

PIC Security Administration

Table of Contents

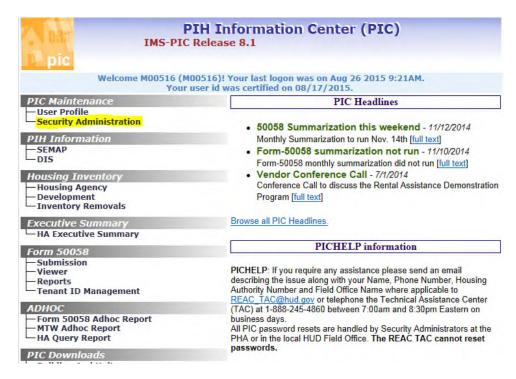
Overview	3
Create New Users	4
Assign Roles to a User	7
Removing User Roles	11
Terminating User Access	13
Modifying User Details and Editing Expiration Dates	15
Modify Special Privileges – Unmask Privacy Data (PII)	17
Security Reports and Monitoring Access	18
User Security Access Report	19
Privacy Act Access Report	20
Global User Search Report	21
User Access by Submodule Report	22
User Activity Query	23
New Users Report	25
Improper Logoff Report	26
User Account Usage Report	27
Appendix: Sub Module Access Descriptions	28
Appendix: Adding the PIC Link to the Secure Systems Main Menu	30

Overview

There are several items that users who have been designated "security administrators" can do in PIC. Security administrators should always maintain documentation in a secured location that supports the actions that they take.

For all the tasks addressed in this document there are three things to keep in mind:

- 1. You will need to start by going into the Security Administration sub module using the Security Administration link on the PIC Main Page (see screen print below).
- 2. If you have been granted security administration access for multiple entities, you will need to navigate to the appropriate entity before completing your desired task.
- 3. After you have completed all tasks in the system you must log out using the Logoff link. You then need to return to the WASS Main Menu to continue to work in other systems or to log out of Secure Systems using the Logout link.
- ➤ If you do not see the Security Administration link, then you are not setup as a security administrator in PIC. If you are supposed to be setup to do these tasks, then another user who is assigned this role will have to assign it to you or if there is not anyone at your PHA assigned this role then you will need to contact your local PIC coach.



Create New Users

Before you can setup a new user in PIC you will need to have the following pieces of information. There is not an official (OMB approved) PIC access authorization form but some HUD field offices and PHAs may have developed one for use in their jurisdiction. Since this not an official form, it is not required that you complete one, but you should have the details below in writing from HA management or the user's direct supervisor.

- User ID (WASS ID) for PHA users the user ID will begin with an M, for HUD users it will begin with an H. It is six characters long. If a PHA user does not have a user ID, they can register at http://www.hud.gov/offices/reac/online/online_registration.cfm and select Public Housing Agency. They will choose to be a coordinator (can do security work in WASS) or a user. For some users external to HUD (e.g. PHA auditors) the user ID may begin with an I.
- First and last name middle initial can be entered but is not a required field
- Email address
- A list of roles that will be assigned to the user this task will be in addressed in another section.

PIC user types – there are four types of users in PIC, which one(s) you can select depend on your user type.

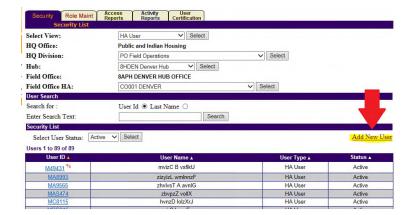
- HA housing authority users and users that work for companies that submit 50058s on behalf of PHAs (contractors, software vendors)
- HUD HUD employees
- Guest Generally HUD contractors or contractors working for a PHA (exception is 50058-related contractors)
- Super a limited number of HUD users who can perform functions in the system that regular HUD users cannot (also generally referred to as "power users")

Note:

- •
- For the new user to access PIC (to see the link for PIC) the Secure Systems coordinator (may or
 may not be the same person as the PIC security administrator) will also need to assign the role
 for PIC in WASS in Secure Systems. This is addressed in the appendix section at the end of this
 document.
- If a user needs access to more than one PHA or HUD field office this is done by assigning roles to those additional entities. The user ID will be listed (housed) under their first/primary entity.

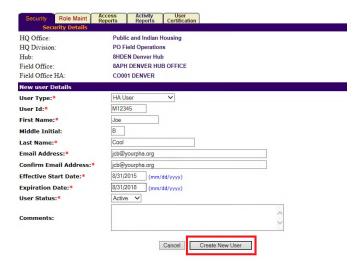
The instructions below are for PHA users and as a reference point for HUD users as to the process for adding a new user. New HUD users are inserted via a DIAMS system request submitted by the user's supervisor in DIAMS. The supervisor should include the office the user's office in the "Special Instructions". The security administrator in the user's office **should not** insert new users. Once the DIAMS request is processed, the DIAMS processor will add the link for PIC on the Secure Systems Main Menu page. At that point, the security administrator in the user's office can assign roles using the information in the assigning roles section of this document.

1. Single click on the Add New User link on the right side of the page.

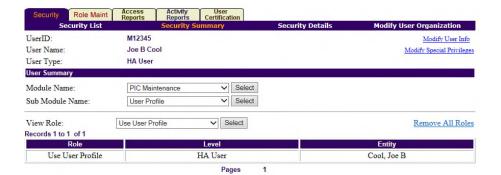


- 2. On the Create New User page enter the details for that user. Keep in mind the following items:
 - Ensure that you select the correct user type from the User Type drop down box.
 - The effective start date is generally the day the user is added.
 - ➤ The expiration date can be up to three years in the future. Keep in mind that once this date is reached not after the user will not be able to access the system unless you have gone in and extended the date.
 - ➤ Do not make a selection from the User Status drop down box; leave it at the default status of "Active".
 - ➤ The Comments box is to make any notes about the user, for instance if they are only in PIC to facilitate adding them as a user in EIV you may enter "EIV only user".

When you have entered all the information for this user single click on the Create New User button.



- 3. The page will refresh, and you will see the Security Administration Summary screen for the new user. If you need to add roles to this user, please proceed to step 2 of the "Assigning Roles" section. If this user was added so that EIV access can be granted you will need to wait overnight for the user ID to be available in EIV.
- 4. If you do not need to assign roles to the user, you may log out of PIC using the Logoff link. Make sure to use the link on the next page to go back to the WASS Main Menu so you can also log out of Secure Systems.



Page 6 of 30

Assign Roles to a User

Assigning roles to a user is done when a user is first created in PIC or later when access needs change. There are different levels of access that can be assigned to a user. PHA management should use care when deciding what access to assign to a user. Access can be modified at any time as duties change. A user should only be granted enough access to accomplish the functions of their job. Ensuring users cannot access or edit data that is not necessary to their job protects the integrity of the data in PIC.

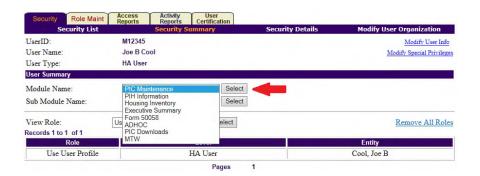
Levels of access – <u>only one role should be assigned per sub module</u> to prevent multiple roles from conflicting with each other and causing some system tasks to be unavailable.

- Read only allows a user to view data but not edit or submit data
- Edit allows a user to view and edit data
- Submit (HA user only) allows a user to view, edit, and submit data
- Approve (HUD user only) allows a user to view, edit, and approve data (in rare cases data can also be submitted)

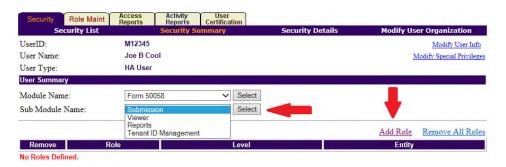
PIC is organized in a module and sub module structure. A description of each sub module is included in the appendix at the end of this document. This will help management decide what access a user needs. Security administrators will be responsible for assigning the desired role in the sub module(s) the user needs access to.

Note:

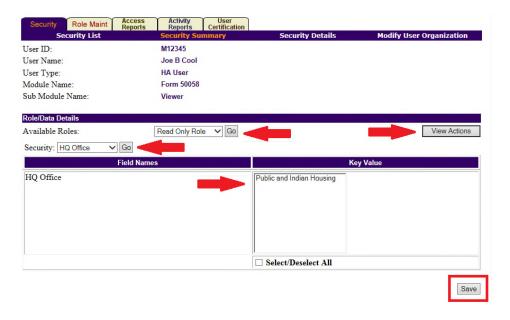
- By default, the system automatically assigns the user the User Profile role under the User Profile sub module when their user ID is added to the system. This allows the user to maintain their user information such as name, email, office address, and phone number.
- If a user needs access to more than one PHA or HUD field office this is done by assigning roles to those additional entities in step 8 below.
- 1. In the Security Administration sub module, single click on the user ID for the user you wish to add roles to.
- 2. On the Security Administration Summary page single click on the Module Name drop down box to see the list of modules you can navigate to. Single click on the module name and then single click on the Select button to refresh the page.
 - ➤ If you do not see the name of a module you need to assign access to it is because you do not have it and therefore cannot assign access to it. Please consult with another security administrator at your PHA, if there is one, to see if it should be assigned to you or if they can assign that role or contact your local PIC coach for assistance.



- 3. Single click on the Sub Module Name drop down box to see the list of sub modules you can navigate to. Single click on the sub module name and then single click on the Select button to refresh the page.
 - If you do not see the name of a sub module you need to assign access to it is because you do not have it and therefore cannot assign access to it. Please consult with another security administrator at your PHA, if there is one, to see if it should be assigned to you or if they can assign that role or contact your local PIC coach for assistance.

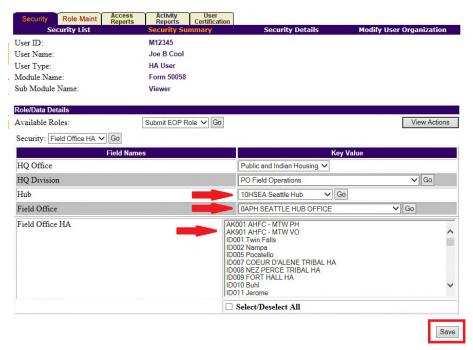


- 4. When the page refreshes you will be able to see if there is already a role assigned to the user for this sub module. If the desired role is already assigned, you can stop here. If a different role than the one you want to assign is already assigned, you will need to remove this role **before** you can add one. See the section in this document about modifying user access for information on removing the existing role. Proceed to the next step if you see the message "No Roles Defined" underneath the role table.
- 5. Single click on the Add Role link. A page similar to the screen print below will appear.



6. On the Add Role page you need to select the role you want to assign. Single click on the Go button to select it. If you are unsure what actions that role will enable the user to perform, you can single click on the View Actions button. If you want to see the actions for a different role you will need to

- select that role and single click on the Go button to refresh the list. If you click on the View Actions button again it will hide the list of actions after you look at them.
- 7. Once you have selected the role you will need to select the Security level from the Security drop down box. When you single click on the drop down box you will see a list of levels. This list may change slightly from one sub module to another. The tips below will help you know what to select. Once you have selected the security level single click the Go button to continue.
 - ➤ HA security administrators will typically select "Field Office HA". For larger PHAs, "Development" may be selected for the Development sub module if a user only needs access to specific developments.
 - ➤ HUD security administrators may select "Hub" for all PHAs in that region or "Field Office" for all PHAs under their field office. Do not select "Field Office HA" since this does not work properly for HUD users. Only security administrators with HQ level security administration access can assign national access.
- 8. What you see in the table at the bottom of the page depends on what security level of access the security administrator has and what was select for the security level for the user being worked on. Do not change the HQ Office or HQ Division drop down boxes if they are present. Make the appropriate selections from the hub, field office, and field office HA boxes as necessary. When you make a selection in the hub or field office drop down boxes you will need to use the Go button to cause the page to refresh and show you an updated list of choices. This is where you would select more than one entity if needed. When you are finished, single click the Save button to finish assigning the role to the user.



Add Role – Security level selection for the selected role



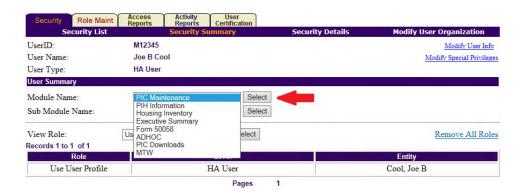
Security Administration Summary – shows the role just assigned

9. You will repeat steps 2-8 to assign additional roles to this user. When you have completed your work remember to log out of PIC using the Logoff link and to also log out of Secure Systems.

Removing User Roles

When a user changes jobs, takes on additional responsibilities, or no longer needs to be able to do tasks in the system their access needs to be modified to reflect this. It is important for security administrators to always ensure that users only have the amount of access they need to accomplish their job functions.

- 1. In the Security Administration sub module, single click on the user ID for the user you wish to the modify access for.
- 2. On the Security Administration Summary page single click on the Module Name drop down box to see the list of modules you can navigate to. Single click on the module name and then single click on the Select button to refresh the page.
 - ➤ If you do not see the name of a module you need to maintain access for it is because you do not have it and therefore cannot assign access to it. Please consult with another security administrator at your PHA, if there is one, to see if it should be assigned to you or if they can assign that role or contact your local PIC coach for assistance.

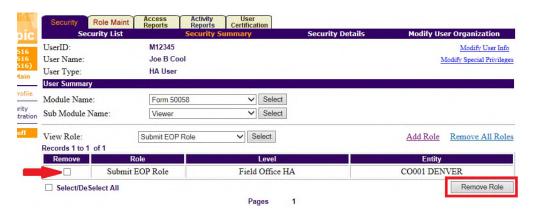


- 3. Single click on the Sub Module Name drop down box to see the list of sub modules you can navigate to. Single click on the sub module name and then single click on the Select button to refresh the page.
 - ➤ If you do not see the name of a sub module you need to maintain access for it is because you do not have it and therefore cannot assign access to it. Please consult with another security administrator at your PHA, if there is one, to see if it should be assigned to you or if they can assign that role or contact your local PIC coach for assistance.



4. When the page refreshes you will be able to see if there is already a role assigned to the user for this sub module. If you see a role that the user no longer needs, single click on the Remove checkbox to place a checkmark in it. Then single click the Remove Role button to remove the role. You will see

a pop-up message box that asks you to confirm that you want to delete the role. Single click on OK to confirm or cancel if you do not want to take this action.



5. The page will refresh and you will see the message "No roles defined". *If you do not see this message it most likely means that more than one role was assigned. If you also need to remove this role you would repeat step 4 until you see the "No roles defined" message.*

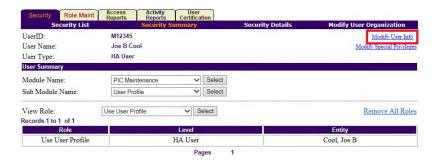


Terminating User Access

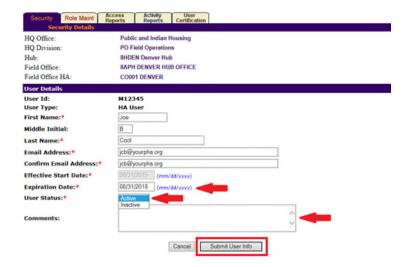
If a user no longer needs access to PIC, the security administrator should terminate their access to the system. In PIC, users are made inactive when they no longer require access so that we retain the history that the user was active at one point. If a user no longer needs access to other systems, including Secure Systems, those should be handled according to the procedures for that system.

Notes about users with EIV access:

- Access must first be terminated in EIV before a user is made inactive in PIC. If this is not done, this will cause an issue in EIV.
- This also applies to users who are only in PIC to access to the EIV system (aka "EIV only" users). If EIV access is terminated for an "EIV only" user, then access would need to be terminated in PIC as well.
- If a user that previously had access to sub modules in PIC and has access to EIV no longer needs access to the sub modules in PIC, but will remain an EIV user, follow the steps for removing the user's roles all roles would be removed. This will keep the user in PIC, which is required to have EIV access, but they will not have access to any data in PIC. View the User Security Access Report to make sure that the only role assigned is the User Profile role.
- 1. In the Security Administration sub module, single click on the user ID for the user you wish to terminate access for.
- 2. On the Security Administration Summary page single click on the Modify User Info link.



- 3. On the Security Details page, you must input data into two fields and can optionally input data into one other field. These fields are as follows and are highlighted in the screen print below.
 - > Change the Expiration Date to the current date. The system will not let you enter a date prior to today's date. It can be set to a future date if you are trying to begin this process in advance but you will still need to return to this page on that date to finish the rest of the entries so that is not recommended.
 - ➤ Change the User Status drop down box to Inactive.
 - Enter any comments that may be useful about the user's status, such as the date that access was no longer needed if it is prior to the current date. These can be useful if someone needs to maintain this user in the future. It is also useful to include the date you are entering the comments at the beginning of the comment. An example may be "09/08/15 no longer employed at PHA as of 08/31/15."



- 4. Once you have completed your entries single click on the Submit User Info button to save the change.
- 5. The page will refresh and show the Security Administration Summary page. Single click on the Security tab at the top of the page to go back to the Security Administration List page. You should no longer see the user listed in the list of active users, which is what is displayed by default.

Modifying User Details and Editing Expiration Dates

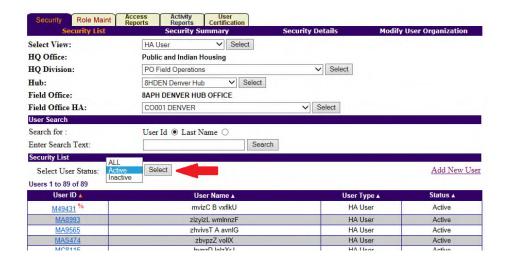
Each user can edit their user details – name, email address, phone number, etc. – by accessing their user profile. This page can be accessed by single clicking on the User Profile sub module link under the PIC Maintenance module on the PIC Main page. Because of this, security administrators (both PHA and HUD) should not need to assist with these changes.

Only a security administrator can edit a user's expiration date. The expiration date is a legacy field from when PIC did not utilize single sign on through Secure Systems. Due to lack of resources we have been unable to remove this field; therefore, we must continue to ensure this date is a future date for users to be able to access the system. There are three reasons why an expiration date may need to be changed. The first reason is because the expiration date is approaching in the near future and the user still requires access. The date can be extended up to three users in the future, depending on the status of the user's employment and/or need to have access. It is strongly suggested that security administrators have some way of keeping track of what they input for the user account expiration date for each user so that they can maintain these dates in an orderly fashion to prevent interruption of access for the users in their entity.

The other two reasons involve reactivating a user's access. There are two instances when you may need to reactivate a user. First, once the expiration date is reached the user will receive a message that says their access is expired when they try to access PIC. Second, there are times when a user's access may have been terminated (made inactive) because it was no longer needed but now due to a change in job and/or job duties at the same entity access is needed again.

Updating the expiration date or reactivating a user:

- 1. In the Security Administration sub module, single click on the user ID for the user you wish to edit the expiration date for.
 - If the user's access has expired, you will see (exp) next to their user ID.
 - ➤ If the user's access was previously terminated (by making them an inactive user) you will need to navigate to the inactive user list by selecting Inactive from the Select User Status drop down box and single click the Select button. The page will refresh and you should see the user listed.



2. On the Security Administration Summary page single click on the Modify User Info link.



- 3. On the Security Details page, you will need to input a new expiration date. It can be up to three years in the future depending on the status of the user's employment and/or need to have access. If you are reactivating a terminated user, you also need to select Active from the User Status drop down box. While the Comments field is not required it can be helpful when maintaining a user in the future. Enter comments if you think they would be helpful, but do not delete any comments that are already present. Simply add the new text at the end and include the date you are entering the comments.
- 4. Once you have completed your entries single click on the Submit User Info button to save the change.



5. The page will refresh and show the Security Administration Summary page. If you were reactivating an expired user, you have completed this task. If you were reactivating an inactive (terminated) user, you should view the User Security Access Report under the Access Reports tab to see which roles were previously assigned to the user. Information on how to access this report is found in a separate section of this document. You can then add and/or remove roles from the user depending on what access they need now. Please see the applicable sections of this document for further information on how to perform these steps.

Modify Special Privileges - Unmask Privacy Data (PII)

By default, when a user is added in PIC privacy act data, including Social Security Number (SSN), first name, and date of birth (DOB) are masked so that only a portion of it is visible. This was enacted in response to an OIG audit finding. The security administrator at a PHA can unmask tenant data for a user by following the steps below. This should be done sparingly since HUD does not want all users at a PHA to have this level of access. The exception could be a very small PHA. Documentation should be kept in a secured location as to who has access to unmasked tenant data and the justification as to why it is needed to complete work in the system. For HUD staff, there is a limit to two staff per field office. Only a HUD super user in HQ can grant this access after it has been approved by management in the user's network.

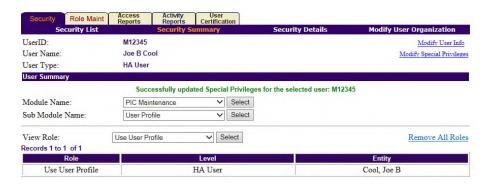
- 1. In the Security Administration sub module, single click on the user ID for the user you wish to unmask privacy data for.
- 2. On the Security Administration Summary page single click on the Modify Special Privileges link.



3. Single click the checkbox next to View Unmasked Privacy Data. Then single click on the Save Special Privileges button to save the change.



 You will be taken back to the Security Administration Summary page and will see a confirmation message that states, "Successfully updated Special Privileges for the selected user: M_____" (for a HUD user it would say H_____).



Security Reports and Monitoring Access

There are several reports available to security administrators to enable them to monitor user access and know what access a user has. The reports are divided into two areas, Access Reports and Activity Reports. The names and descriptions of the reports are listed below.

The reports available under the Access Reports tab are:

- User Security Access This report lists user identification information and a detailed view of what roles are assigned to the user in each module and sub module. It also lists the actions a user can complete for each role they are assigned.
- Privacy Act Access The report lists users who have accessed data protected by the Privacy Act and what page the data was located on in the system.
- Global User Search Use this feature to search for a PIC user if you believe they are listed under another PHA or HUD field office.
- User Access by Submodule This report lists users who have access to a specific sub module and the role that is assigned to the user.

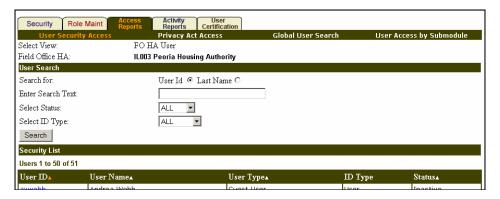
The reports available under the Activity Reports tab are:

- User Activity Query The report provides detailed information about each time the selected user was logged into the system during the timeframe specified. The information included is the date and time, web browser used, IP address (if detected), which of the PIC servers the user was logged into, activity status, and the length of the session.
- New Users This report lists users that were added to the system during the specified timeframe.
- Improper Logoff The report provides detailed information about connections to the PIC system terminated by an action other than using the Logoff link. It lists the user name, user ID, web browser, date and time for the login session, and description for why connection was terminated
- User Account Usage This report lists users who have not accessed the system within the specified timeframe.

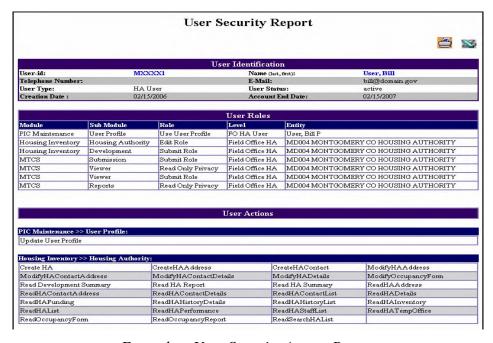
These reports can be accessed by single clicking on the applicable tab on the top of the page in the Security Administration sub module. The following pages will provide some additional details on accessing each report.

User Security Access Report

- 1. Single click on the Access Reports tab at the top of the page. The User Security Access report page is the default page displayed.
- 2. Locate the user in the Security List at the bottom of the page. If you have trouble finding the user, you may need to apply search criteria to narrow down the list. This can be done by:
 - ✓ Single click the User ID or Last Name radio button. Then type all or part of the ID or last name in the Enter Search Text textbox.
 - ✓ You can select the user status active or inactive from the Select Status drop down box. If you are unsure or have entered information in the Enter Search Text textbox you can leave this at the default of All.
 - ✓ You do not need to make a selection from the Select ID Type drop down box.
 - ✓ When all criteria have been entered single click the Search button.
- 3. Once you have located the user ID in the list single click on the user ID link to generate the report in a new browser window.



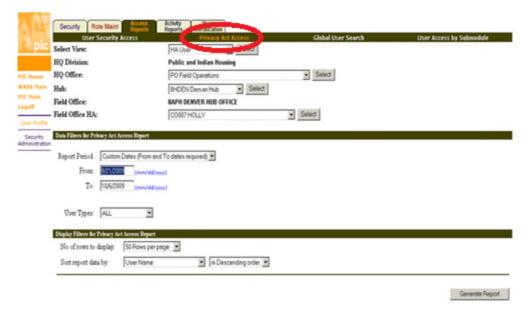
User Security Access report selection criteria



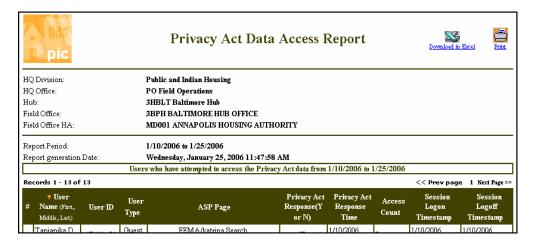
Example – User Security Access Report

Privacy Act Access Report

- 1. Single click on the Access Reports tab at the top of the page. When the page refreshes single click on the Privacy Act Access link.
- 2. Select a pre-defined report range from the Report Period dropdown box or use the Custom Dates option to type dates in the From and To fields.
- 3. Select the user type from the User Type dropdown box or leave it at All to get all results under your PHA or field office.
- 4. If desired, select the options you desire under the Display Filters for Privacy Act Access Report heading, or you may accept the defaults.
- 5. Single click the Generate Report button to open the report in a new browser window.



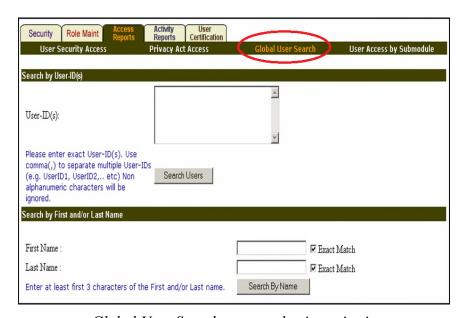
Privacy Act Access report selection criteria



Example - Privacy Act Access Report

Global User Search Report

- 1. Single click on the Access Reports tab at the top of the page. When the page refreshes single click on the Global User Search link.
- 2. Determine if you want to search by user ID or by name.
 - ➤ If you want to search by user ID enter the user ID in the User ID(s) textbox. Ensure that you use capital letters for the letters. If you want to search for more than one user, you will enter them with a comma between each one do not include a space after the comma.
 - ➤ If you want to search by name enter at least three characters in the first name or last name or both. If you are not entering a full name mark sure to uncheck the Exact Match checkbox.
- 3. After you have entered your search criteria single click on the Search Users button to search by user ID or the Search By Name button to search by name. The report will open in a new browser window.



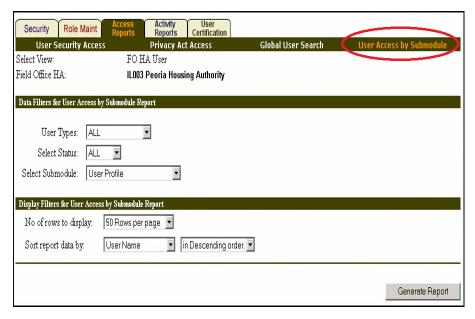
Global User Search report selection criteria



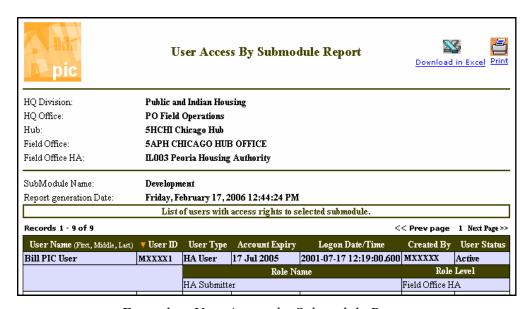
Example - Global User Search Report

User Access by Submodule Report

- 1. Single click on the Access Reports tab at the top of the page. When the page refreshes single click on the User Access by Submodule link.
- 2. Select the data filters for the report. You will need to select the user type, user status, and the sub module that you want to view information for. This will only display information for the entity that you previously navigated to.
- 3. Select the display filters for the report or accept the defaults.
- 4. Single click on the Generate Report button to open the report in a new browser window.



User Access by Submodule report selection criteria



Example - User Access by Submodule Report

User Activity Query

- 1. Single click on the Activity Reports tab at the top of the page. The User Activity Query report page is the default page displayed.
- 2. Locate the user in the Security List at the bottom of the page but do not click on the user ID yet. If you have trouble finding the user, you may need to apply search criteria to narrow down the list. This can be done by:
 - ✓ Single click the User ID or Last Name radio button. Then type all or part of the ID or last name in the Enter Search Text textbox.
 - ✓ You can select the user status active or inactive from the Select Status drop down box. If you are unsure or have entered information in the Enter Search Text textbox you can leave this at the default of All.
 - ✓ When all criteria have been entered single click the Search button.
- 3. Enter the date range you want to view data for under the Activity Period header.
- 4. Once you have located the user ID in the list single click on the user ID link to generate the report in a new browser window.



User Activity Query report selection criteria

User Activity Information

Selected View: HA User

HQ Office: Public and Indian Housing HQ Division: PO Field Operations 7HKNC Kansas City Hub 7DPH OMAHA PROGRAM CENTER Hub:

Field Office:

Field Office HA: NE001 OMAHA

Report Start Date: 8/10/2015 Report End Date: 9/10/2015

First Name: Last Name: Middle Initial: Phone Number: Phone Number Extn: E-Mail Address: @ohauthority.org



Activity Report

Summary Report

Total Connect Time		Total Number of Logins	Average Connect Time					
	10:42:8	34	0:18:53					

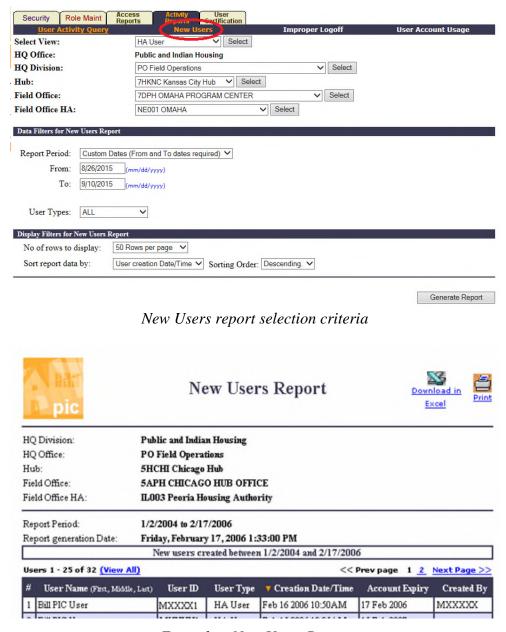
Detailed Report

Sr No.	Date	Operating System	Browser Name/Version	Client IP Address	Web Server Name	Activity Status	Login Begin	Login End	Total Time Logged On
1	09/10/2015 10:59:21	Windows NT	Internet Explorer 9.0		HWVANWP3613	CRRNT	09/10/2015 10:59:21	*	*
2	09/10/2015 09:55:41	Windows NT	Internet Explorer 9.0		HWVANWP3613	LOGOFF	09/10/2015 09:55:41	09/10/2015 10:28:12	0:32:31

Example – User Activity Query Report

New Users Report

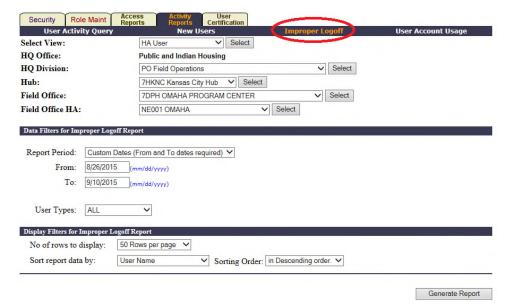
- 1. Single click on the Activity Reports tab at the top of the page. When the page refreshes single click on the New Users link.
- 2. Select a pre-defined report range from the Report Period dropdown box or use the Custom Dates option to type dates in the From and To fields.
- 3. Select the user type from the User Type dropdown box or leave it at All to get all results under your PHA or field office.
- 4. If desired, select the options you desire under the Display Filters for New Users Report heading, or you may accept the defaults.
- 5. Single click the Generate Report button to open the report in a new browser window.



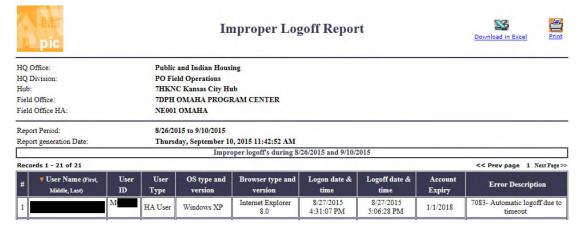
Example – New Users Report

Improper Logoff Report

- 1. Single click on the Activity Reports tab at the top of the page. When the page refreshes single click on the Improper Logoff link.
- 2. Select a pre-defined report range from the Report Period dropdown box or use the Custom Dates option to type dates in the From and To fields.
- 3. Select the user type from the User Type dropdown box or leave it at All to get all results under your PHA or field office.
- 4. If desired, select the options you desire under the Display Filters for Improper Logoff Report heading, or you may accept the defaults.
- 5. Single click the Generate Report button to open the report in a new browser window.



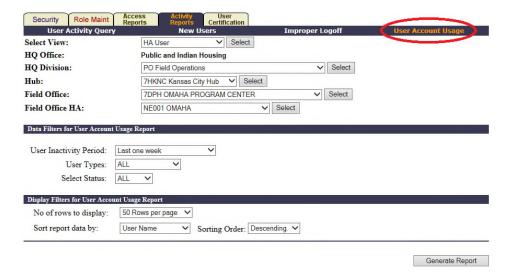
Improper Logoff report selection criteria



Example – Improper Logoff Report

User Account Usage Report

- 1. Single click on the Activity Reports tab at the top of the page. When the page refreshes single click on the User Account Usage link.
- 2. Select a pre-defined report range from the User Inactivity Period dropdown box.
- 3. Select the user type from the User Type dropdown box or leave it at All to get all results under your PHA or field office.
- 4. Select the user status from the Select Status drop down box.
- 5. If desired, select the options you desire under the Display Filters for User Account Usage Report heading, or you may accept the defaults.
- 6. Single click the Generate Report button to open the report in a new browser window.



User Account Usage report selection criteria



Example – User Account Usage Report

Appendix: Sub Module Access Descriptions

Below is a description of each sub module in the PIC system. In each sub module there are varying levels of access that can be given to a specific user, which will affect whether they can view (read only), edit, submit, or approve data. Some sub modules will not have all these choices; it is dependent upon the content and functions available in that area and whether the user is an HA or HUD user.

Module name: PIC Maintenance

- User Profile allows the user to edit their user profile, which contains the user's name, address, phone number, and email address.
- Reference used by select HUD users that are setup as super users to perform administrative tasks in the system.
- Security Administration allows the user to add users and maintain PIC access for users in their jurisdiction.

Module name: PIH Information

- SEMAP used by PHAs administering the Housing Choice Voucher (Section 8) program to complete and submit their SEMAP (Section Eight Management Assessment Program) certifications. Also used by HUD staff to score SEMAP profiles and monitor PHA performance.
- Risk Assessment for HUD users only, this is no longer used and access should not be provided.
- DIS Disaster Information System, used by PHA and HUD users to maintain households receiving assistance under a disaster voucher.

Module name: Housing Inventory

- Housing Authority enables the user to maintain housing authority information, HA Contacts, and view other details about a PHA.
- Development allows a user to view and maintain the building and unit information for each of the developments in their housing authority. The user can also view the various building and unit reports. HUD super users can make modifications to some data not editable by other users with supporting documentation.
- Inventory Removals allows a user to view, create and submit Demolition/Disposition applications. Also allows user to create and submit transactions to remove land/buildings/units from inventory.

Module name: Executive Summary

• HA Executive Summary – allows a user to view the Executive Summary, which contains various types of information about a housing authority.

<u>Module name: Form-50058</u>. May or may not be used by MTW PHAs depending on their agreement with HUD and other factors listed below.

- Submission allows a user can submit files from vendor software that contain Form-50058 data. Users can view the resulting error reports as well.
- Viewer allows a user to view the Form-50058 data that has been successfully submitted without fatal errors in the Form-50058 Submission sub module. Users who have been given submit access can submit an EOP online if they are unable to use their software to do it (this function is a last resort to do an EOP). A user also has access to Form-50058 reports such as

- MTCS Transaction Report, Portability Billing Report, Overlapping Date Report, etc. *The Portability Billing Report and Overlapping Date Report will contain some data for MTW PHAs.*
- Reports allows a user to view the Form-50058 monthly reports that are generated and available
 in PIC each month including but not limited to the Delinquency Report, Reexamination Report,
 HQS Inspection Report, and SEMAP Indicators Report.
- Tenant ID Management allows a user to generate alternate IDs (AIDs) for tenants (head of household and household members) that do not have a valid Social Security Number (SSN). Users can also replace an AID with an SSN, correct an invalid SSN, and correct data in a previously generated AID. Reports that can be viewed include the AID Report, Possible Duplicate Report, and Invalid Tenant ID Report.

Module name: Adhoc

- Form 50058 Adhoc Report this is a customizable report that includes information on households that have been submitted on the Form-50058 to PIC. This report only displays data on Form-50058s that were submitted in the Form-50058 Submission sub module and are present in the current database. Historical information from previous Form-50058 submissions is not available.
- MTW Adhoc Report this is a customizable report that includes information on households that have been submitted on the MTW Form-50058 to PIC. This report only displays data on Form-50058s that were submitted in the MTW Data Collection sub module and are present in the current database. Historical information from previous Form-50058 submissions is not available.
- HA Query Report this is a read only report that allows a user to see if an SSN is the head of household on a Form-50058 in the current database. It does not search household members or the historical database.

Module name: PIC Downloads

• Building and Unit – allow a user to download a current set of building data or unit data for analysis in the standard building and unit spreadsheet format. Note that the format that data is downloaded in does not match the current B&U template. It is recommended that access not be provided to this sub module to avoid confusion. Building and unit data details are available in the Development sub module.

Module name: MTW

- Data Collection allows MTW agencies to submit tenant data on the MTW Form-50058. This is done by CSV or Excel file submission or online data entry.
- Viewer allows a user to view the Form-50058 data that has been successfully submitted without fatal errors in the Data Collection sub module.
- Reports allows a user to view the MTW Delinquency Report. This report is generated at the same time as the reports in the Form-50058 Reports sub module.

Appendix: Adding the PIC Link to the Secure Systems Main Menu

The steps below are to be done by a PHA's Secure Systems coordinator. HUD staff should not be doing this function for PHAs. If a PHA only has one user, the Secure Systems coordinator, that user can assign the role to themselves. For HUD staff, this is should be completed when the DIAMS system request for a new IMS-PIC user is processed.

- 1. The PHA's Secure Systems coordinator should access User Maintenance in WASS and search for the user.
- 2. If the search was done by user ID, the user's information will appear. If the search was done by name, single click on the user ID for the user.

Note: If the Secure Systems coordinator is assigning access to themselves, before doing step 3 below they will first need to do the following to see the PIC system in User Maintenance.

- 1. Select Maintain User Profile Actions and single click the Submit button.
- 2. Under the PIC PIC System heading, single click the checkbox to the left of Administration.
- 3. Single click the Assign/Unassign Actions button at the bottom of the page. When prompted, single click OK to confirm.
- 4. Go back to Step 3 to do the role assignment.
- 3. From the Choose a Function dropdown box, select Maintain User Profile Roles. Single click the Submit button.
- 4. Under the PIC PIC System heading, single click the checkbox to the left of PIC PIC Generic.
- 5. At the bottom of the page, single click the Assign/Unassign Roles button. If prompted, confirm the assignment on the next page.