



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.

PIH Information Center (PIC)
IMS-PIC Release 8.1

Welcome M00516 (M00516)! Your last logon was on Aug 26 2015 9:21AM.
Your user id was certified on 08/17/2015.

PIC Maintenance	PIC Headlines
<ul style="list-style-type: none">User ProfileSecurity Administration	<ul style="list-style-type: none">50058 Summarization this weekend - 11/12/2014 Monthly Summarization to run Nov. 14th [full text]Form-50058 summarization not run - 11/10/2014 Form-50058 monthly summarization did not run [full text]Vendor Conference Call - 7/1/2014 Conference Call to discuss the Rental Assistance Demonstration Program [full text]
PIH Information <ul style="list-style-type: none">SEMAPDIS	Browse all PIC Headlines.
Housing Inventory <ul style="list-style-type: none">Housing AgencyDevelopmentInventory Removals	PICHELP information
Executive Summary <ul style="list-style-type: none">HA Executive Summary	<p>PICHELP: If you require any assistance please send an email describing the issue along with your Name, Phone Number, Housing Authority Number and Field Office Name where applicable to REAC_TAC@hud.gov or telephone the Technical Assistance Center (TAC) at 1-888-245-4860 between 7:00am and 8:30pm Eastern on business days. All PIC password resets are handled by Security Administrators at the PHA or in the local HUD Field Office. The REAC TAC cannot reset passwords.</p>
Form 50058 <ul style="list-style-type: none">SubmissionViewerReportsTenant ID Management	
ADHOC <ul style="list-style-type: none">Form 50058 Adhoc ReportMTW Adhoc ReportHA Query Report	
PIC Downloads	

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.

Security | Role Maint | Access Reports | Activity Reports | User Certification

Security List

Select View: HA User

HQ Office: Public and Indian Housing

HQ Division: PO Field Operations

Hub: 8HDEN Denver Hub

Field Office: 8APH DENVER HUB OFFICE

Field Office HA: CO001 DENVER

User Search

Search for: User Id ☒ Last Name ☐

Enter Search Text:

Security List

Select User Status: Active

[Add New User](#)

Users 1 to 89 of 89

User ID ▲	User Name ▲	User Type ▲	Status ▲
MA9431 ^{9a}	mvizC B vxfikU	HA User	Active
MA8993	zizyzL wmlnznF	HA User	Active
MA9555	zhvvsT A avnIG	HA User	Active
MA9474	zbvypZ volIX	HA User	Active
MC8115	hvnzD lolzXrJ	HA User	Active

- 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.

Security | Role Maint | Access Reports | Activity Reports | User Certification

Security Details

HQ Office: Public and Indian Housing

HQ Division: PO Field Operations

Hub: 8HDEN Denver Hub

Field Office: 8APH DENVER HUB OFFICE

Field Office HA: CO001 DENVER

New user Details

User Type: HA User

User Id: M12345

First Name: Joe

Middle Initial: B

Last Name: Cool

Email Address: jcb@yourpha.org

Confirm Email Address: jcb@yourpha.org

Effective Start Date: 8/31/2015 (mm/dd/yyyy)

Expiration Date: 8/31/2018 (mm/dd/yyyy)

User Status: Active

Comments:

- 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.
- 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.

Security

Role Maint

Access Reports

Activity Reports

User Certification

Security List

Security Summary

Security Details

Modify User Organization

UserID:

M12345

[Modify User Info](#)

User Name:

Joe B Cool

[Modify Special Privileges](#)

User Type:

HA User

User Summary

Module Name:

PIC Maintenance

Select

Sub Module Name:

User Profile

Select

View Role:

Use User Profile

Select

[Remove All Roles](#)

Records 1 to 1 of 1

Role	Level	Entity
Use User Profile	HA User	Cool, Joe B

Pages

1

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 – **only one role should be assigned per sub module** 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.

Security	Role Maint	Access Reports	Activity Reports	User Certification						
Security List Security Summary Security Details Modify User Organization										
User ID:	M12345									
User Name:	Joe B Cool									
User Type:	HA User									
Modify User Info										
Modify Special Privileges										
User Summary										
Module Name:	<div>PIC Maintenance PIH Information Housing Inventory Executive Summary Form 50058 ADHOC PIC Downloads MTW</div>									
Sub Module Name:	<div>Select</div>									
View Role:	<div>Us</div>									
Records 1 to 1 of 1	<div>select</div>									
Remove All Roles										
<table border="1"><thead><tr><th>Role</th><th>Entity</th></tr></thead><tbody><tr><td>Use User Profile</td><td>Cool, Joe B</td></tr><tr><td>HA User</td><td></td></tr></tbody></table>					Role	Entity	Use User Profile	Cool, Joe B	HA User	
Role	Entity									
Use User Profile	Cool, Joe B									
HA User										
Pages 1										

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.

The screenshot shows the 'Security Summary' page for user M12345 (Joe B Cool, HA User). The 'Module Name' is set to 'Form 50058'. The 'Sub Module Name' dropdown is open, showing options: 'Submission', 'Viewer', 'Reports', and 'Tenant ID Management'. A red arrow points to the 'Submission' option, and another red arrow points to the 'Select' button next to it. Below the dropdown, there are links for 'Add Role' and 'Remove All Roles'. At the bottom, a table header is visible with columns: 'Remove', 'Role', 'Level', and 'Entity'. The text 'No Roles Defined.' is displayed below the table header.

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.

The screenshot shows the 'Role/Data Details' page. The 'Available Roles' dropdown is set to 'Read Only Role', and the 'Security' dropdown is set to 'HQ Office'. Red arrows point to the 'Go' buttons next to both dropdowns. A 'View Actions' button is also visible. Below the dropdowns, there is a table with two columns: 'Field Names' and 'Key Value'. The 'Field Names' column contains 'HQ Office', and the 'Key Value' column contains 'Public and Indian Housing'. A red arrow points from the 'Field Names' column to the 'Key Value' column. At the bottom right, there is a 'Save' button highlighted with a red box.

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.

Security		Role Maint		Access Reports		Activity Reports		User Certification	
Security List		Security Summary		Security Details		Modify User Organization			
User ID:	M12345								
User Name:	Joe B Cool								
User Type:	HA User								
Module Name:	Form 50058								
Sub Module Name:	Viewer								
Role/Data Details									
Available Roles:		Submit EOP Role		Go		View Actions			
Security:		Field Office HA		Go					
Field Names		Key Value							
HQ Office		Public and Indian Housing							
HQ Division		PO Field Operations							
Hub		10HSEA Seattle Hub							
Field Office		0APH SEATTLE HUB OFFICE							
Field Office HA		AK001 AHFC - MTW PH AK901 AHFC - MTW VO ID001 Twin Falls ID002 Nampa ID005 Pocatello ID007 COEUR D'ALENE TRIBAL HA ID008 NEZ PERCE TRIBAL HA ID009 FORT HALL HA ID010 Buhl ID011 Jerome							
<input type="checkbox"/> Select/Deselect All									
<div style="text-align: right;">Save</div>									

Add Role – Security level selection for the selected role

Security	Role Maint	Access Reports	Activity Reports	User Certification
Security List		Security Summary		Security Details
Modify User Organization				
UserID:	M12345			Modify User Info
User Name:	Joe B Cool			Modify Special Privileges
User Type:	HA User			
User Summary				
Module Name:	Form 50058	▼	Select	
Sub Module Name:	Viewer	▼	Select	
View Role:	Submit EOP Role	▼	Select	Add Role Remove All Roles
Records 1 to 1 of 1				
Remove	Role	Level	Entity	
<input type="checkbox"/>	Submit EOP Role	Field Office HA	CO001 DENVER	
<input type="checkbox"/> Select/DeSelect All				
Remove Role				
Pages 1				

Security Administration Summary – shows the role just assigned

- 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.

The screenshot shows the 'Security Administration Summary' page. At the top, there are tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below these are sections: Security List, Security Summary, Security Details, and Modify User Organization. The 'Security Summary' section displays user information: UserID: M12345, User Name: Joe B Cool, and User Type: HA User. There are links for 'Modify User Info' and 'Modify Special Privileges'. Below this is the 'User Summary' section. It has a 'Module Name' dropdown menu that is open, showing a list of modules: PIC Maintenance, PIH Information, Housing Inventory, Executive Summary, Form 50058, ADHOC, PIC Downloads, and MTW. A red arrow points to the 'Select' button next to the dropdown. There is also a 'Sub Module Name' dropdown and another 'Select' button. At the bottom, there is a table with columns 'Role' and 'Entity'. The table shows 'Use User Profile' for the role and 'Cool, Joe B' for the entity. The page number '1' is at the bottom.

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.

The screenshot shows the 'Security Administration Summary' page, similar to the previous one. The 'Module Name' dropdown is now set to 'Form 50058'. The 'Sub Module Name' dropdown is open, showing a list of sub-modules: Submission, Viewer, Reports, and Tenant ID Management. A red arrow points to the 'Select' button next to the dropdown. At the bottom, there is a table with columns 'Remove', 'Role', 'Level', and 'Entity'. The table is empty, and the text 'No Roles Defined.' is displayed. There are links for 'Add Role' and 'Remove All Roles'.

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.

Security | **Role Maint** | Access Reports | Activity Reports | User Certification

Security List | **Security Summary** | Security Details | Modify User Organization

UserID: M12345 [Modify User Info](#)
 User Name: Joe B Cool [Modify Special Privileges](#)
 User Type: HA User

User Summary

Module Name: Form 50058
 Sub Module Name: Viewer

View Role: Submit EOP Role [Add Role](#) [Remove All Roles](#)

Records 1 to 1 of 1

Remove	Role	Level	Entity
<input type="checkbox"/>	Submit EOP Role	Field Office HA	CO001 DENVER

☐ Select/De Select All

Pages 1

- 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.*

Security | **Role Maint** | Access Reports | Activity Reports | User Certification

Security List | **Security Summary** | Security Details | Modify User Organization

UserID: M12345 [Modify User Info](#)
 User Name: Joe B Cool [Modify Special Privileges](#)
 User Type: HA User

User Summary

Module Name: Form 50058
 Sub Module Name: Viewer

View Role: Submit EOP Role [Add Role](#) [Remove All Roles](#)

Remove	Role	Level	Entity
No Roles Defined.			

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.

The screenshot shows the 'Security Administration Summary' page for user M12345. The page has a navigation bar with tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. The main content area is divided into sections: Security List, Security Summary, Security Details, and Modify User Organization. The Security Summary section displays user information: UserID: M12345, User Name: Joe B Cool, and User Type: HA User. Below this is the 'User Summary' section with dropdown menus for Module Name (PIC Maintenance) and Sub Module Name (User Profile), each with a 'Select' button. At the bottom, there is a 'View Role' dropdown (Use User Profile) and a 'Remove All Roles' link. A table at the bottom shows the user's roles:

Role	Level	Entity
Use User Profile	HA User	Cool, Joe B

Pages 1

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."

Security		Role Maint	Access Reports	Activity Reports	User Certification
Security Details					
HQ Office:	Public and Indian Housing				
HQ Division:	PO Field Operations				
Hub:	BHDEN Denver Hub				
Field Office:	BAPH DENVER HUB OFFICE				
Field Office HA:	CO001 DENVER				
User Details					
User Id:	M12345				
User Type:	HA User				
First Name:	<input type="text" value="Joe"/>				
Middle Initial:	<input type="text" value="B"/>				
Last Name:	<input type="text" value="Cool"/>				
Email Address:	<input type="text" value="jcb@yourpha.org"/>				
Confirm Email Address:	<input type="text" value="jcb@yourpha.org"/>				
Effective Start Date:	<input type="text" value="08/31/2015"/> (mm/dd/yyyy)				
Expiration Date:	<input type="text" value="08/31/2018"/> (mm/dd/yyyy)				
User Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive				
Comments:	<input type="text"/>				
<input type="button" value="Cancel"/> <input type="button" value="Submit User Info"/>					

- Once you have completed your entries single click on the Submit User Info button to save the change.
- 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.

Security Administration sub module interface showing the 'Security List' tab. The 'Select User Status' dropdown is open, showing 'ALL', 'Active', and 'Inactive' options. A red arrow points to the 'Inactive' option. Below the dropdown is a table of users with columns: User ID, User Name, User Type, and Status. The table lists four users: MA9431, MA8993, MA9565, and MAS474, all with status 'Active'.

User ID	User Name	User Type	Status
MA9431	mvizC B vxflkU	HA User	Active
MA8993	zizyizL wmlnzzF	HA User	Active
MA9565	zhvivsT A avnlG	HA User	Active
MAS474	zbpvzZ volIX	HA User	Active

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

Security Administration Summary page. The 'Modify User Info' link is highlighted with a red box. The page shows user details for M12345, Joe B Cool, HA User. Below is a 'User Summary' section with dropdowns for Module Name (PIC Maintenance), Sub Module Name (User Profile), and View Role (Use User Profile). A table shows the role 'Use User Profile' at level 'HA User' for entity 'Cool, Joe B'.

Role	Level	Entity
Use User Profile	HA User	Cool, Joe B

- 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.
- Once you have completed your entries single click on the Submit User Info button to save the change.

Security Details page. The 'Submit User Info' button is highlighted with a red box. The page shows user details for M12345, HA User. The 'Expiration Date' is set to 08/31/2018 and the 'User Status' is set to Active. Red arrows point to the 'Expiration Date' and 'User Status' fields. The 'Comments' field is empty.

- 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.

The screenshot shows the 'Security Administration Summary' page for user M12345. The page has a navigation bar with tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below the navigation bar, there are sections for 'Security List', 'Security Summary', 'Security Details', and 'Modify User Organization'. The 'Security Summary' section displays user information: UserID: M12345, User Name: Joe B Cool, and User Type: HA User. To the right of this information, there are two links: 'Modify User Info' and 'Modify Special Privileges'. The 'Modify Special Privileges' link is highlighted with a red box. Below the user information, there is a 'User Summary' section with two dropdown menus: 'Module Name' (set to 'PIC Maintenance') and 'Sub Module Name' (set to 'User Profile'), each with a 'Select' button.

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

The screenshot shows the 'Special Systemwide Privileges' section. It contains a checkbox labeled 'View Unmasked Privacy Data.' which is checked. A red arrow points to this checkbox. Below the checkbox are two buttons: 'Cancel' and 'Save Special privileges'. The 'Save Special privileges' button is highlighted with a red box. The page also includes a link '<< Back to User Security Summary'.

4. 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_____).

The screenshot shows the 'Security Administration Summary' page after the update. A green confirmation message is displayed: 'Successfully updated Special Privileges for the selected user: M12345'. The page layout is similar to the previous screenshots, showing user information and the 'User Summary' section. At the bottom, there is a table with the following data:

Role	Level	Entity
Use User Profile	HA User	Cool, Joe B

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.

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.

Security	Role Maint	Access Reports	Activity Reports	User Certification
User Security Access		Privacy Act Access		Global User Search
Select View:		FO HA User		
Field Office HA:		IL003 Peoria Housing Authority		
User Search				
Search for:		User Id <input checked="" type="radio"/> Last Name <input type="radio"/>		
Enter Search Text:		<input type="text"/>		
Select Status:		<input type="text" value="ALL"/>		
Select ID Type:		<input type="text" value="ALL"/>		
<input type="button" value="Search"/>				
Security List				
Users 1 to 50 of 51				
User ID▲	User Name▲	User Type▲	ID Type	Status▲

User Security Access report selection criteria

User Security Report				
<div>   </div>				
User Identification				
User-id:	MXXXXX	Name (last, first):	User, Bill	
Telephone Number:		E-Mail:	bill@domain.gov	
User Type:	HA User	User Status:	active	
Creation Date :	02/15/2006	Account End Date:	02/15/2007	
User Roles				
Module	Sub Module	Role	Level	Entity
PIC Maintenance	User Profile	Use User Profile	FO HA User	User, Bill P
Housing Inventory	Housing Authority	Edit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
Housing Inventory	Development	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Submission	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Viewer	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Viewer	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Reports	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
User Actions				
PIC Maintenance >> User Profile:				
Update User Profile				
Housing Inventory >> Housing Authority:				
Create HA	CreateHAAAddress	CreateHAAContact	ModifyHAAAddress	
ModifyHAAContactAddress	ModifyHAAContactDetails	ModifyHAADetails	ModifyOccupancyForm	
Read Development Summary	Read HA Report	Read HA Summary	ReadHAAAddress	
ReadHAAContactAddress	ReadHAAContactDetails	ReadHAAContactList	ReadHAADetails	
ReadHAAFunding	ReadHAAHistoryDetails	ReadHAAHistoryList	ReadHAAInventory	
ReadHAAList	ReadHAAPerformance	ReadHAAStaffList	ReadHAAtempOffice	
ReadOccupancyForm	ReadOccupancyReport	ReadSearchHAAList		

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.

Security Administration

Security | Role Maint | Access Reports | Activity Reports | **Privacy Act Access** | Global User Search | User Access by Submodule

Select View: HA User

HQ Division: Public and Indian Housing

HQ Office: PO Field Operations [Select]

Hub: 3HBLT Denver Hub [Select]

Field Office: 3BPH DENVER HUB OFFICE

Field Office HA: C0007 HOLLY [Select]

Data Filters for Privacy Act Access Report

Report Period: Custom Dates (from and to dates required)

From: 1/10/2006 (mm/dd/yyyy)

To: 1/25/2006 (mm/dd/yyyy)

User Types: ALL


Display Filters for Privacy Act Access Report

No. of rows to display: 50 Rows per page



Sort report data by: User Name in Descending order

[Generate Report](#)

Privacy Act Access report selection criteria



Privacy Act Data Access Report


[Download in Excel](#)

[Print](#)

HQ Division:

HQ Office:

Hub:

Field Office:

Field Office HA:

Public and Indian Housing

PO Field Operations

3HBLT Baltimore Hub

3BPH BALTIMORE HUB OFFICE

MD001 ANNAPOLIS HOUSING AUTHORITY

Report Period:

Report generation Date:

1/10/2006 to 1/25/2006

Wednesday, January 25, 2006 11:47:58 AM

Users who have attempted to access the Privacy Act data from 1/10/2006 to 1/25/2006

Records 1 - 13 of 13

<< Prev page

1

Next Page >>

#	<div>▼ User</div> <div>Name (First, Middle, Last)</div>	User ID	User Type	ASP Page	Privacy Act Response(Y or N)	Privacy Act Response Time	Access Count	Session Logon Timestamp	Session Logoff Timestamp
1	Tanjanika D.		Guest	EFMA/katrina Search		1/10/2006		1/10/2006	1/10/2006

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.

The screenshot shows the 'Global User Search' tab selected in the top navigation bar. Below the navigation bar, there are two main search sections. The first section, 'Search by User-ID(s)', has a text input field for 'User-ID(s)' and a 'Search Users' button. A note below the field states: 'Please enter exact User-ID(s). Use comma(,) to separate multiple User-IDs (e.g. UserID1, UserID2,... etc) Non alphanumeric characters will be ignored.' The second section, 'Search by First and/or Last Name', has input fields for 'First Name' and 'Last Name', each with an 'Exact Match' checkbox. A note below these fields states: 'Enter at least first 3 characters of the First and/or Last name.' There is a 'Search By Name' button at the bottom of this section.

Global User Search report selection criteria

The screenshot shows the 'Global User Search Report' header with a 'pic' logo on the left and 'Download in Excel' and 'Print' links on the right. Below the header, a section titled 'Details of the users found in system' shows the search criteria: 'Search criteria: User-ID(s) = MXXXXX,MXXXX1'. Below this, a table lists the users found in the system.

2 User(s) found in the System :							
#	User-ID(s)	User Type	Full Name	Organization	Entity	Active?	Effective end date
1	MXXXX1	HA User	Bill PIC User	Field Office HA	IL003 Peoria Housing Authority	Y	02/15/2007
2	MXXXXX	HA User	Another Test User	Field Office HA	CT002 Norwalk Housing Authority	Y	02/08/2007

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 submodule 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.

Security Role Maint **Access Reports** Activity Reports User Certification

User Security Access Privacy Act Access Global User Search **User Access by Submodule**

Select View: FO HA User
Field Office HA: IL003 Peoria Housing Authority

Data Filters for User Access by Submodule Report

User Types: ALL
Select Status: ALL
Select Submodule: User Profile

Display Filters for User Access by Submodule Report

No of rows to display: 50 Rows per page
Sort report data by: User Name in Descending order

Generate Report

User Access by Submodule report selection criteria

User Access By Submodule Report

Download in Excel Print

HQ Division: **Public and Indian Housing**
 HQ Office: **PO Field Operations**
 Hub: **5HCHI Chicago Hub**
 Field Office: **5APH CHICAGO HUB OFFICE**
 Field Office HA: **IL003 Peoria Housing Authority**

SubModule Name: **Development**
 Report generation Date: **Friday, February 17, 2006 12:44:24 PM**

List of users with access rights to selected submodule.

Records 1 - 9 of 9 << Prev page 1 Next Page >>

User Name (First, Middle, Last)	User ID	User Type	Account Expiry	Logon Date/Time	Created By	User Status
Bill PIC User	MXXXX1	HA User	17 Jul 2005	2001-07-17 12:19:00.600	MXXXXX	Active
		Role Name		Role Level		
		HA Submitter		Field Office HA		

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.

The screenshot displays the 'User Activity Query' interface. At the top, there are tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports' (which is selected), and 'User Certification'. Below these are sub-tabs: 'User Activity Query', 'New Users', 'Improper Logoff', and 'User Account Usage'. The 'User Activity Query' sub-tab is active, showing various selection criteria. These include 'Select View' (set to 'HA User'), 'HQ Office' (set to 'Public and Indian Housing'), 'HQ Division' (set to 'PO Field Operations'), 'Hub' (set to '7HKNC Kansas City Hub'), 'Field Office' (set to '7DPH OMAHA PROGRAM CENTER'), and 'Field Office HA' (set to 'NE001 OMAHA'). Each of these has a 'Select' button. Below these is the 'User Search' section, which includes a 'Search for:' dropdown (set to 'User Id'), a radio button for 'Last Name', an 'Enter Search Text' input field, a 'Select Status' dropdown (set to 'ALL'), and a 'Search' button. The 'Activity Period' section has 'From' and 'To' date pickers set to '8/10/2015' and '9/10/2015' respectively. At the bottom, the 'Security List' section shows 'Users 1 to 50 of 153' and a table with columns: 'User ID', 'User Name', 'User Type', 'ID Type', and 'Status'.



User Activity Query report selection criteria

User Activity Information

Selected View: HA User
HQ Office: Public and Indian Housing
HQ Division: PO Field Operations
Hub: 7HKNC Kansas City Hub
Field Office: 7DPH OMAHA PROGRAM CENTER
Field Office HA: NE001 OMAHA
Report Start Date: 8/10/2015

Report End Date: 9/10/2015

First Name: [REDACTED]
Last Name: [REDACTED]
Middle Initial:
Phone Number: 402 [REDACTED]
Phone Number Extn:
E-Mail Address: [REDACTED]@ohauthority.org

 
Download in Excel. Print Page.

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.

Security Role Maint Access Reports **Activity Reports** User Certification

User Activity Query **New Users** Improper Logoff User Account Usage

Select View: HA User Select

HQ Office: Public and Indian Housing

HQ Division: PO Field Operations Select

Hub: 7HKNC Kansas City Hub Select

Field Office: 7DPH OMAHA PROGRAM CENTER Select

Field Office HA: NE001 OMAHA Select

Data Filters for New Users Report

Report Period: Custom Dates (From and To dates required) Select

From: 8/26/2015 (mm/dd/yyyy)

To: 9/10/2015 (mm/dd/yyyy)

User Types: ALL Select

Display Filters for New Users Report

No of rows to display: 50 Rows per page Select

Sort report data by: User creation Date/Time Select Sorting Order: Descending Select

Generate Report

New Users report selection criteria

New Users Report

Download in Excel Print

HQ Division: Public and Indian Housing

HQ Office: PO Field Operations

Hub: 5HCHI Chicago Hub

Field Office: 5APH CHICAGO HUB OFFICE

Field Office HA: IL003 Peoria Housing Authority

Report Period: 1/2/2004 to 2/17/2006

Report generation Date: Friday, February 17, 2006 1:33:00 PM

New users created between 1/2/2004 and 2/17/2006

Users 1 - 25 of 32 [\(View All\)](#) << Prev page 1 2 Next Page >>

#	User Name (First, Middle, Last)	User ID	User Type	Creation Date/Time	Account Expiry	Created By
1	Bill PIC User	MXXXXX1	HA User	Feb 16 2006 10:50AM	17 Feb 2006	MXXXXXX

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.

Security **Role Maint** **Access Reports** **Activity Reports** **User Certification**

User Activity Query **New Users** **Improper Logoff** **User Account Usage**

Select View: HA User

HQ Office: Public and Indian Housing

HQ Division: PO Field Operations

Hub: 7HKNC Kansas City Hub

Field Office: 7DPH OMAHA PROGRAM CENTER

Field Office HA: NE001 OMAHA

Data Filters for Improper Logoff Report

Report Period: Custom Dates (From and To dates required)

From: 8/26/2015 (mm/dd/yyyy)

To: 9/10/2015 (mm/dd/yyyy)

User Types: ALL

Display Filters for Improper Logoff Report

No of rows to display: 50 Rows per page

Sort report data by: User Name Sorting Order: in Descending order.

Improper Logoff report selection criteria

<div> Improper Logoff Report Download in Excel Print </div>									
HQ Office:		Public and Indian Housing							
HQ Division:		PO Field Operations							
Hub:		7HKNC Kansas City Hub							
Field Office:		7DPH OMAHA PROGRAM CENTER							
Field Office HA:		NE001 OMAHA							
Report Period:		8/26/2015 to 9/10/2015							
Report generation Date:		Thursday, September 10, 2015 11:42:52 AM							
Improper logoff's during 8/26/2015 and 9/10/2015									
Records 1 - 21 of 21 << Prev page 1 Next Page >>									
#	▼ User Name (First, Middle, Last)	User ID	User Type	OS type and version	Browser type and version	Logon date & time	Logoff date & time	Account Expiry	Error Description
1		M	HA User	Windows XP	Internet Explorer 8.0	8/27/2015 4:31:07 PM	8/27/2015 5:06:28 PM	1/1/2018	7083- Automatic logoff due to timeout

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.

Security
Role Maint
Access Reports
Activity Reports
User Certification

User Activity Query
New Users
Improper Logoff
User Account Usage

Select View:

HA User
Select

HQ Office:
Public and Indian Housing

HQ Division:

PO Field Operations
Select

Hub:

7HKNC Kansas City Hub
Select

Field Office:

7DPH OMAHA PROGRAM CENTER
Select

Field Office HA:

NE001 OMAHA
Select

Data Filters for User Account Usage Report

User Inactivity Period:

Last one week

User Types:

ALL

Select Status:

ALL

Display Filters for User Account Usage Report

No of rows to display:

50 Rows per page

Sort report data by:


User Name

Sorting Order:



Descending

Generate Report

User Account Usage report selection criteria



User Account Usage Report

HQ Office:
HQ Division:
Hub:
Field Office:
Field Office HA:

Public and Indian Housing
PO Field Operations
7HKNC Kansas City Hub
7DPH OMAHA PROGRAM CENTER
NE001 OMAHA

Report Period:
Report generation Date:

9/3/2015 to 9/10/2015
Thursday, September 10, 2015 11:49:50 AM

List of users who didn't access the system in last one week (9/3/2015 - 9/10/2015).

Records 1 - 50 of 85 (View All)
<< Prev page 1 2 Next Page >>

User Name (First, Middle, Last)	User ID	User Type	Last Logon Date/Time	Account Expiry Date	User Status
	M	HA User	2015-05-06 13:49:00.297	01 Jan 2018	Active
		Role Name	Role Level		
		Read Only - Privacy	Field Office HA		
		Use User Profile	HA User		
	M	HA User	2011-05-05 14:09:45.980	01 Jan 2018	Active
		Role Name	Role Level		

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.

Module name: Form-50058. *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.