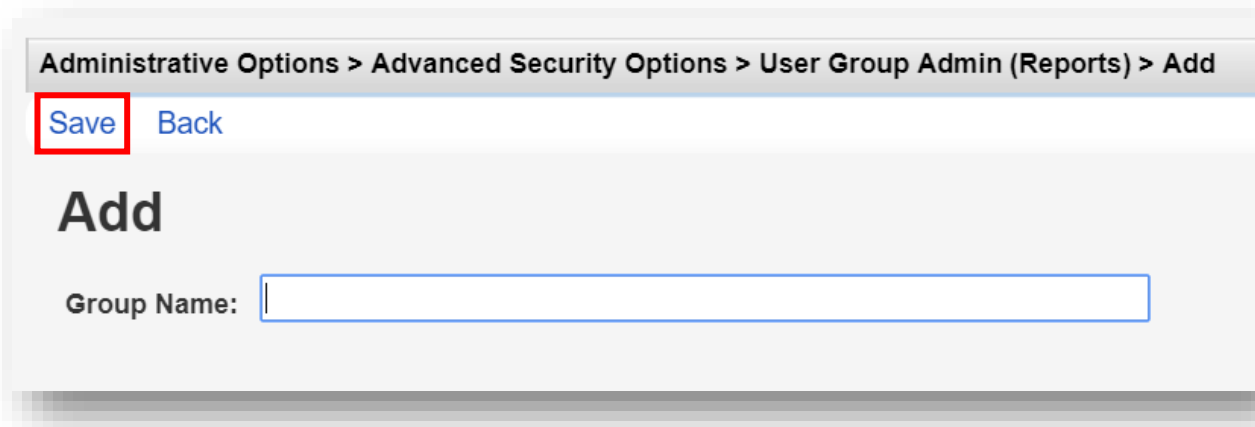
Manage **Add** Delete Back Print or Export

User Group Admin (Reports)

Search:

User Group	Restrictions
Default User Group	0
PII Restricted Group	5

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



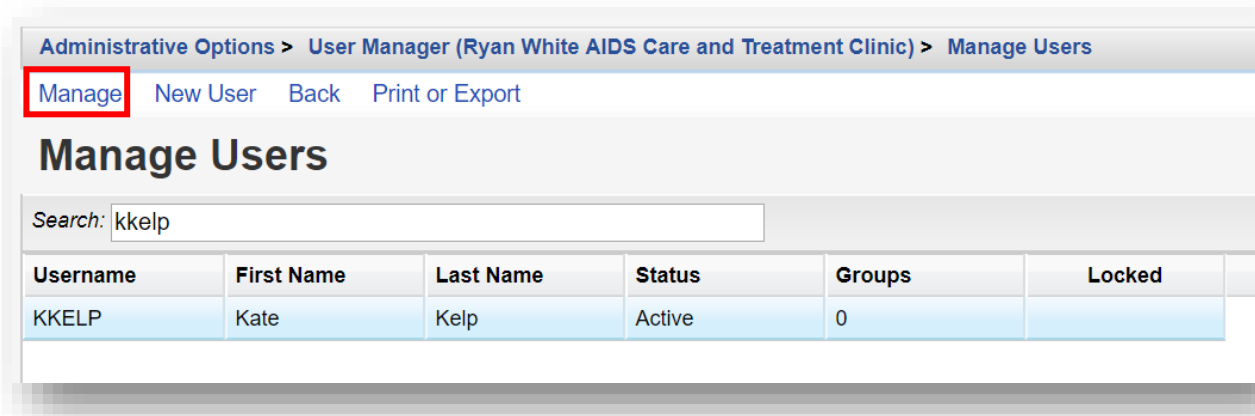
Administrative Options > Advanced Security Options > User Group Admin (Reports) > Add

Save Back

Add

Group Name:

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



Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Manage Users

Manage New User Back Print or Export

Manage Users

Search: kkelp

Username	First Name	Last Name	Status	Groups	Locked
KKELP	Kate	Kelp	Active	0	

9. Select Manage Report Field Restrictions.

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Manage Users > KKELP

Back

User Info Kate Kelp (KKELP)

Manage Permissions 0 / 350 permissions granted

Change Password User password last updated on 4/22/2019 1:06 PM

Manage Report Field Restrictions Custom report field restrictions in effect: 0. Custom report restriction groups in effect: 0

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

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Manage Users > KKELP > Report Field Restrictions for User: KKELP

Manage Restrictions Back Print or Export

Report Field Restrictions for User: KKELP

Search:

Report Field Restrictions

11. Select the desired Group name by placing a check in the Granted column. Click **Save**.

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Manage Users > KKELP > Report Field Restrictions for User: KKELP > Manage Restrictions

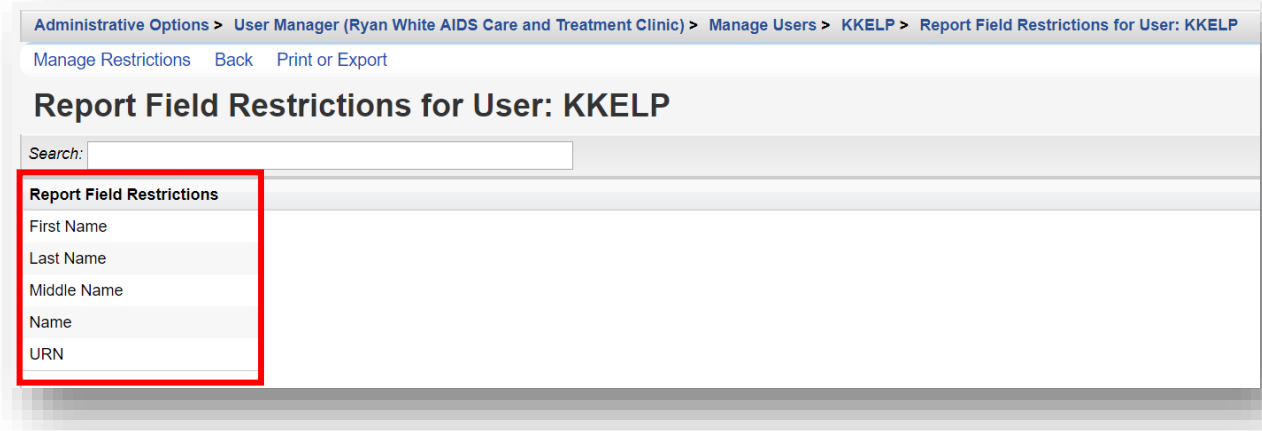
Save Back Print or Export

Manage Restrictions

Search:

Granted	Group Name
<input type="checkbox"/>	Default User Group
<input checked="" type="checkbox"/>	PII Restricted Group

12. The Report Field Restrictions are now displayed for the selected user.

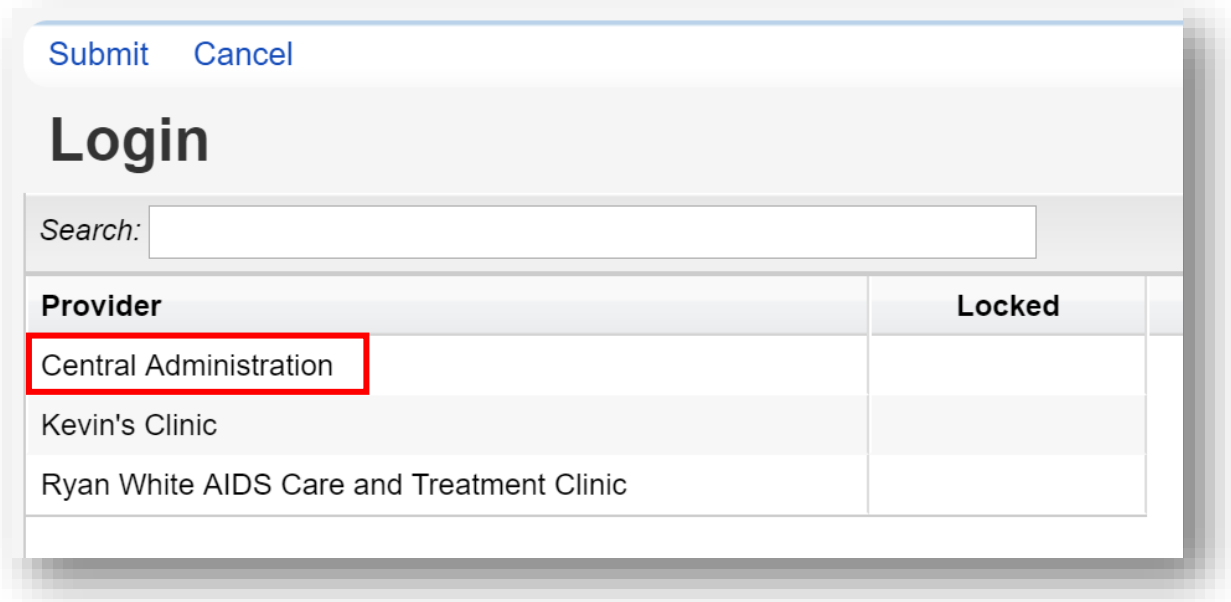


Configuring Provider Permissions

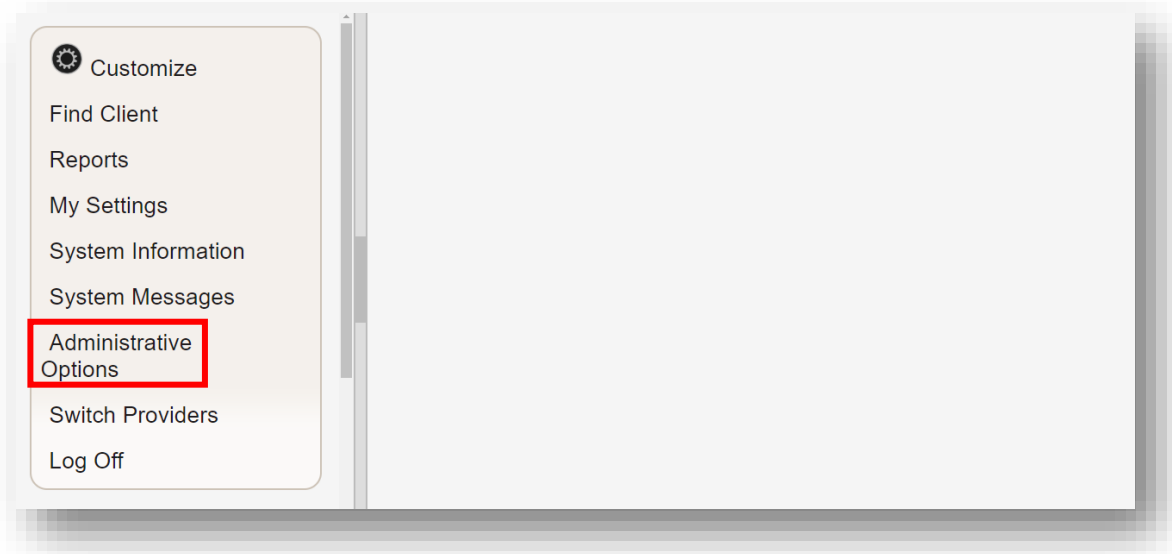
Once you've set up your Central Administration user, it's time to set up your provider permissions. These will restrict the permissions available to users within the provider domain. For instance, as the central administrator, you may want to control whether or not providers can make changes to contracts.

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.



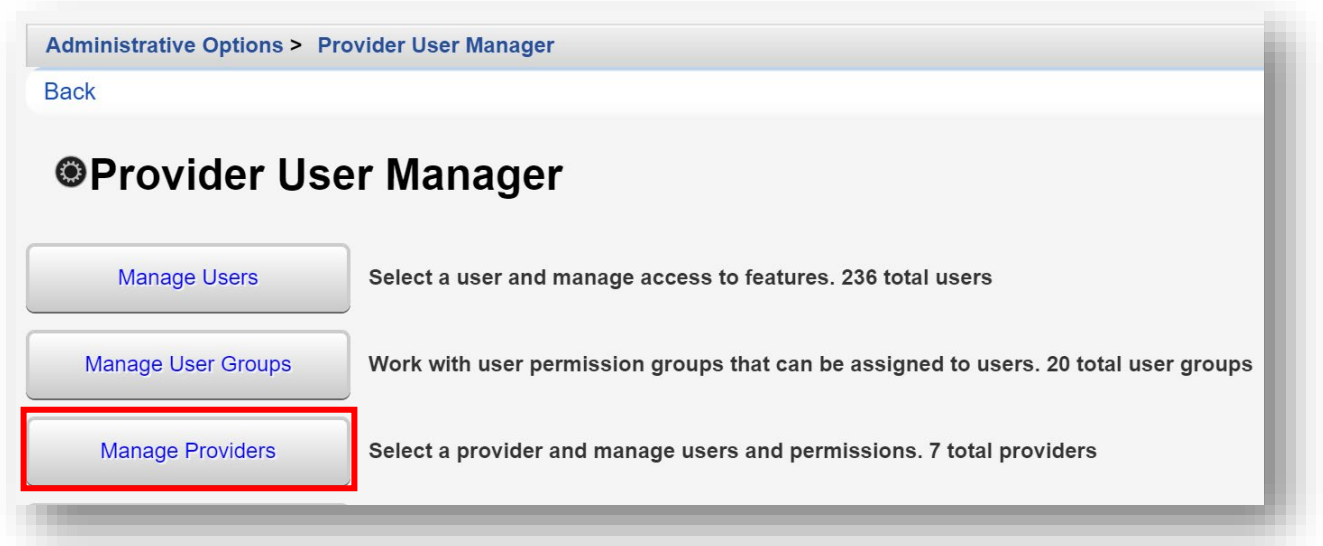
2. Select **Administrative Options** from the **Main Menu**.



3. Select **Provider User Manager** from the links menu.



- From the Provider User Manager menu, select **Manage Providers** from the links menu.



- Select the relevant provider and click **Manage** from the action bar.



6. Select **Manage Permissions** from the link menu.

Administrative Options > Provider User Manager > Manage Providers > Ryan White AIDS Care and Treatment Clinic

Back

Ryan White AIDS Care and Treatment Clinic

- [Manage Users](#) Select a user and manage access to features within the provider. 32 total users
- [Manage User Groups](#) Work with user permission groups that can be assigned to users. 14 total user groups
- [Manage Permissions](#)** 332 / 350 permissions granted
- [Deactivate Provider](#) Provider currently active
- [Change Cross-Provider Report Fields](#) 214 / 281 permissions granted

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.

Administrative Options > Provider User Manager > Manage Providers > Ryan White AIDS Care and Treatment Clinic > Permissions for Provider: Ryan White AIDS Care and Treatment Clinic

Assign Provider Groups Grant Individual Permission **Revoke Individual Permission** Back Print or Export

Permissions for Provider: Ryan White AIDS Care and Treatment Clinic

Search:

Final Permission Status	Permission	Granted Individually	Granted via Group	Permission Category
Granted	Delete Drug Service Records	Yes	No	ADAP
Granted	Edit formulary/drug list	Yes	No	ADAP
Granted	View Drug Service Records	Yes	No	ADAP
Granted	Add/Edit Drug Service Records	Yes	No	ADAP
Granted	ADAP Drug Services Import	Yes	No	ADAP

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.

Administrative Options > User Manager (Ryan White AIDS Care and Treatment Clinic) > Manage Users > KKELP > Permissions for User: KKELP

Assign User Groups Grant Individual Permission Revoke Individual Permission Back Print or Export

Permissions for User: KKELP

Search: ADAP drug

Permission	Final Permission Status	Granted via Groups	Granted Individually	Permission Category
Delete Drug Service Records	Denied	No (Locked for Provider)	No	ADAP
Edit formulary/drug list	Denied	No (Locked for Provider)	No	ADAP
View Drug Service Records	Denied	No (Locked for Provider)	No	ADAP
Add/Edit Drug Service Records	Denied	No (Locked for Provider)	No	ADAP
ADAP Drug Services Import	Denied	No (Locked for Provider)	No	ADAP

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.

Administrative Options > Provider User Manager > Manage Providers

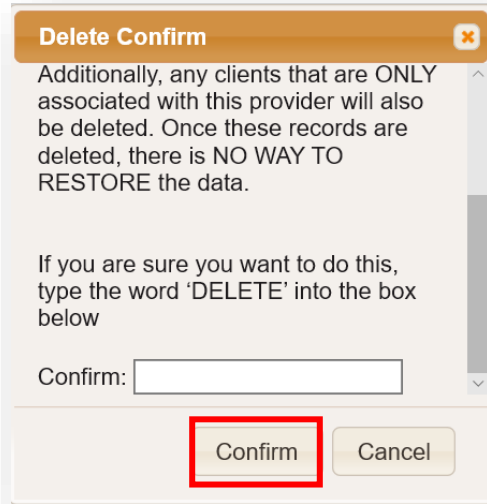
Manage Add Provider **Delete** Back Print or Export

Manage Providers

Search: Ryan White

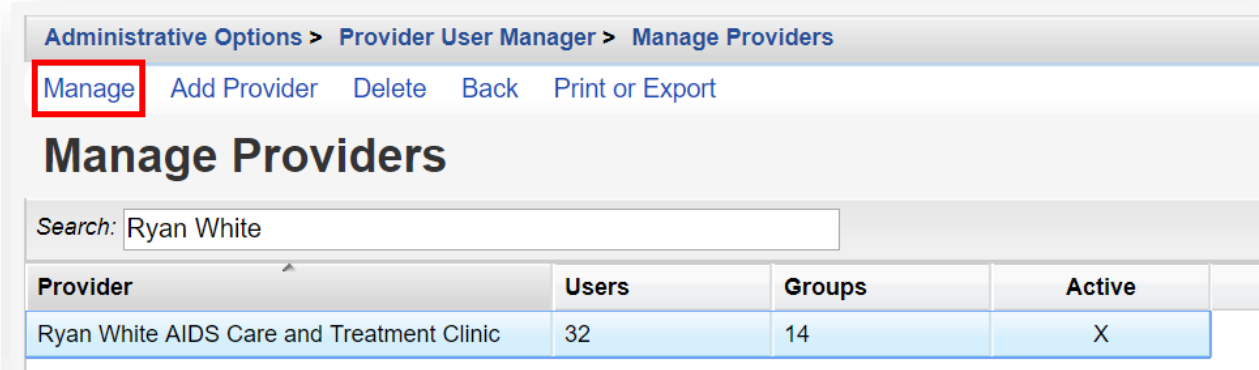
Provider	Users	Groups	Active
Ryan White AIDS Care and Treatment Clinic	32	14	X

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.

The screenshot shows the administrative interface for the 'Ryan White AIDS Care and Treatment Clinic'. The breadcrumb trail is 'Administrative Options > Provider User Manager > Manage Providers > Ryan White AIDS Care and Treatment Clinic'. Below the breadcrumb is a 'Back' link. The main heading is 'Ryan White AIDS Care and Treatment Clinic'. There are five buttons with corresponding descriptions:

Button Label	Description
Manage Users	Select a user and manage access to features within the provider. 32 total users
Manage User Groups	Work with user permission groups that can be assigned to users. 14 total user groups
Manage Permissions	332 / 350 permissions granted
Deactivate Provider	Provider currently active
Change Cross-Provider Report Fields	214 / 281 permissions granted

The 'Deactivate Provider' button is highlighted with a red border.

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

The screenshot shows the administrative interface for the 'Ryan White AIDS Care and Treatment Clinic' after the provider has been deactivated. The breadcrumb trail is 'Administrative Options > Provider User Manager > Manage Providers > Ryan White AIDS Care and Treatment Clinic'. Below the breadcrumb is a 'Back' link. The main heading is 'Ryan White AIDS Care and Treatment Clinic'. There are five buttons with corresponding descriptions:

Button Label	Description
Manage Users	Select a user and manage access to features within the provider. 32 total users
Manage User Groups	Work with user permission groups that can be assigned to users. 14 total user groups
Manage Permissions	332 / 350 permissions granted
Reactive Provider	Provider currently inactive
Change Cross-Provider Report Fields	214 / 281 permissions granted

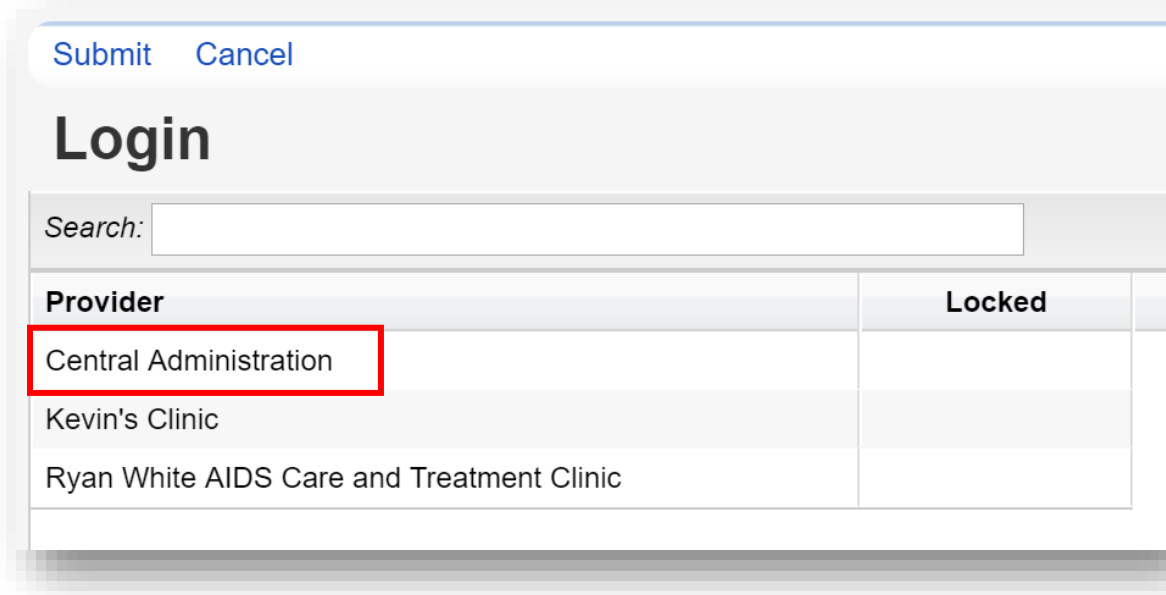
The 'Reactive Provider' button is highlighted with a red border.

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.

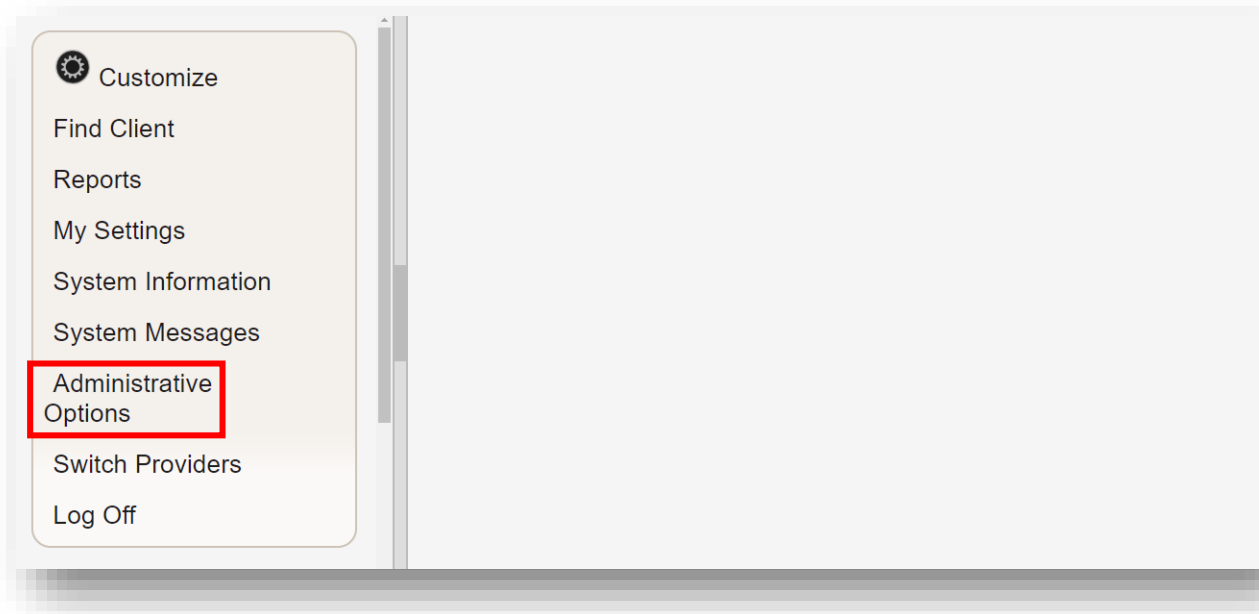
From Central Administration, you can set up all providers.

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



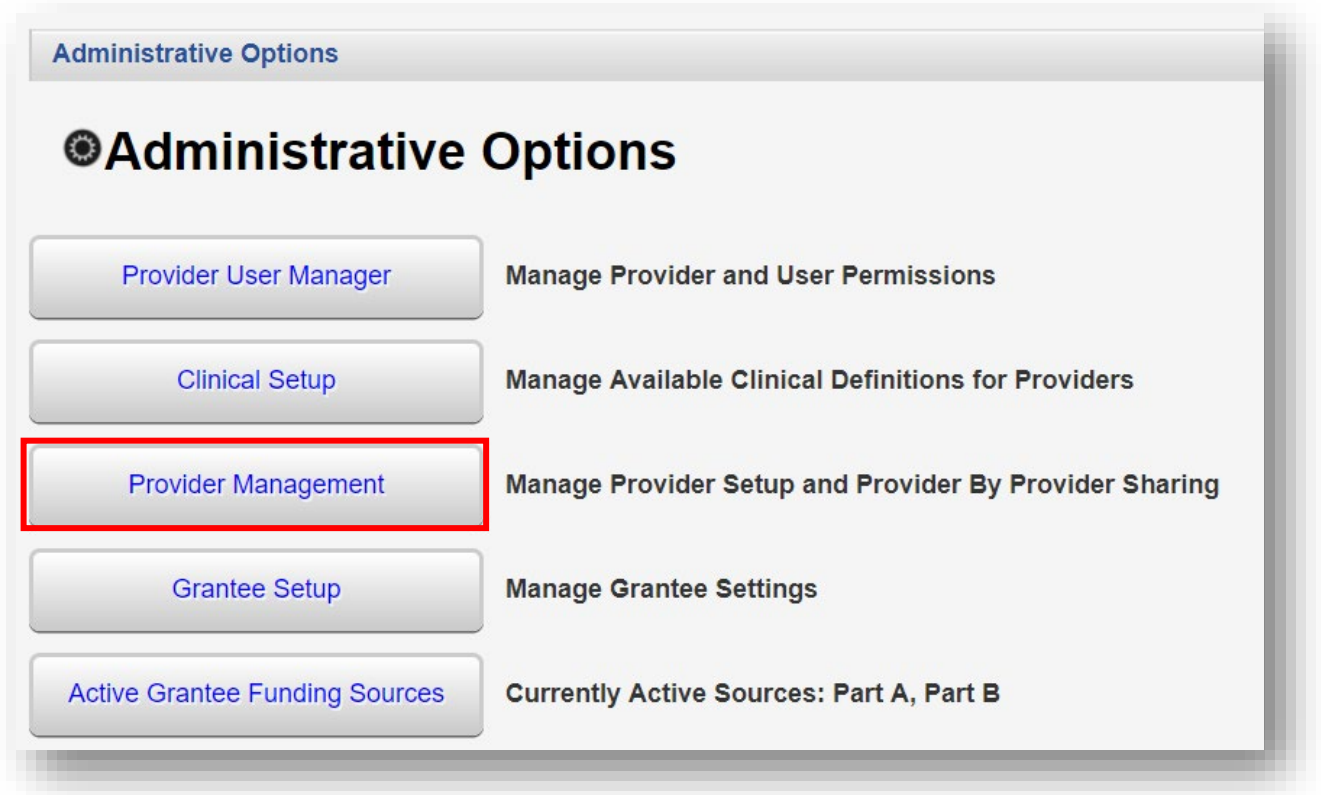
Provider	Locked
Central Administration	
Kevin's Clinic	
Ryan White AIDS Care and Treatment Clinic	

2. Select **Administrative Options** from the **Main Menu**.



- Customize
- Find Client
- Reports
- My Settings
- System Information
- System Messages
- Administrative Options
- Switch Providers
- Log Off

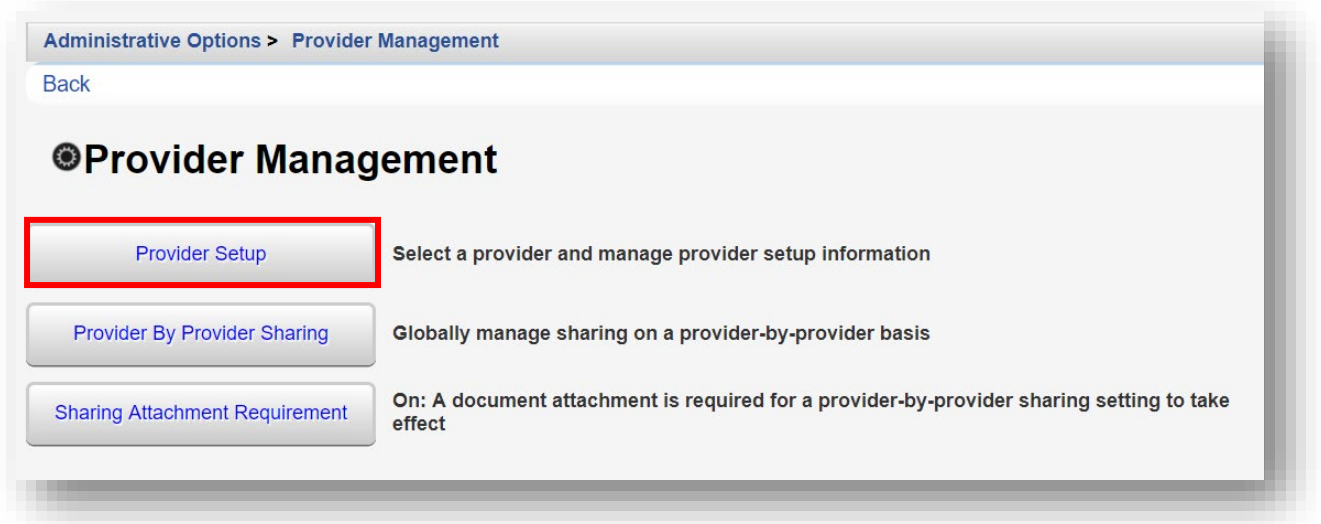
- 3. Select **Provider Management** from the links menu.



The screenshot shows a web interface titled "Administrative Options". At the top, there is a sub-header "Administrative Options" in blue. Below it is a large heading "Administrative Options" with a gear icon. A list of five menu items is displayed, each with a button and a description. The "Provider Management" button is highlighted with a red rectangular border. The items are:

- Provider User Manager**: Manage Provider and User Permissions
- Clinical Setup**: Manage Available Clinical Definitions for Providers
- Provider Management**: Manage Provider Setup and Provider By Provider Sharing
- Grantee Setup**: Manage Grantee Settings
- Active Grantee Funding Sources**: Currently Active Sources: Part A, Part B

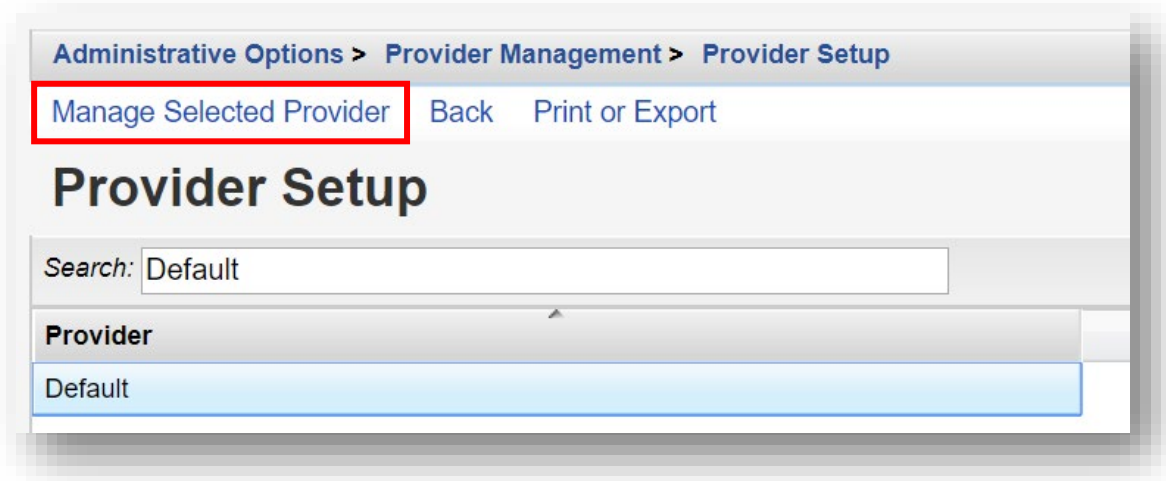
- 4. Select **Provider Setup**.



The screenshot shows the "Provider Management" page. At the top, there is a breadcrumb trail "Administrative Options > Provider Management" and a "Back" link. Below is a large heading "Provider Management" with a gear icon. A list of three menu items is displayed, each with a button and a description. The "Provider Setup" button is highlighted with a red rectangular border. The items are:

- Provider Setup**: Select a provider and manage provider setup information
- Provider By Provider Sharing**: Globally manage sharing on a provider-by-provider basis
- Sharing Attachment Requirement**: On: A document attachment is required for a provider-by-provider sharing setting to take effect

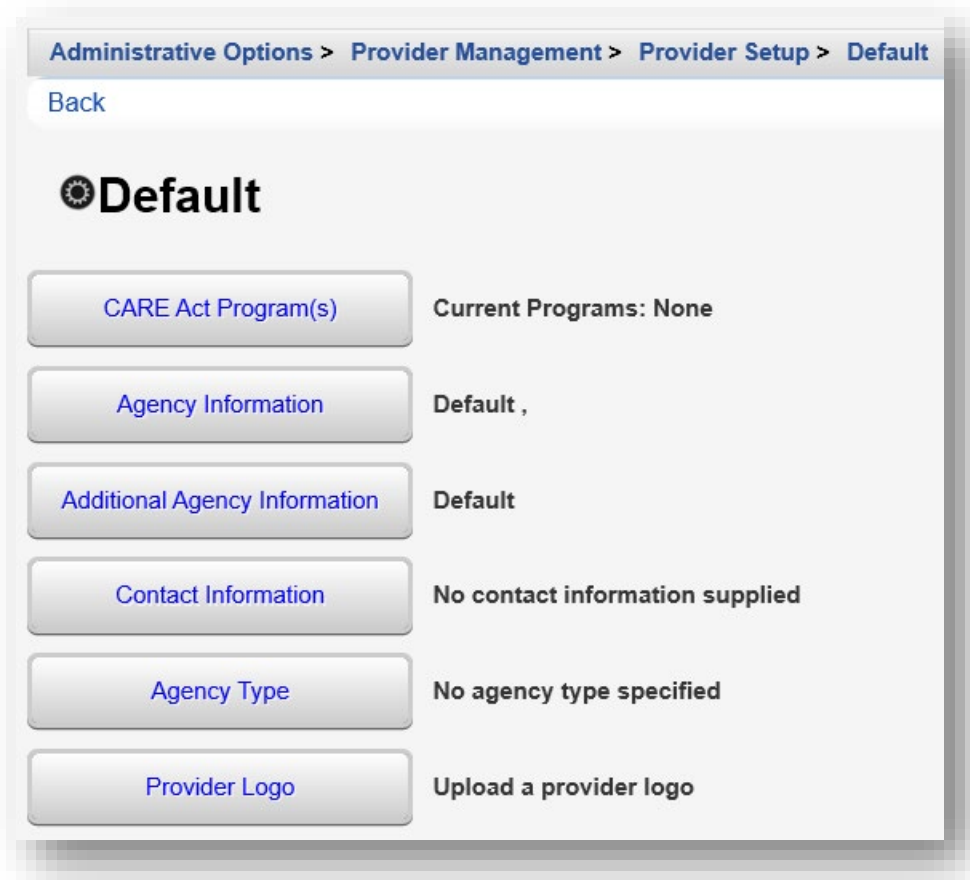
5. Select “Default” provider, then click **Manage Selected Provider** from the action bar.



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**.

Administrative Options > Provider Management > Provider Setup > Default > CARE Act Program(s) > Edit

[Save](#) [Cancel](#)

CARE Act Program(s)

Part A:

Part B:

Part C:

Part D:

HIP:

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**.

Administrative Options > Provider Management > Provider Setup > Default > Agency Information > Edit

[Save](#) [Cancel](#)

Agency Information

Name:

Street Address:

City:

State:

County:

Area:

Zip:

- 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**.

Administrative Options > Provider Management > Provider Setup > Default > Additional Agency Information > Edit

[Save](#) [Cancel](#)

Additional Agency Information

Part A ID:

Part B ID:


Taxpayer ID:


Part A Grantee ID:


Part B Grantee ID:


Part C Grantee ID:


Part D Grantee ID:

Receives 330 Funding: 


Receives MAI Funding: 

Agency Type: 

Reporting Scope: 

Provider Type: 

Other Provider Type:

Ownership Status: 

 **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**.

Administrative Options > Provider Management > Provider Setup > Default > Contact Information > Edit

[Save](#) [Cancel](#)

Contact Information

Contact Name:

Title:

Phone:

Fax:

Email:

11. Select **Agency Type**. Enter all that apply for your agency. Click **Save**.

Administrative Options > Provider Management > Provider Setup > Default > Agency Type > Edit

[Save](#) [Cancel](#)

Agency Type

An agency in which racial/ethnic minority group members make up greater than 50% of the agency's board members.:

Racial/ethnic minority group members make up greater than 50% of the agency's professional staff members in HIV direct services.:

Solo or group private health care practice in which greater than 50% of the clinicians are racial/ethnic minority group members.:

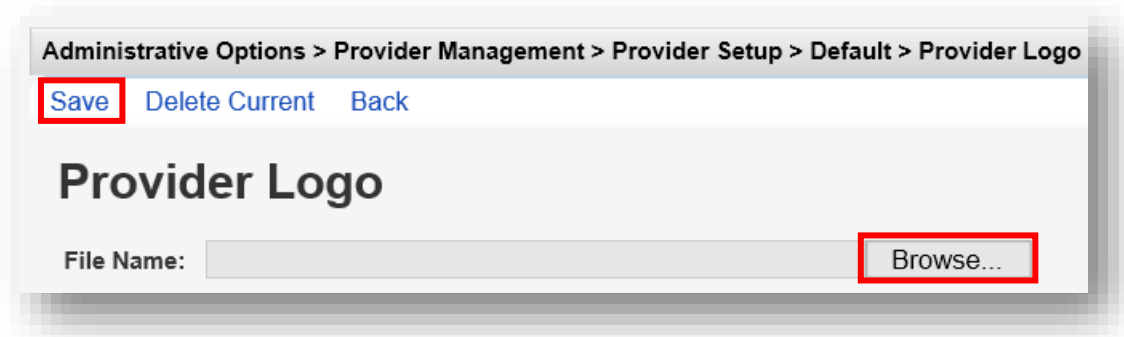
Other "traditional" provider that has historically served racial/ethnic minority patients/clients but does not meet the criteria above.:

Other type of agency or facility:

Total Paid HIV Staff in FTE's:

Total Volunteer HIV Staff in FTE's:

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.

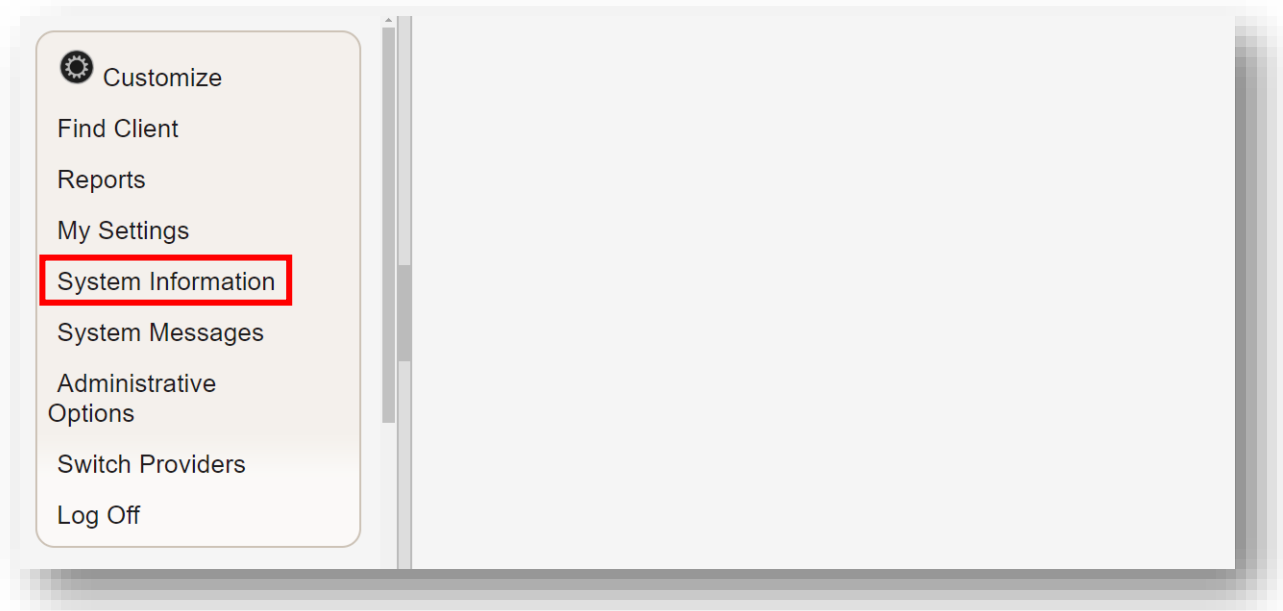


System Information and Messages

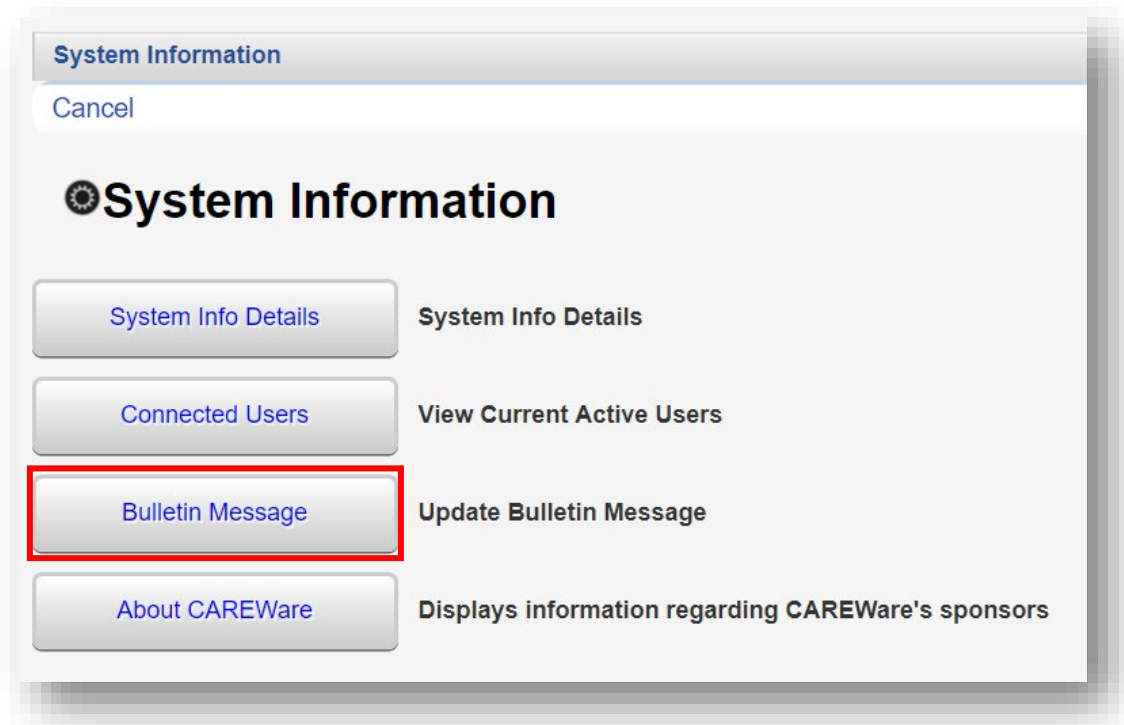
System Information

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**.



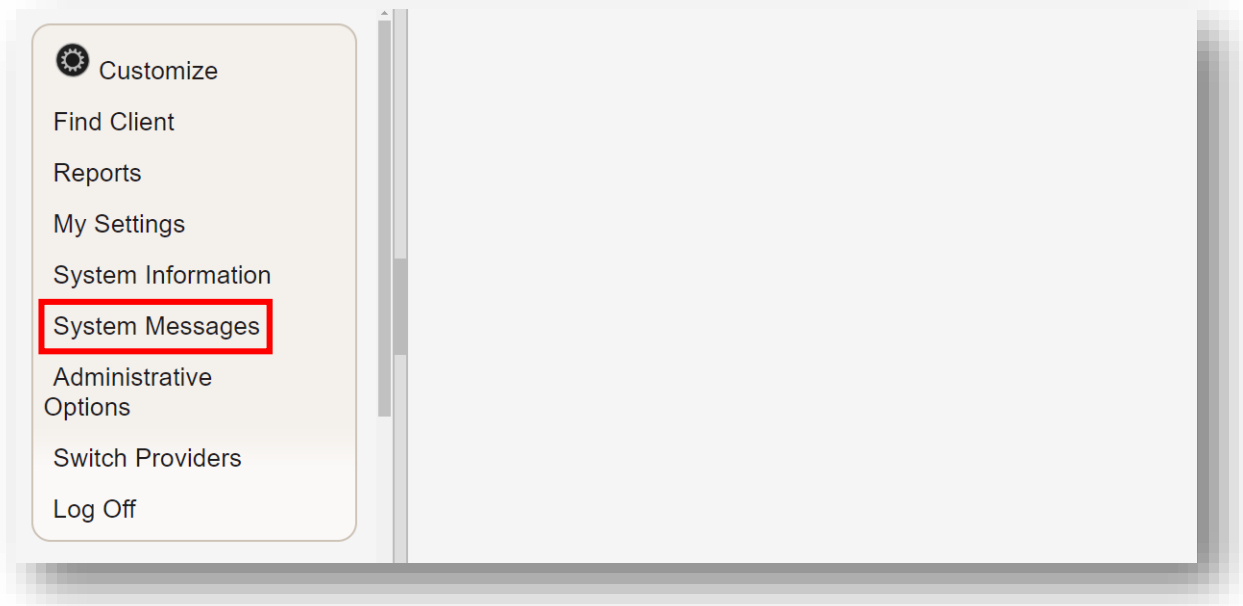
3. Here, you can publish a “bulletin message” that will appear on all users’ screens. Enter a message into the text box and click **Save**.



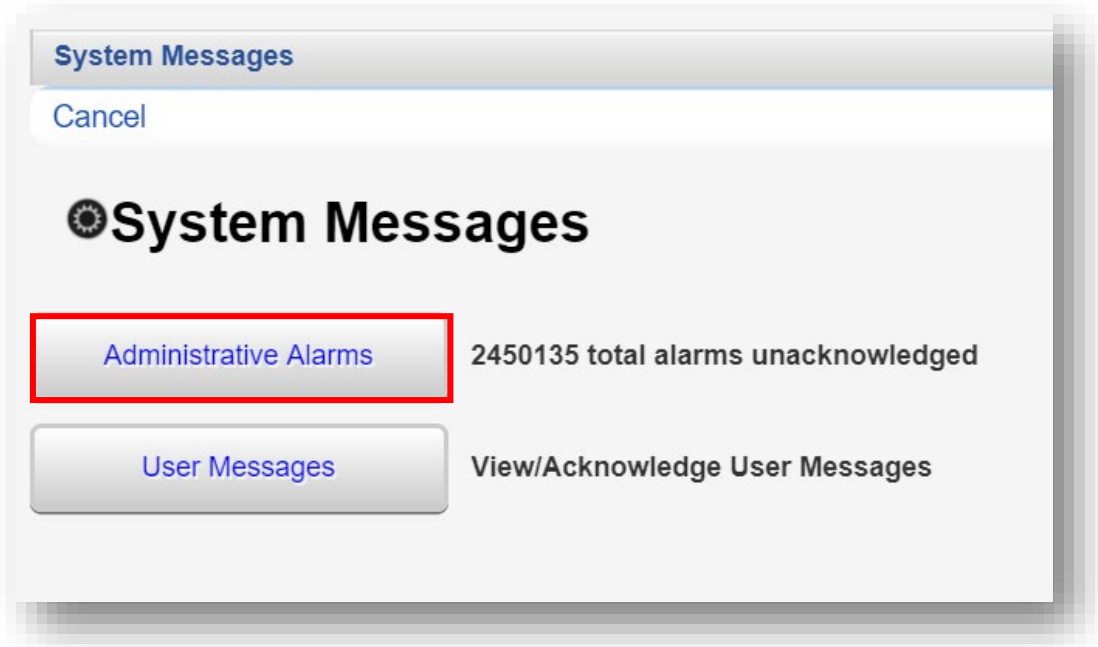
System Messages

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

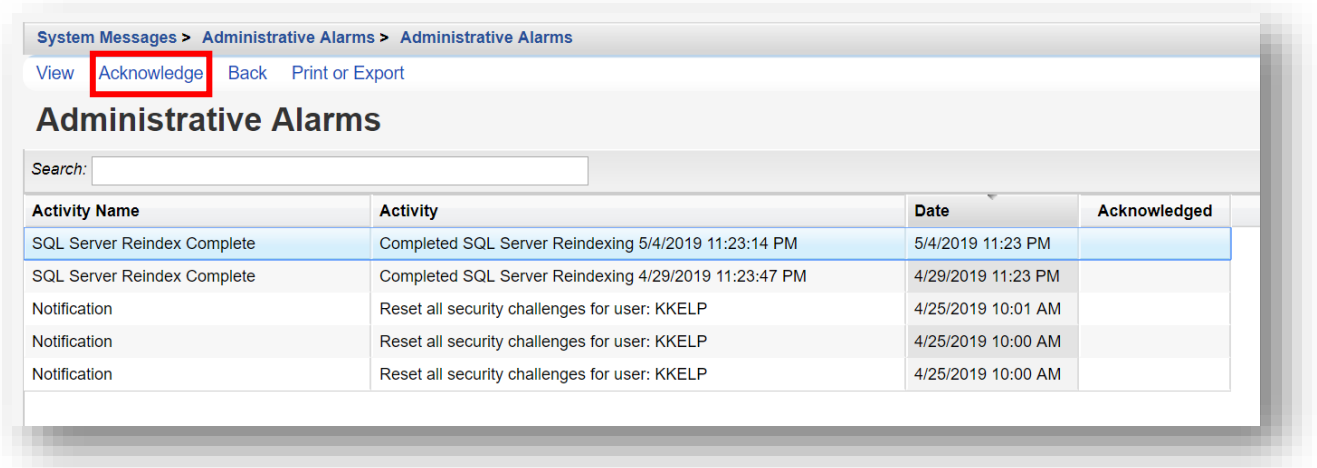
1. Select **System Messages** from the **Main Menu**.



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.



System Messages > Administrative Alarms > Administrative Alarms

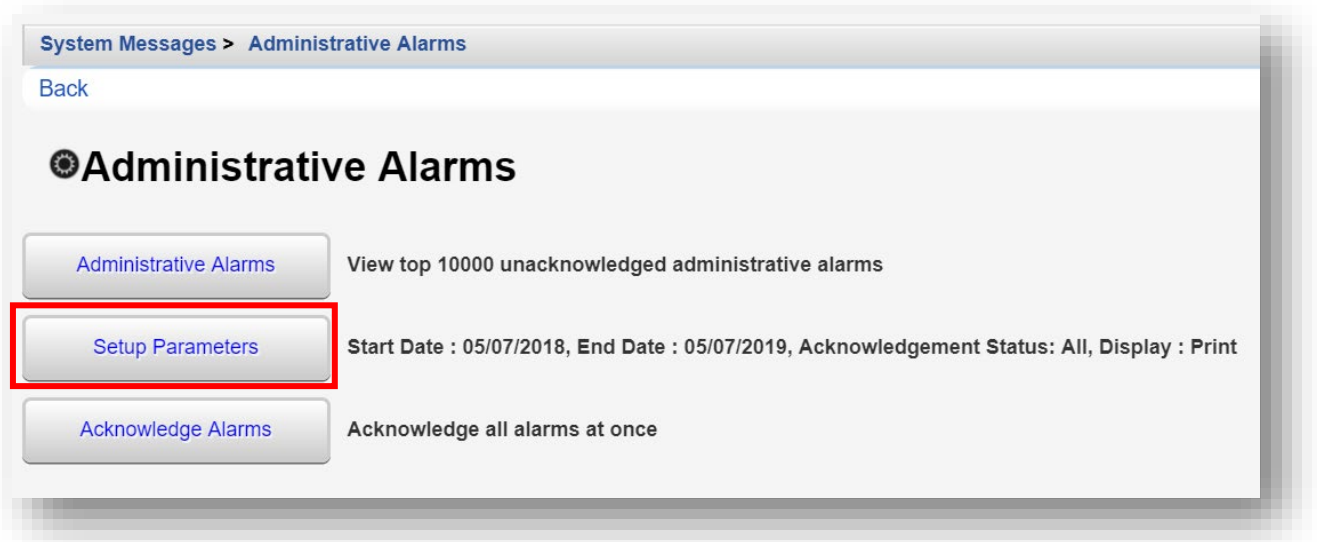
View **Acknowledge** Back Print or Export

Administrative Alarms

Search:

Activity Name	Activity	Date	Acknowledged
SQL Server Reindex Complete	Completed SQL Server Reindexing 5/4/2019 11:23:14 PM	5/4/2019 11:23 PM	
SQL Server Reindex Complete	Completed SQL Server Reindexing 4/29/2019 11:23:47 PM	4/29/2019 11:23 PM	
Notification	Reset all security challenges for user: KKELP	4/25/2019 10:01 AM	
Notification	Reset all security challenges for user: KKELP	4/25/2019 10:00 AM	
Notification	Reset all security challenges for user: KKELP	4/25/2019 10:00 AM	

4. Administrative alarms can also be sorted and printed like other reports in CAREWare. Select **Setup Parameters** from the **Administrative Alarms** link menu.



System Messages > Administrative Alarms

Back

⚙️ Administrative Alarms

[Administrative Alarms](#) View top 10000 unacknowledged administrative alarms

[Setup Parameters](#) Start Date : 05/07/2018, End Date : 05/07/2019, Acknowledgement Status: All, Display : Print

[Acknowledge Alarms](#) Acknowledge all alarms at once

- 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**.

System Messages > Administrative Alarms > Admin Alarm Settings

[Edit](#) [Run Report](#) [Back](#)

Admin Alarm Settings

Parameters

Date From: 5/7/2018

Date Through: 5/7/2019

Acknowledgement Status: All

Output Display: Open in New Window

- 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.)

System Messages > Administrative Alarms

[Back](#)

Administrative Alarms

[Administrative Alarms](#) View top 10000 unacknowledged administrative alarms

[Setup Parameters](#) Start Date : 05/07/2018, End Date : 05/07/2019, Acknowledgement Status: All, Display : Print

[Acknowledge Alarms](#) Acknowledge all alarms at once