CAREWare 5

Build 580

New Features User Guide

October 2011

Table of Contents

Security Questions 3
Unlock Users at the Provider Level 9
Restriction of PII in Custom and Canned Reports 13
Global User Account 20
Copying Custom Reports 23

Security Questions

The purpose of the (optional) Security Questions feature is to add another layer of security to the CAREWare system, beyond the standard combination of a user name and password. 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 the login will be complete and access to CAREWare data is returned. If the user fails to answer the questions correctly, the account will be locked again.

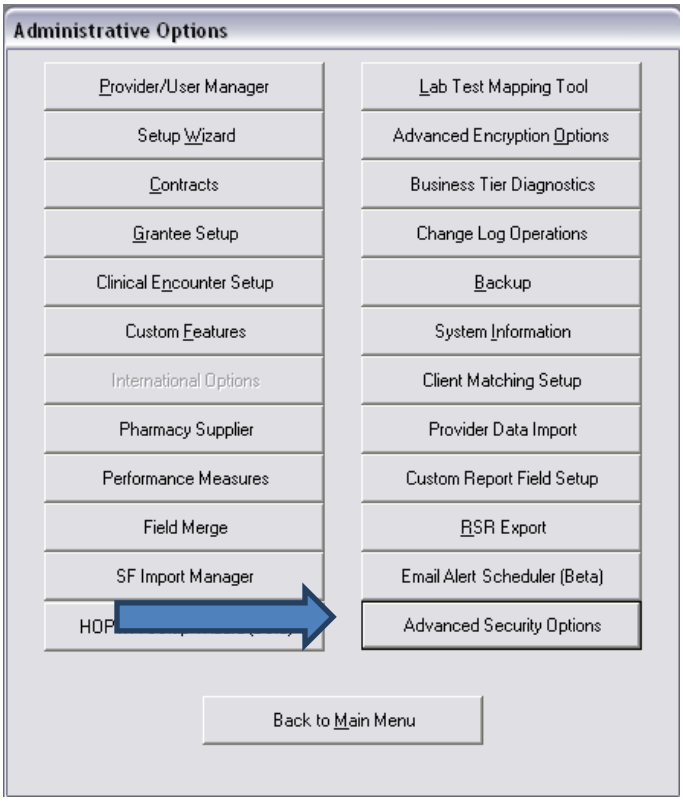
The Central Administrator is responsible for setting up the pool of questions that users can choose from, and also for setting the number of questions that must be answered correctly before login after a password reset is completed. The Central Administrator also sets the maximum number of attempts a user gets to answer a question correctly (1 or more). Central administrators will also have the ability to completely reset a user account in the event that the password is reset and security questions cannot be answered correctly.

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.

Setting up the Security Questions (Central Administrator)

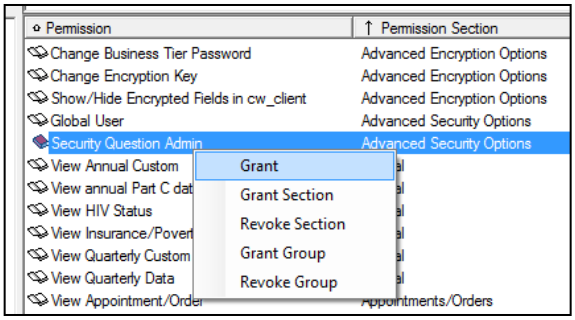
When logged in to the Central Administration domain, there is a new button on the Administrative Options menu, called Advanced Security Options.

If the button is not active, the Central Administration user may need to add the permission to his/her Central Administration account using the Provider/User Manager.



The Security Question Administration permission is found in the Advanced Security Options section of the Administration Permission Group. There are two components of the Advanced Security Section, Global User and Security Question Admin. Right click on Security Question Admin and choose Grant to activate this feature. (The Global User feature will be discussed in another section of this guide).

When done granting permissions, click on the F1-Save button and Close to return to the Administrative Options menu where the Advanced Security Options button should now be activated.

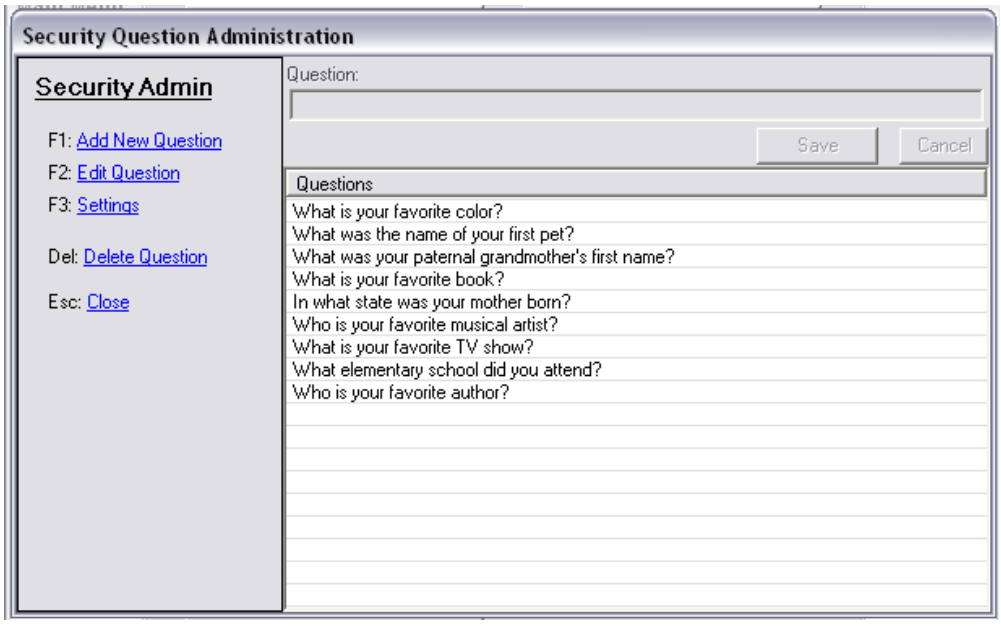


Click on the Advanced Security Options button and a new screen will appear with two options available, Security Questions Admin and User Group Admin (Reports). (The User Group Admin feature is described in another section of this guide).

Choose the Security Questions Admin button to open the screen that is used to setup the pool of questions that will be used for this feature.

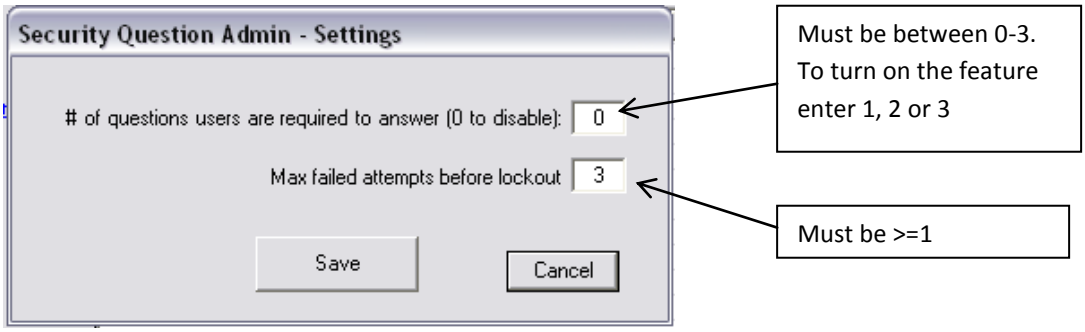
To add a list of questions type the F1 key or click on the Add New Question link, then type in the question in the box that opens at the top of the screen.

Click on Save to save the question and add it to the list. Repeat the process until there is a satisfactory list of questions available for users to choose as their Security Questions. When finished with this task the screen will look something like the example below.



Now click on the Settings link, (or type the F3 key) and a new window will appear that allows the Central Administrator to set the number of Security Questions that a user will have to answer when logging in to CAREWare for the first time in the event their account has been unlocked and their password reset. This

is also where the Central Administrator can set how many chances a user has to answer the questions correctly.



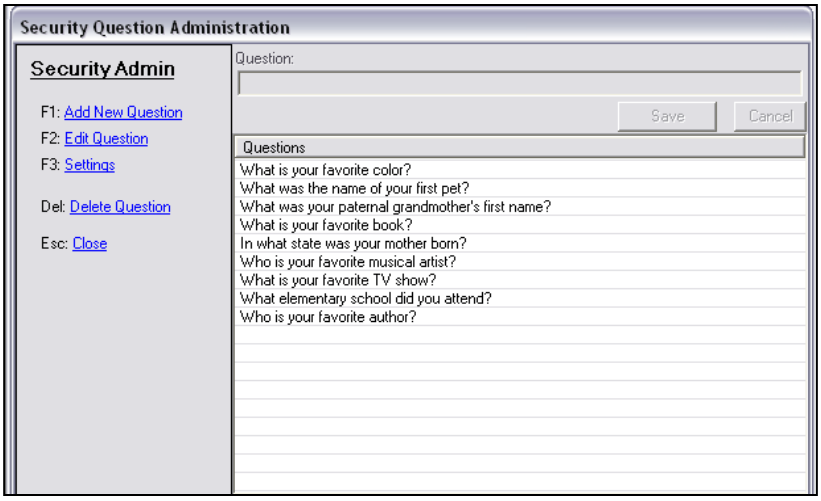
Changing the value in the first box (# of questions users are required to answer) from zero to 1, 2 or 3 turns on the Security Question feature. If the value is left at 0 (zero), even though a list of security questions has been added, the feature will not be active.

The number entered in the box determines how many questions a user will be required to answer if their password has been reset. For example, if the Central Administrator sets this number to 1, the user will just need to answer one question to complete a successful login after a password reset.

The number in the second box determines how many failed attempts to answer the security questions will be allowed. For example, if the number of questions to answer is set to two, and the number of failed attempts is set to two, the user can miss one question twice, or each question once before the account will be locked again.

When the numbers have been entered in to the Setting boxes, click Save to return to the Security Question screen.

To edit a question in the list, highlight it and click the Edit Question link or type the F2 key. The question will appear again in the Question box at the top and can be revised there. Click Save to save the edits made to the question.



To delete a question from the list, highlight it and press the Delete key or click on the Delete Question link.

If the deleted question is in use by any user as a selected security

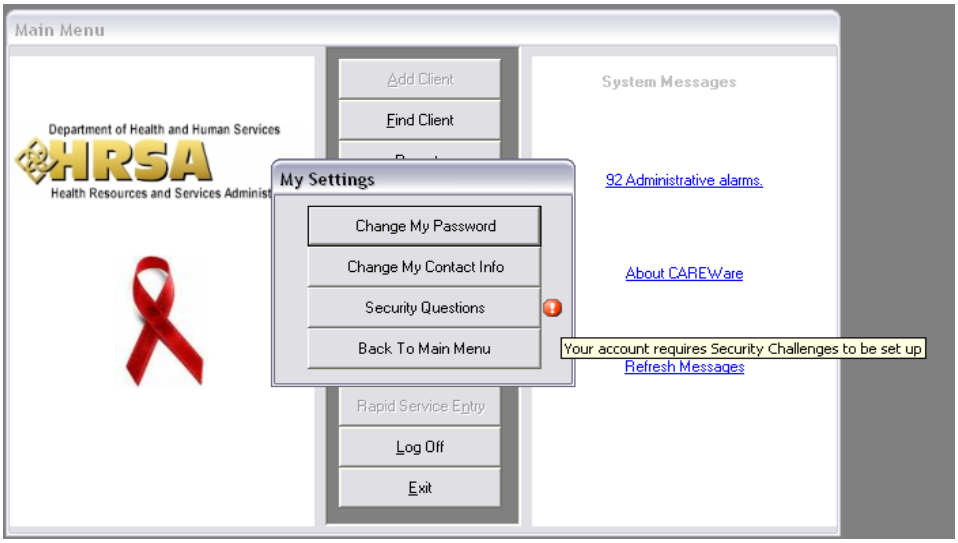
question, the user will be required to select a new security question on first login after the deletion.

When satisfied with the list of Security Questions, and after turning on the feature in the Settings screen, click the Close link to close the screen and save the questions. Click Close again on the Advanced Security Options menu to return to the Administrative Options menu and then back to the Main Menu.

Security Questions and the CAREWare User

After the Security Question feature has been activated by the Central Administrator, users will be prompted to select three Security Questions and enter answers to the selected questions. This will happen the first time a user logs in after the feature has been activated. It will also happen the first time a new user logs in to CAREWare.

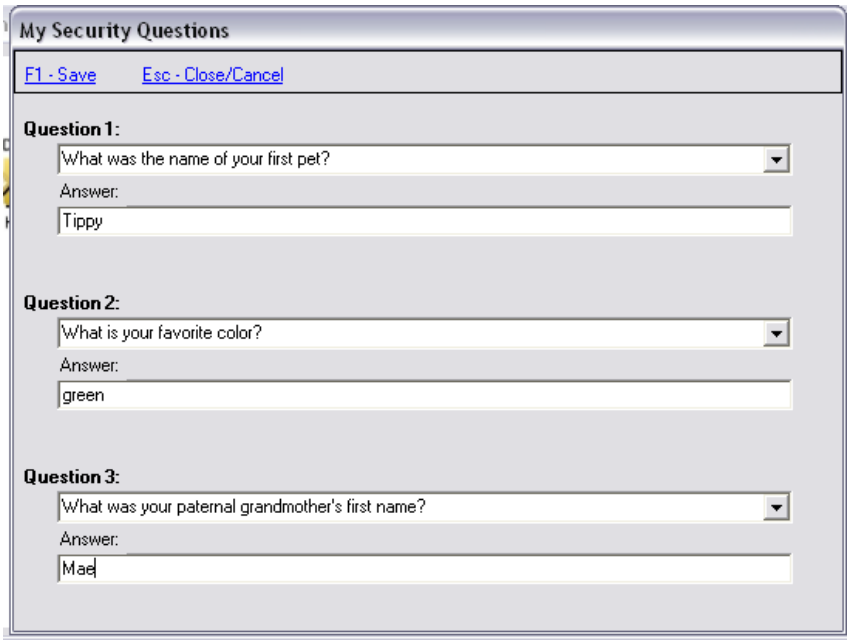
On first login after Security Questions have been activated, the user will see the Main Menu as usual, but all the buttons except My Settings, Log Off and Exit will be grayed out (inactive). There will be a warning icon next to the My Settings button. Hovering over the icon will bring up a message box that says "Your account requires security questions to be set up." Click on the My Settings button to proceed.



The My Settings menu will open. It has a new button on it labeled Security Questions. Click on the Security Questions button.

This will open the My Security Questions screen. To choose a question, open the dropdown list of the Question 1 box. Select a question by highlighting and clicking on it. Then type in an answer in the Answer box. The answer is not case sensitive and it may contain spaces or other punctuation.

Repeat these steps to choose and answer Questions 2 and 3.



Three different questions must be selected and each must have an answer.

When done, click on Save or press the F1 key.

Click on the Back to Main Menu button on the My Settings screen.

The buttons that usually are available on the Main Menu will now be active again, and the user will have access to other CAREWare features.

Users can change or review their Security Questions and answers at any time by returning to the My Security Questions screen through the My Settings menu.

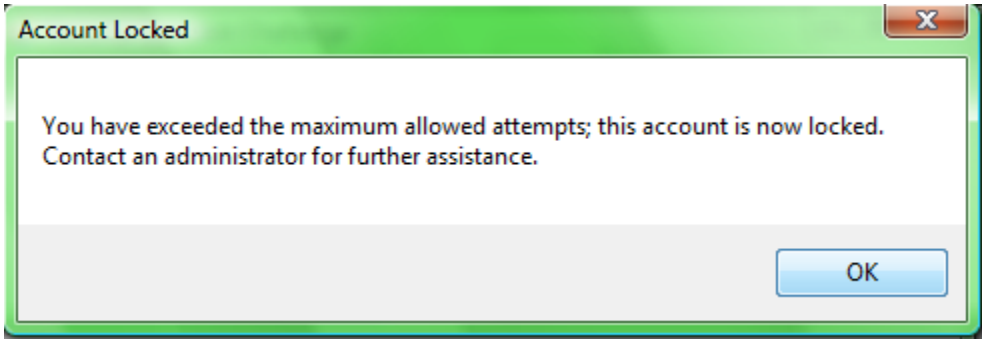
Once the security questions have been activated by Central Administration and chosen by users, they will be used to verify the identity of the user when the administrator has reset the password.

When the user logs in to CAREWare with the new password, one or more Security Question Challenge windows will appear, asking the security questions previously selected.

Users may be required to answer more than one security question, depending on how many are required by the Central Administrator. CAREWare cycles through the stored questions in order, even when there are more stored questions than required at login. For example, if a user stores three questions but is only required to answer two, she will answer questions 1 and 2 the first time her password is reset and questions 3 and 1 the second time.

Although not case sensitive the answer must otherwise match the stored answer exactly. If the questions are answered correctly, the user will be allowed to log in to CAREWare as usual.

If the user enters the wrong answer, the question is repeated. If the number of incorrect answers exceeds the number allowed, the account will again be locked. A window will appear notifying the user that he/she has exceeded the maximum allowed attempts and the account is now locked.



It is important to understand that the number of allowed attempts (or wrong answers) is the total allowed for all security questions. For example: users are required to answer 3 questions and the maximum tries is set to 3. The users will need to answer each of their 3 personal questions correctly. If they give 3 incorrect answers total (not 3 per question, 3 *total* wrong answers) before they give the correct answer to all 3 of their questions, then their account would be locked.

Central administrators will have the ability to completely reset a user account in the event that the password is reset and security questions cannot be answered correctly. This will delete all user questions and treat the user as a brand new user. The Central Admin will set a temporary password for the user and the user will be required to select 3 security questions when they log in.

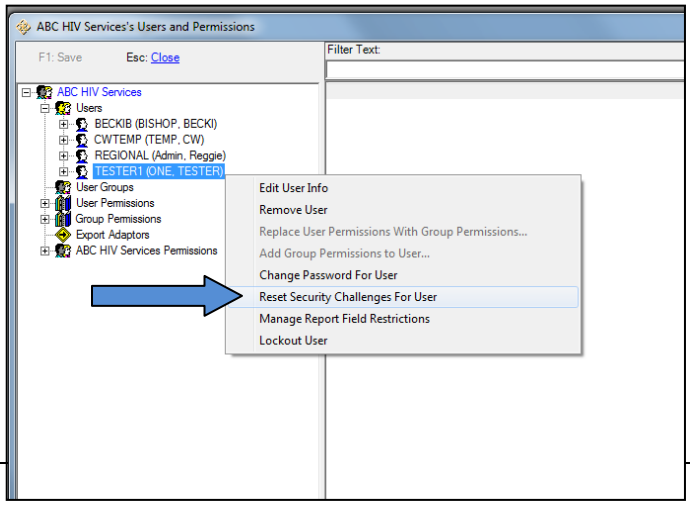
The Central Administrator resets the user account, including the Security Questions, through the Provider/User Manager in the Central Administration domain.

In the Provider/User Manager, under Real-Time Providers, select the Provider Domain of the user in question.

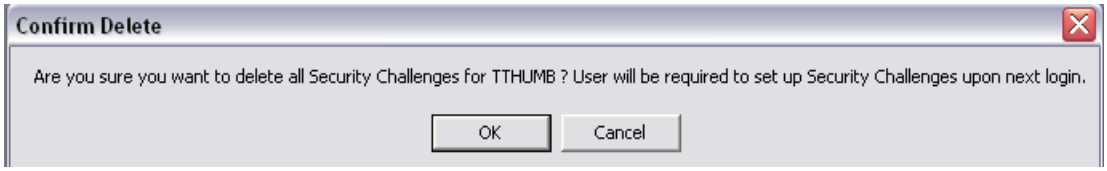
Open the Provider Domain (double click on the name or right-click and choose View Provider).

Expand the list of Users, and select the user whose account will be reset.

Right-click on the user name and select Reset Security Challenges for User from the list.



A Confirm Delete window will appear to verify this action. Click OK to confirm the deletion.



A Quality Check window will appear stating that Security Challenges have been reset. Click OK.

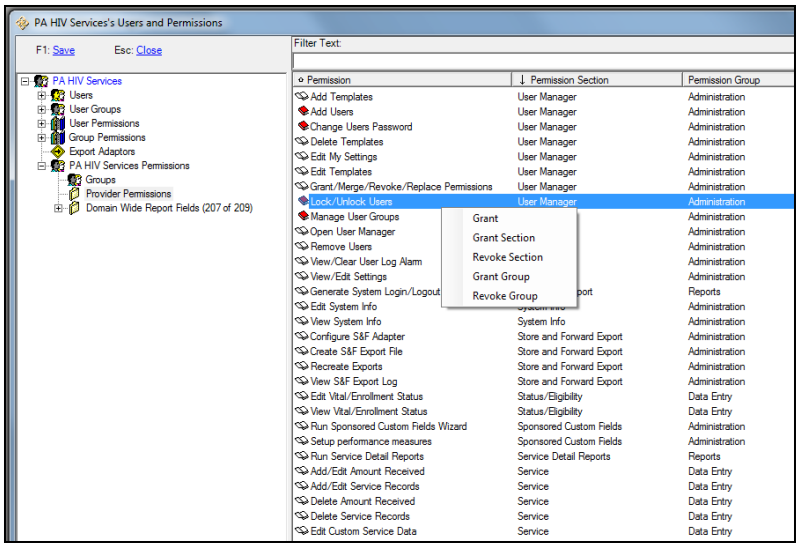
Reset the password for the user again (if necessary) by selecting this option from the right-click menu while highlighting the user name. Type in the new password for the user (twice) and click Change Password button. Click OK on the Password Has Been Reset notice.

Click Close and Close again to exit the Provider/User Manager.

The effected user will be prompted to choose three security questions and answers again upon logging in with the new password.

Unlock Users at the Provider Level

CAREWare can now be set up to allow users to be unlocked at the Provider Level. The permissions of Change Users Password and Lock/Unlock Users have been added as ones that can be granted to the Provider Domain and to Users in that Provider Domain. The permissions must be granted originally through the Provider/User Manager in the Central Administration domain. Once granted, a local provider administrator will be able to lock and unlock users and reset passwords when necessary. (Note that users will be required to answer Security Challenge Questions after a password reset; see above).



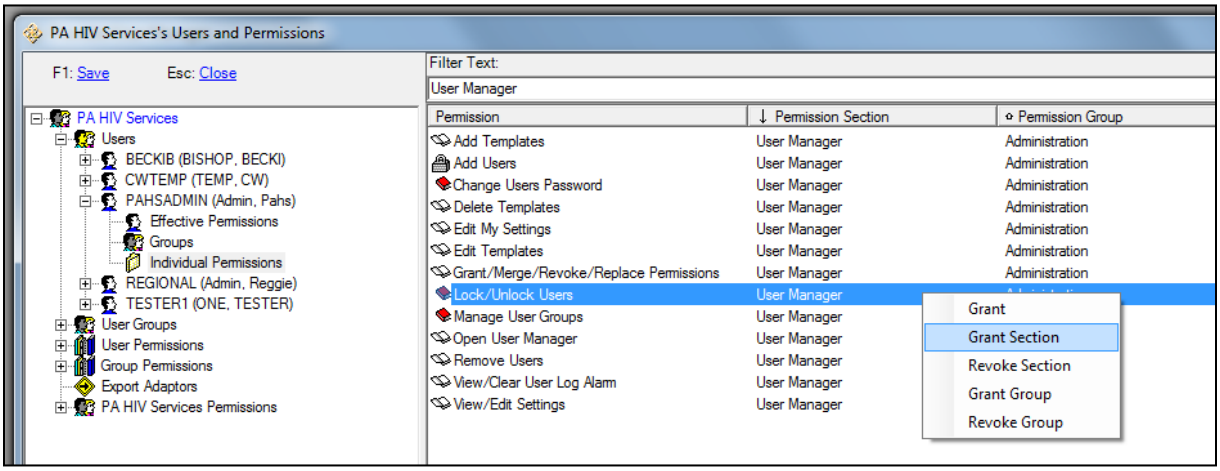
To enable this feature, login to the Central Administration domain and choose Administrative Options, and Provider/User Manager. Expand the Real-Time Providers section and open the Provider domain where the permissions will be granted.

First grant permissions to the Provider. Expand the Provider's

Permissions section and highlight Provider Permissions. In the Administration Permission Group, under the User Manager Section are the two new permissions, *Change Users Password* and *Lock/Unlock User.* Right-click on each new permission and choose Grant from the right-click menu. Click on Save to save the changes to the Provider Permissions.

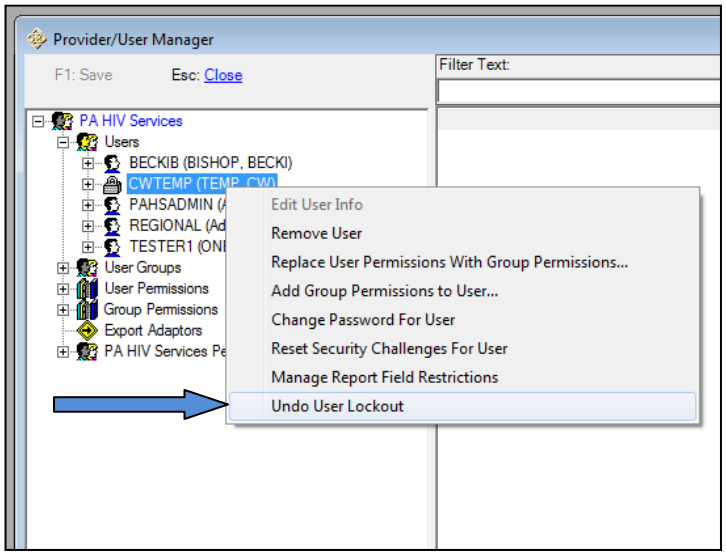
After permissions to *Change Users Password* and *Lock/Unlock Users* have been granted to the Provider, the same permissions must be granted to one or more users in that Provider domain.

Move to the Users section, expand the list of Users and select the Individual Permissions Section under the user who will be acting as the provider administrator.



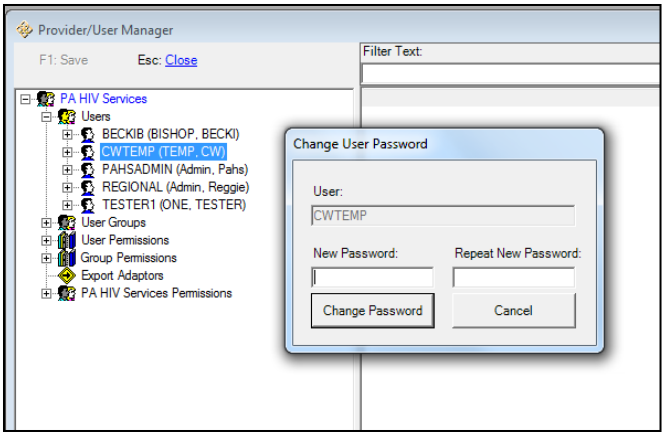
Type *User Manager* in the Filter Text box at the top of the Permission List to quickly find Permission Section that contains the new permissions. Right-click on one of the new permissions and choose Grant Section to add all the new User Manager permissions to this user. An alternate approach is to add the permissions to a User Group (say for a Provider Administrator) and then make the user a member of the User Group.

When finished, click on Save. Now this user at this provider will be able to manage the tasks of unlocking users and resetting passwords. The user is now a Provider Administrator.



Now, when a user at the provider site gets locked out of CAREWare because of a forgotten or mistyped password, the new Provider Administrator can unlock the user's account and reset the password (prompting the Security Questions feature—see above)

without needing to call a Central Administrator.



To do this, open the Provider/User Manager from the Administrative Options menu, and locate the locked account by expanding the list of users. To unlock the user, right-click on the user name and choose Undo User Lockout from the right-click menu.

Once the user is unlocked, right click again on the user name and select Change Password for User. The Password Reset screen will appear.

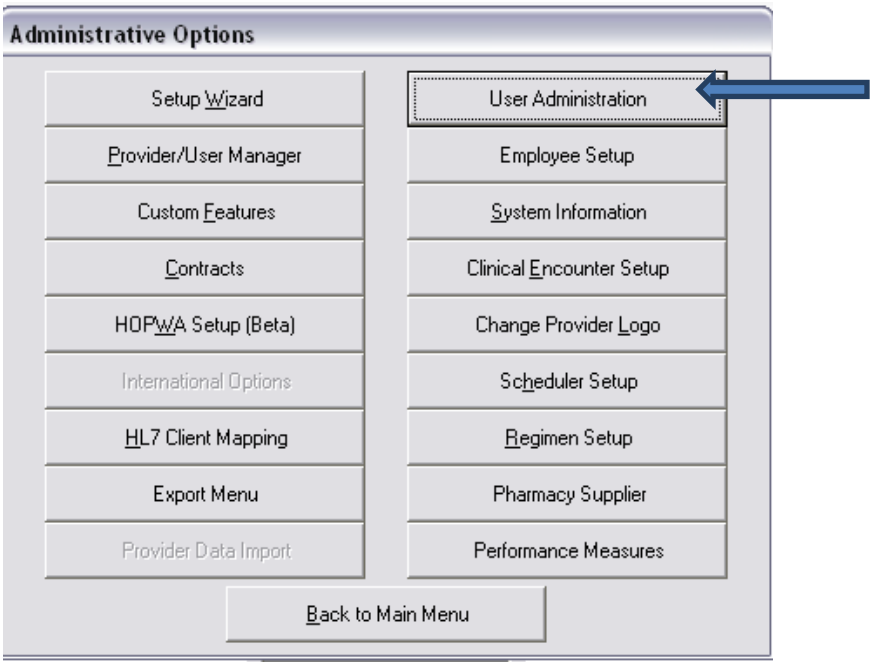
To change the password, type in a new password in the two available boxes, select Change Password, and then select OK on the Quality Check window.

Click on Save and then Close to end the Provider/User Manager session.

If Security Questions have been enabled the person whose password was reset will be prompted to answer one or more security questions before the login with the new password will be completed.

In addition to the method for unlocking users and resetting passwords through the Provider/User Manager as described above, the Provider Administrator will have another option available. This is through a new button on the Administrative Options menu called User Administration. Administrators at the provider level, with permissions, will also be able to reset a user's security questions from this screen, just as Central Administrators can do.

The User Administration screen also gives access to the Report Field Restrictions feature of CAREWare, discussed in the next section of this guide.


Administrative Options
Setup Wizard
User Administration
Provider/User Manager
Employee Setup
Custom Features
System Information
Contracts
Clinical Encounter Setup
HOPWA Setup (Beta)
Change Provider Logo
International Options
Scheduler Setup
HL7 Client Mapping
Regimen Setup
Export Menu
Pharmacy Supplier
Provider Data Import
Performance Measures
Back to Main Menu

Restriction of PII in Custom and Canned Reports

This new feature of CAREWare 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 can appear in CAREWare's built-in reports.

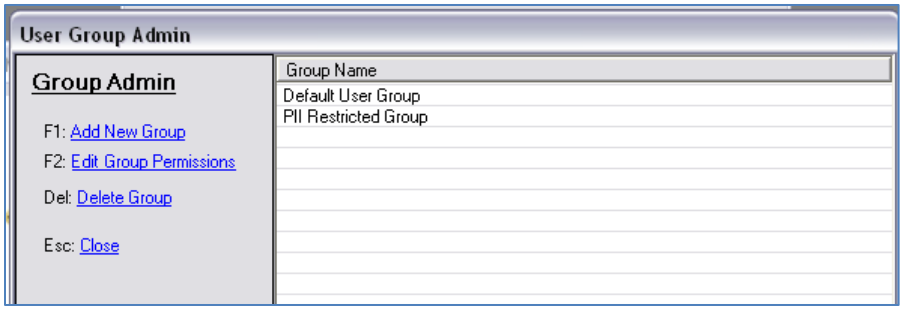
Report restrictions are managed via permission 'Groups' that can be configured via the Advanced Security Options menu or through the Provider/User Manager at the Central Administration level and through the User Manager button or Provider/User Manager at the Provider Domain level.

Each canned report that shows PII has a new check box to "Hide PII Fields". For users whose access to PII in reports has been restricted by administrators, this check box will be automatically checked and deactivated so that it cannot be unchecked. Users whose permissions allow PII to show in reports can elect to check this box before running a canned report. When PII are hidden in canned 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 the canned 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.

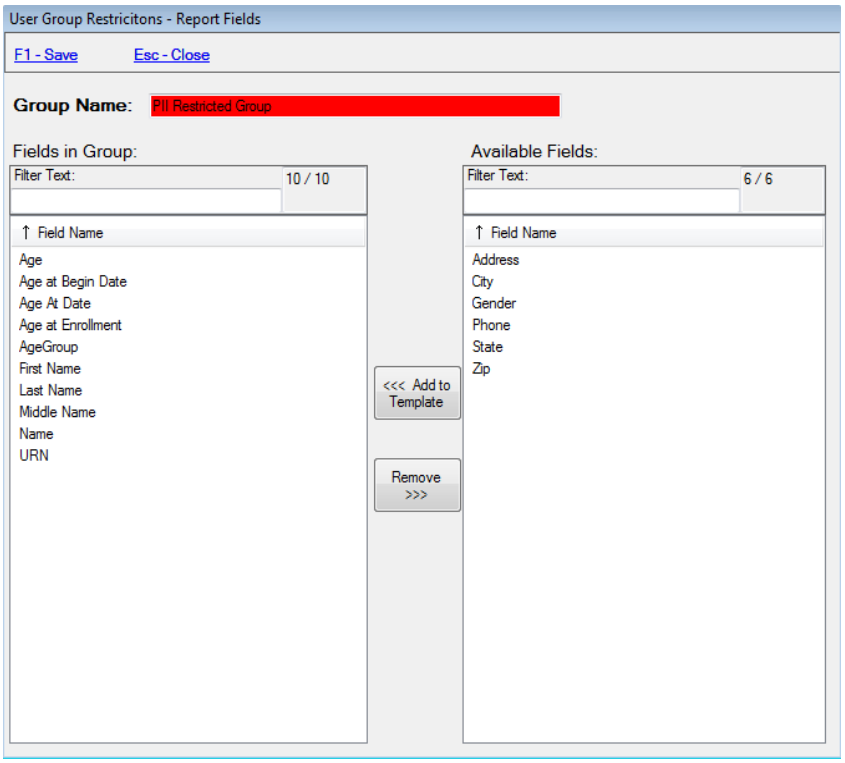
Setting up Report Groups

In the Central Administration domain, Report Groups can be setup using either the Provider/User Manager or using the Advanced Security Options button on the Administrative Options screen. The following example uses the Advanced Security Options button.



Choose Advanced Security Options from the Administrative Options menu, and then choose User Group Admin (Reports) from the Advanced Security Options menu. A new screen will open. On the left side of the screen are the links to the available actions, Add, Edit or Delete Group. On the right is the list of Group Names. To begin there are two groups, Default User Group and PII Restricted group. Highlight the PII Restricted Group and choose the Edit Group Permissions link or type the F2 key. A new screen will open.

This is the screen used to set up the User Group restrictions. In this screen shot there are already some fields that have been added to the list that will be in the PII Restricted Group.



To add more fields, such as Zip code or address, highlight those fields in the available fields list on the right. Then click the Add to Template button. To remove fields from the restricted list, highlight the fields on the left and click on the Remove button.

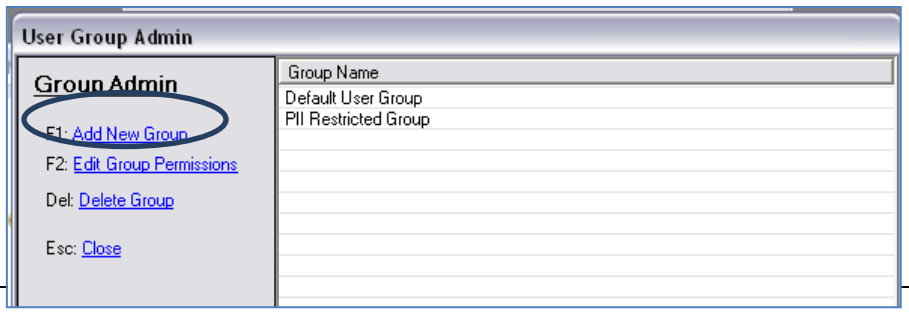
The red Group Name indicates that this is a built-in Restriction Group. The Group Name cannot be changed for built-in groups, and the group cannot be deleted, but users are still allowed to define which fields are included in the group. There are two built-in Restriction Groups in CAREWare:

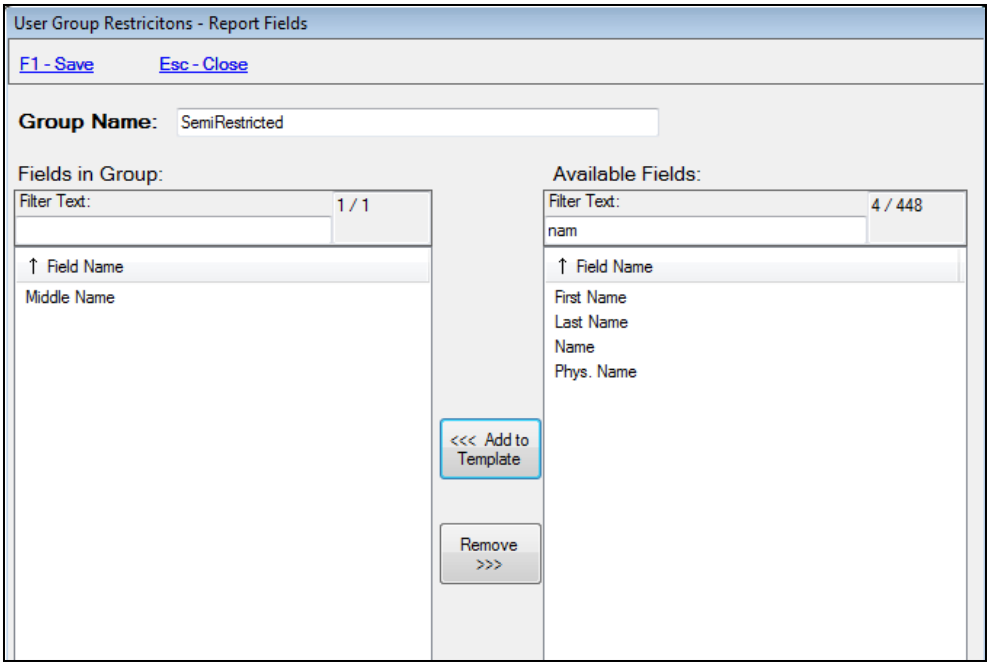
The PII Restricted Group only has a limited number of available fields – those that are relevant Personal Identifying Information. Note that this group also defines what fields are hidden when Hide PII Fields is selected for canned reports.

The Default User Group is automatically added to any new user that is added to CAREWare. This is a useful security feature that allows a site to, by default, limit access to report data for all new users. If a site does not wish to have default restrictions, they can simply add no fields to this group. It comes with no restricted fields to begin with.

When satisfied with the selections of fields to be restricted in the PII group, click on the Save link or type the F1 key. The PII Restricted Group is now saved and the User Group Admin screen will appear again.

To add a new Report Restriction group, click on the Add New Group link or type the F1 key.



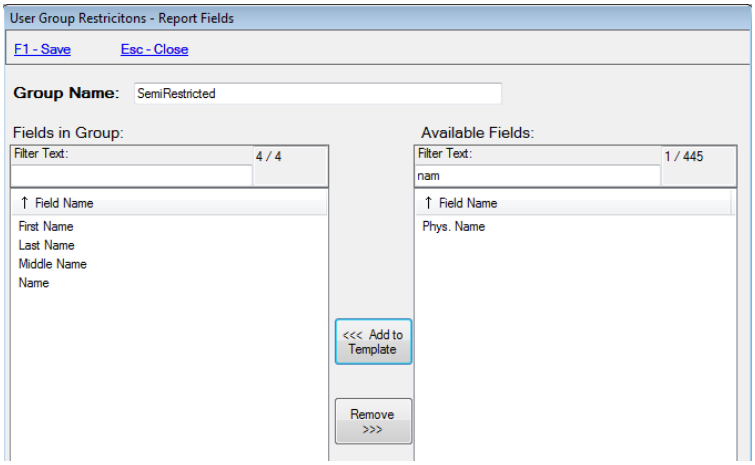


Type in a label for the new group in the Group Name box. This one says SemiRestricted.

To find a particular field in the available fields list, type part of its name in the Filter Text box, as in the example above. Select the fields and then click Add to Template. The selected fields will be moved to the list of fields in the group on the left.

Here is the new Report Restriction Group labeled SemiRestricted after the Add to Template button has been clicked. In this example, only the names of clients are restricted (so far).

The list of available fields on the right is only showing the Physician name because "nam" has been typed in to the Filter Text box and all the other name fields have been moved to the restricted list. When the text in the filter box is removed the full list of available fields will appear again. When satisfied with the list of fields that will be restricted in this SemiRestricted group, click on the Save link or press the F1 key.

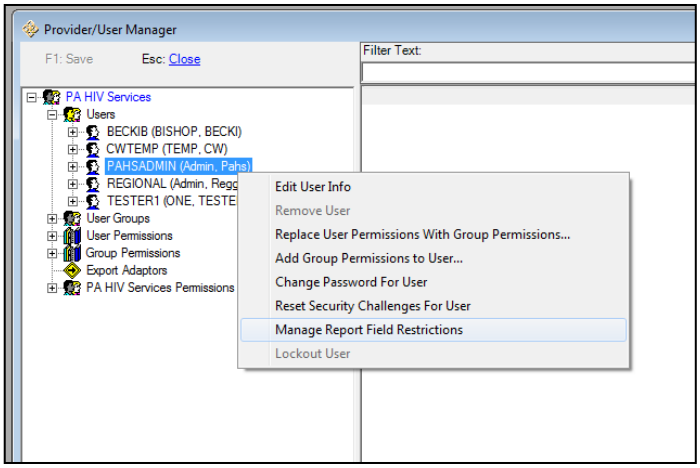


The Default Restriction group has no fields restricted. If you want to add restrictions to this group, it is done the same way as has been described for the PII Restricted Group and the new group created as in the above example (SemiRestricted).

To delete a Report Group from the list, highlight the name of the Report Group, and click the Delete Group link or type the Delete key. A Confirm Delete window will appear asking Delete the selected Group? Click OK to delete or Cancel to stop the deletion process.

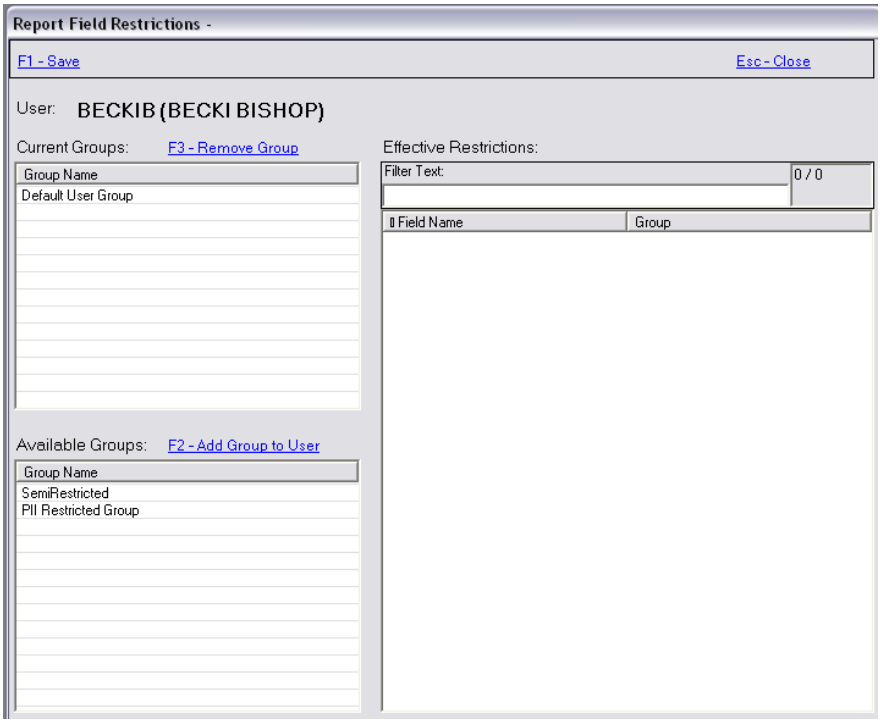
When finished setting up report groups, choose the Close link or type the Esc key to return to the Advanced Security Options menu. Click Close on that menu to return to the Administrative options screen.

Now it is time to assign report groups to the users at the various Provider Domains. In the Central Administration domain this is done through the Provider/User Manager. Open the Provider Domain under the Real-Time Providers section and expand the Users list. Highlight the name of a user and right-click. From the right-click menu, choose Manage Report Field Restrictions.



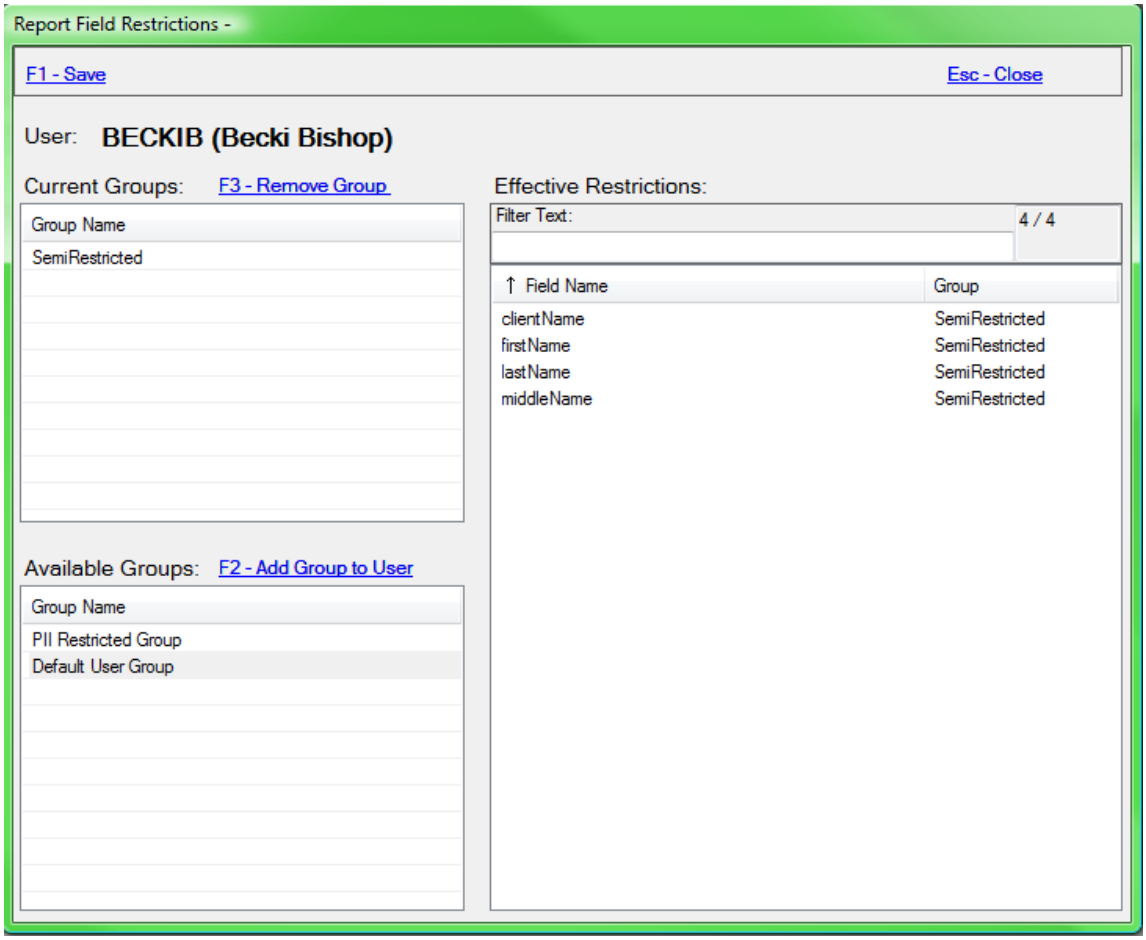
This will open a new screen where the various report groups that have been established can be assigned to the user. (Report group assignment to users can also be done by Provider Administrators through the User Administration button).

The Report Field Restrictions screen allows an administrator to assign a particular report group restriction to the user. In the example on the right, the user belongs to the Default User Group, showing in the Current Groups list in the top left box. This group has no field restrictions so none are showing in the Effective Restrictions box on the right of the screen. The available report restriction groups that can be used are in the Available Groups list on the bottom left side of the screen.



In the next screen shot, the

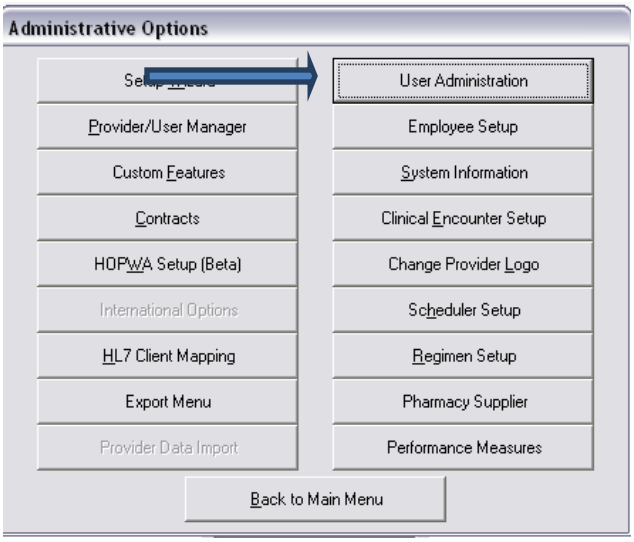
administrator has chosen to change the Report Group assignment for this user by highlighting the Semi Restricted group and clicking the Add Group to User link.



(It is possible to add more than one group to a user at a time, thus accumulating fields that are restricted). In the example above, the administrator removed the Default User Group by highlighting it in the Current Groups box and clicking the Remove Group link. The end result is that the user's restrictions are as defined in the SemiRestricted group. The fields that are restricted now show in the Effective Restrictions box. The Group column in this box shows which group the restrictions come from.

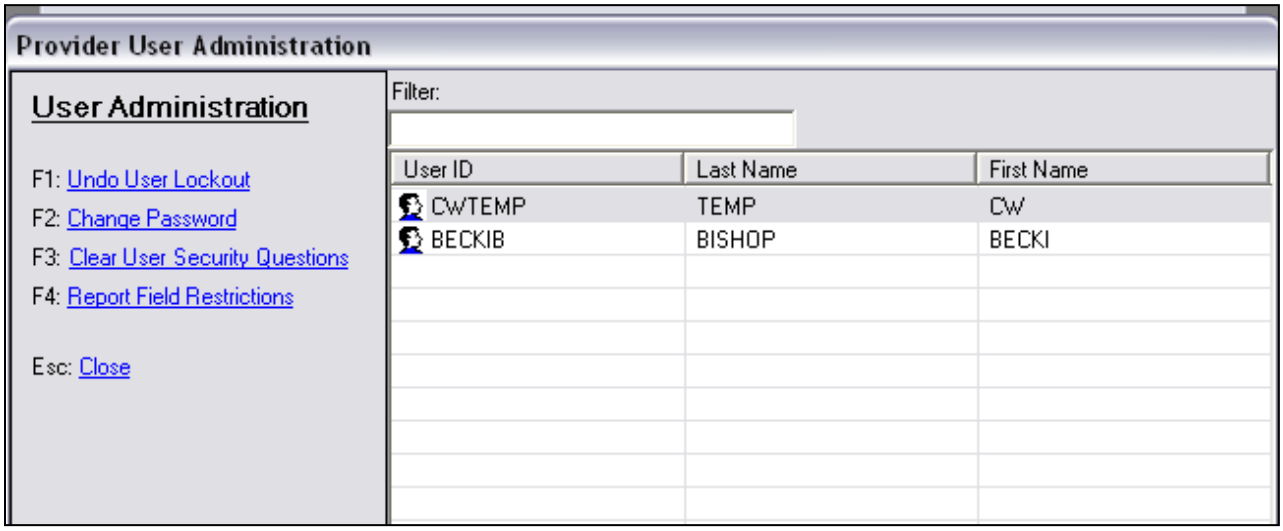
When satisfied with the report group restrictions applied to the user, click on the Save link or type the F1 key. Repeat the group assignment process for each user whose access to fields in reports is to be restricted.

Each user will be assigned the Default User Group to begin with. If the Default User Group is left with no restricted fields in it, then users with that Group assignment will have no report field restrictions. Administrators may want to add restrictions to the Default User Group so that every new user starts out with report field restrictions.



Provider Administrators will be able to perform various administrative tasks related to users either through the User Administration button on the Administrative Options menu or through the Provider/User Manager, also found on the Administrative Options menu.

Choosing the User Administration button opens a Provider User Administration screen with a list of users on the right and a list of available actions on the left. The available options are Undo User Lockout, Change Password, Clear User Security Questions, and Report Field Restrictions.



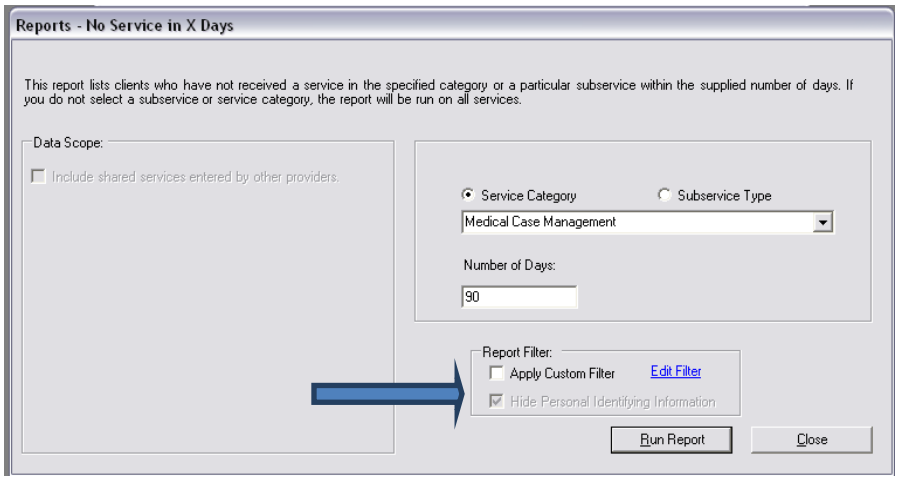
To give the user a Report Field Restriction assignment, highlight the user name in the list and click on the Report Field Restrictions link or press the F4 key. The same screen as appears for the Central Administrator will appear (shown on the previous page) and it works the same way. The available groups are in the bottom left box, the assigned group is in the top left box, and the restricted fields (based on the report group assigned) show in the box on the right.

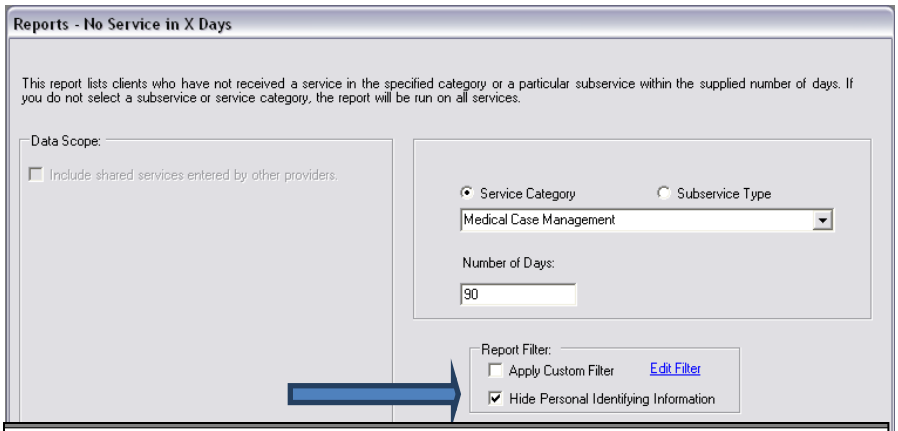
How Report Restriction Groups Effect Custom and Canned Reports

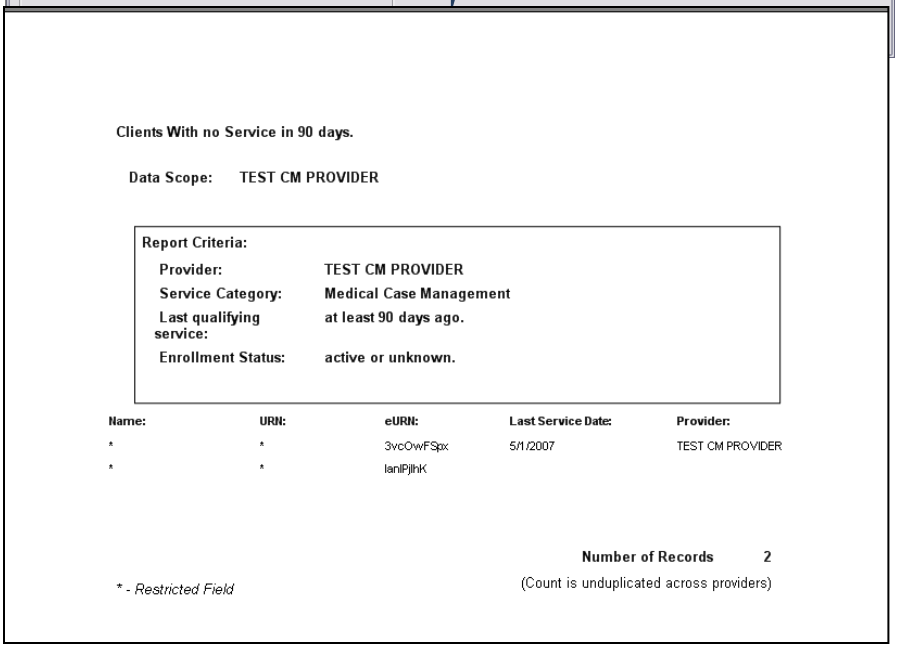
What is the result once the Report Field Restriction Groups have been established and users are assigned to the groups?

In canned reports (those that are built in to CAREWare), if the user has PII fields restricted, the fields defined as part of the PII Restricted Group (see above) will show up in the report as an asterisk. The

eURN (encrypted URN) will be added to the report to have a means of identifying the individuals without revealing their names.







Clients With no Service in 90 days.

Data Scope: TEST CM PROVIDER

Report Criteria:

Provider:	**TEST CM PROVIDER**
Service Category:	**Medical Case Management**
Last qualifying service:	**at least 90 days ago.**
Enrollment Status:	**active or unknown.**

Name:	URN:	eURN:	Last Service Date:	Provider:
*	*	3vcOwFSpx	5/1/2007	TEST CM PROVIDER
*	*	IanlPjlhK		

Number of Records 2

(Count is unduplicated across providers)

** - Restricted Field*

Each canned report screen has a check box that says Hide Personal Identifying Information. For users with PII report restrictions the box is checked and grayed out so it cannot be unchecked.

This screen shot gives an example, using the No Service in X days report. The Hide PII check box is checked and cannot be changed by the user. The report can otherwise be set up as desired.

If a user does not belong to a report group that restricts the display of PII in reports, the Hide PII check box is still available, and the user may choose to check it or not as shown in the screen shot to the left.

When the Run Report button is clicked, and the Hide Personal Identifying Information box is checked, the report will not include PII.

Each field considered PII will be represented by an asterisk instead, as illustrated by this screen shot of a canned report.

The encrypted URN (eURN) is added to the report to

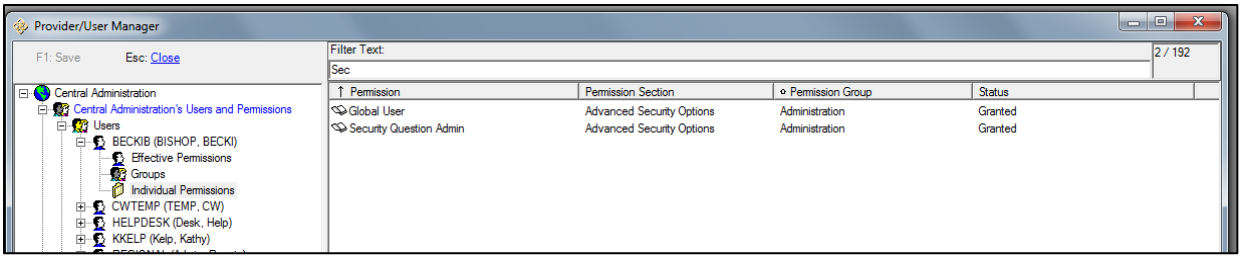
identify the client instead.

For Custom Reports, the user with PII restrictions can choose PII fields when designing a report, but when the report is run it uses asterisks in the place of those fields, just as is done in the canned reports.

Global User Account

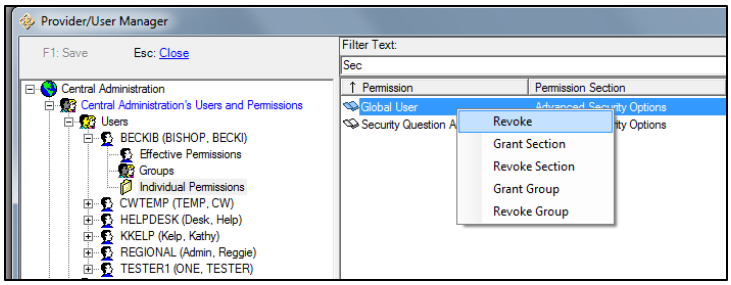
In the original design of CAREWare, all Central Administration users were able to view client records across all providers, run reports across all provider domains or for an individual provider, and complete various configuration tasks on behalf of the Real-Time Provider Domains when logged in to the Central Administration domain. This full access to all data in the Central Administration domain will now be specifically granted through a new "Global User" permission. (The Global User permission will be automatically granted to all current Central Administration users upon installation of the new version of CAREWare).

The Global User permission is found in the Administration Permissions group in the Advanced Security

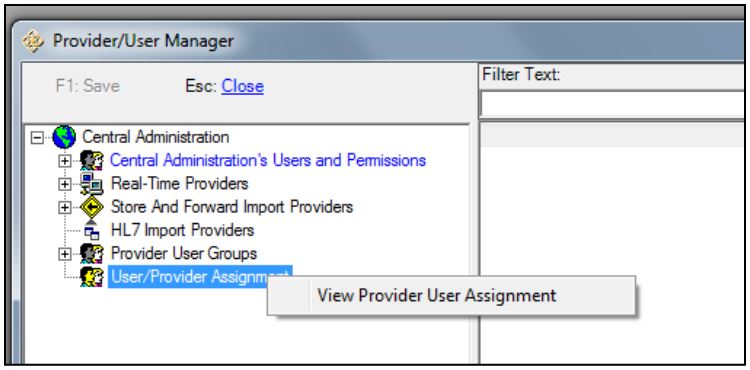


Options Section. To find it quickly, begin typing the word Security in the Filter Text box as shown in the screen shot below.

It is now possible to remove the Global User permission from Central Administration users and restrict the scope of data they may view in the Central Administration Domain. When the Global User permission is turned off for a user, access to data in the Central Domain will be based on the User/Provider assignments granted to the Central Administration users through the Provider/User Manager.

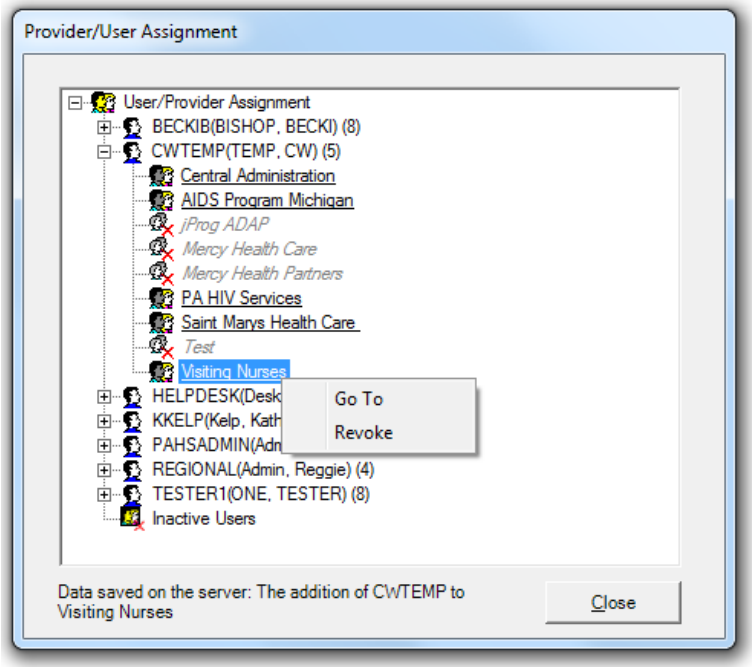


To revoke the Global User permission from a Central Administration user, right-click on the Global User permission in that user's permission list, and choose Revoke from the right-click menu.



The open book (symbolizing a granted permission) will change to a closed red book (symbolizing the permission is not granted).

Once the Global User permission has been revoked from a Central Admin user's account, save the changes made by clicking on the Save button. Now this user's rights in the Central Administration domain can be further restricted through the User/Provider Assignment section of the Provider/User Manager.



Open the User/Provider Assignment section by highlighting and double clicking on it or by right-clicking and choosing View Provider User Assignment.

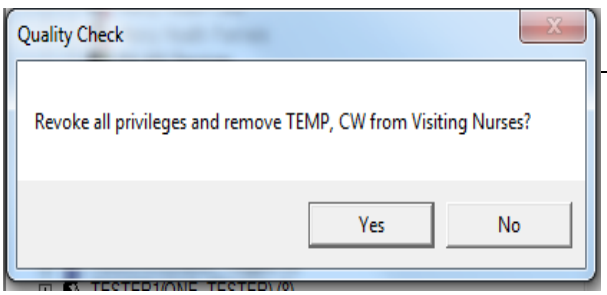
Expand the list under the Central Administration User whose User/Provider Assignment is to be changed.

This screen shows CWTEMP's current User/Provider assignments. To remove access to Visiting Nurses data, highlight the domain name and right click. Choose Revoke from the right-click menu.

(The Go To choice would open the domain's User list in the Central Domain, with CWtemp's User name highlighted. The administrator could then grant or remove permissions for CWtemp in the Visiting Nurses domain. These permissions could allow CWtemp to directly login to the domain. The act of revoking rights to the Visiting Nurses domain will remove any previously granted privileges CWtemp had to that provider domain).

Click Yes on the Quality Check screen to revoke all privileges and remove CWTEMP from the Visiting Nurses domain.

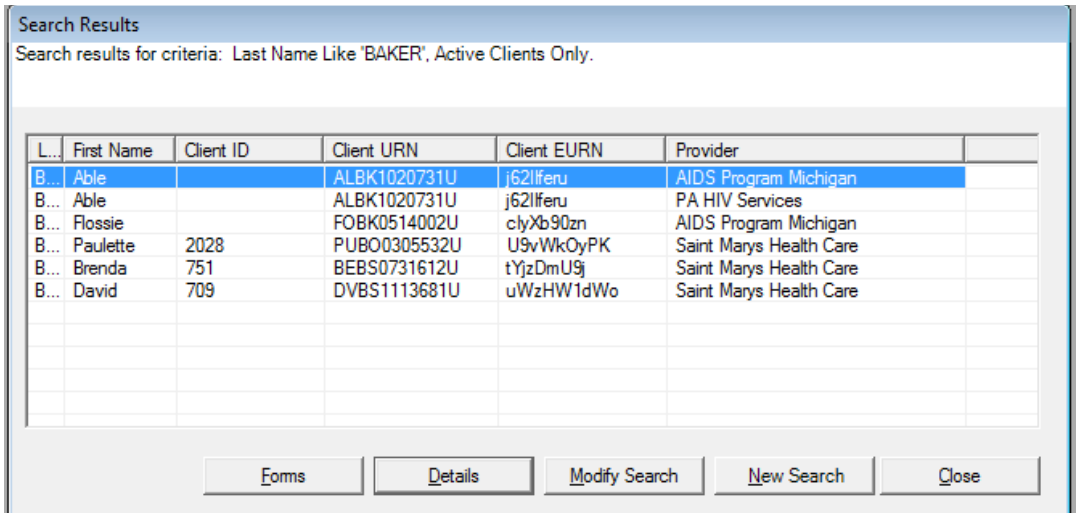
When CAREWare finishes revoking the privileges and saving the changes, the Provider/User Assignment screen will reappear. There will now be a red X icon by the Visiting Nurses domain name for CWTEMP, just as



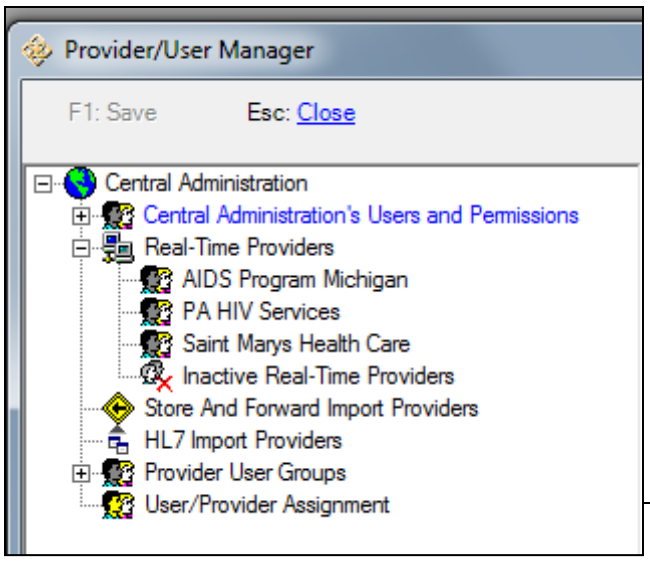
there is for jProg ADAP, Mercy Health Care and Mercy Health Partners in the above screen shot.

CWTEMP now only has privileges at AIDS Program Michigan, Saint Marys Health Care, and PA HIV Services provider domains and to the Central Administration domain. The user BeckiB still has the Global User permission in the Central Administration domain, and has also been granted rights to all the Provider Domains in the CAREWare network. These two Central Administrators now have very different capacities to see and use the data in the Central Administration domain and in the individual Provider Domains.

CWTEMP will be able to view client data and run reports (Custom, Financial, RDR, Performance Measures, etc.) only for the three provider domains that have been granted to that user account. But BeckiB will be able to view all client data across all Provider Domains and run reports for all domains individually or as a group. She can also login as a user in each Provider Domain.



This screen shot shows what CWTEMP will see when searching for client records. Only client records from the three provider domains assigned to CWTEMP will be available when doing client searches. If Central Administrator BeckiB searches client records, data from all provider domains that match the search criteria will appear in the Search Results list.



The screen shot below shows that CWTEMP's view of the Providers in the Real-Time Provider list in the Provider/User Manager only includes the Provider domains that have been granted. The other Real-Time Providers don't even show up.

This means that CWTEMP will only be able to perform Central Administration tasks for these three domains. CWTEMP could be a Regional Administrator with these permission settings.

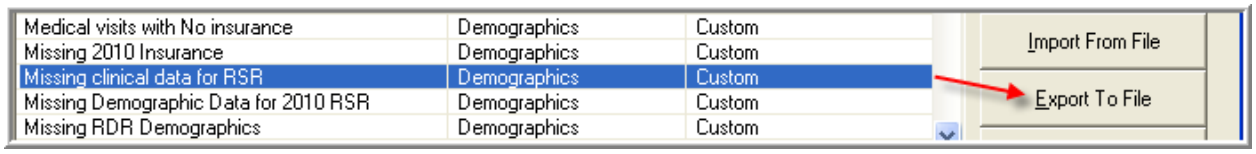
Restricting Central Administration user accounts will provide more privacy for Providers and for clients. Advantages of a restricted centralized database will be realized by the Regional Administrators in accessing aggregate reports from providers within their respective regions.

Copying Custom Reports

You can copy custom reports and send them to other providers and users, just as you can with Performance Measures.

Exporting:

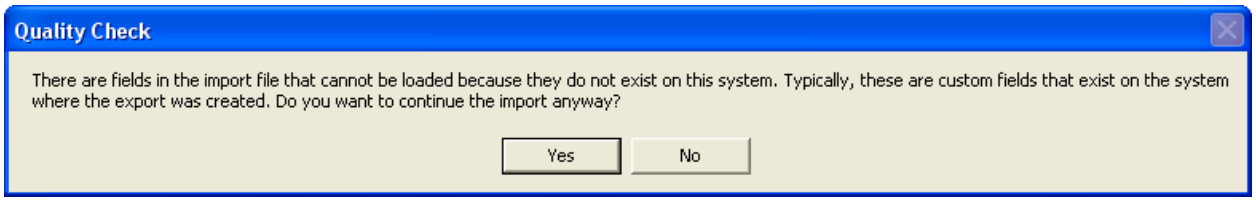
1. In custom reports, select a report that you want to copy and send to another user. Click on Export To File, as shown here:



2. Save the file to a location that is easy to find. Leave the file type as XML, but provide any file name that makes sense.

Importing:

When you import a file from another user, simply select that file and click "Import From File." If the custom report you are importing contains a custom field that your system does not recognize, you will receive the following message:



You can still import the report, just remember that you may need to edit or simply check the field selections and/or filter. Actually, that's probably a good thing to do anyway.