Secure Systems Security Administration

Table of Contents

Introduction

The information in this document applies to PHAs administering the Public Housing and HCV (Housing Choice Voucher) programs. Security administration for multifamily housing systems is similar but will not be addressed in this document.

Due to how Secure Systems (REAC) is designed PHAs must complete their own security administration tasks. HUD staff are not able to complete security administration tasks for PHAs because they do not have access to those screens. What small amount that a limited number of HUD staff (typically PIC coaches and/or EIV coordinators) may be able to access will not match what the PHA sees due to how the system is configured. The instructions in this document will provide information on the most common tasks that need to be performed by PHA security administrators. **Unless otherwise noted it is the Secure Systems coordinator that needs to sign into to perform the steps.** If something is not addressed here, you can contact the REAC Technical Assistance Center at 1-888-245-4860 or by email at reac_tac@hud.gov

There are two types of PHA users in Secure Systems – coordinators and users.

- Coordinators are a type of user that can perform security administration functions on their own user ID as well as for other users within their PHA.
- Users, sometimes called regular users, cannot perform any security administrator functions in Secure Systems.
  - Typically, a PHA will have at least one person that is their overall security administrator, however, it is possible that someone who is a signed up as a user in Secure Systems may perform security administrator functions in a system that has its own security administration functions, such as PIC or EIV.

****Important Items to Keep in Mind****

- If a user ever leaves a PHA they must have their user ID terminated. If they are later employed at another PHA they must apply for a new user ID. User IDs cannot be taken from one PHA to another. While this may have been done many years ago, it has not been allowed in the last several years. This is because there needs to be an accurate record of the business partner relationship for a specific user. Additional relationships can be removed but not the original (primary) business partner relationship cannot be removed.
- If an individual had access to a PHA in Secure Systems and access was terminated but now they require access to that PHA again, they can request that REAC reactivate that their user ID.
- A user can have access to more than one PHA, for instance in cases of contract management, through assignment of the necessary PHA codes under PHA Assignment Maintenance and Business Partner Maintenance.

How to Register for a Secure Systems "Coordinator" User ID

There must be at least one coordinator at each PHA so that someone can maintain user access. If your PHA does not currently have a coordinator you will need to register as one or an existing user will need to request that their user ID be upgraded to a coordinator using the information in the Requesting Additional Updates/Changes to a User ID section of this document.

1. Go to the REAC website: http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/online
2. On the Online Systems page, look for the **Register Online** link on the right side of the page. Single click on this link.
3. On the Need A User ID page, single click on the **Public Housing Agency** link.
4. On the PHA User Registration page you will need to complete the requested information. For User Type you will need to sign up as a **Coordinator**. You must type in your PHA name in the Organization Name box and PHA code (i.e. NE789) in the Organization ID box. Also, **be careful to take note of the password you choose**, when you receive your user ID you will need it. Some or all of the information on this page could be used if you need to have your password reset in the future. You are required to provide your SSN, as this is an item used to verify your identity when making password reset requests. Do not use any other combination of digits.
5. When you have completed all parts of the registration form, click on the **Send Application** button.
6. A page will be displayed that confirms that you are registering for a Secure Systems (REAC) user ID. You should print a copy of this page. In 7 to 10 business days the housing authority will receive a confirmation letter via mail that says the access has been granted and will give the new coordinator ID. **Please be aware that this letter will not identify on the outside what it is and may appear like "ordinary" mail so make sure to be looking for it.** At this point the new coordinator user can log into Secure Systems with the password they picked during registration.
7. You will need to assign actions, roles, and PHA code to your user ID in order to have access to the links for any of the subsystems or systems.

How to Register for a Secure Systems "User" User ID

There must be at least one coordinator at each PHA so that someone can maintain user access. If your PHA does not currently have a coordinator you will need to register as one or an existing user will need to request that their user ID be upgraded to a coordinator using the information in the Requesting Additional Updates/Changes to a User ID section of this document.

1. Go to the REAC website: http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/online
2. On the Online Systems page, look for the **Register Online** link on the right side of the page. Single click on this link.
3. On the Need A User ID page, single click on the **Public Housing Agency** link.
4. On the PHA User Registration page you will need to complete the requested information. For User Type you will need to sign up as a **User**. You must type in your PHA name in the Organization Name box and PHA code (i.e. NE789) in the Organization ID box. Also, **be careful to take note of the password you choose**, when you receive your user ID you will need it. Some or all of the info on this page could be used if you need to have your password reset in the future. You are required to provide your SSN, as this is an item used to verify your identity when making password reset requests. Do not use any other combination of digits.
5. When you have completed all parts of the registration form, click on the **Send Application** button.
6. A page will be displayed that confirms that you are registering for a Secure Systems (REAC) user ID. You should print a copy of this page. Within one to two days the current Secure Systems coordinator at the PHA will receive a confirmation email that states that access has been granted and for who. It will tell them they need to retrieve the user ID within the system.
7. The PHA's Secure Systems Coordinator will need to retrieve the new user ID from inside of Secure Systems and assign actions, roles, and PHA code to the new user ID in order for the new user to have access to the links for any of the subsystems or systems.

How to Retrieve a User ID from Secure Systems (REAC)

1. Login to Secure System (REAC) by going to http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/online and single click on the Login Here link.
    - Note: If the user cannot remember the password they chose OR they have two failed login attempts (user receives the "invalid credentials" error) they will need to ask for a password reset from REAC at https://hudapps.hud.gov/reac/wass/resetPwd.html or by calling REAC at 1-888-245-4860.
2. On the Main Menu page, look for the User Maintenance option under the System Administration heading. Single click on this option.
3. On the User Maintenance page, it will ask you to search for the user you wish to maintain. There are two ways to search for a user ID.
    - In order to get all of the IDs for your PHA at once, go down to the boxes for First Name and Last Name and leave them blank. Single click on the Search Users button. It may take a minute or two since it is searching the whole database for all users with access to your PHA. This will bring up a list of all users for your PHA. It will list user ID, name, type of ID, and status (active or terminated).
    - Type in the first and/or last name for the user you need the user ID for. If the person may have registered with a short/alternative form of their first name you may want to use first initial and last name. Single click on the Search Users button.
4. Once you have obtained the ID, you may proceed with providing them access to other systems (e.g. EIV, PIC, REAC subsystems).
    - Some systems have specific requirements to gain access such as an access form or training. If you are not sure what is required, please check with your local field office.
    - If the person will access EIV, make sure that you insert the user ID in PIC Security Administration even if they will not access PIC since EIV shares the PIC security table.

Assigning Rights to a User ID

The steps below can be used by a coordinator to assign rights to themselves or someone at their PHA registered as a user. The appendix of this document lists the systems that a PHA will typically access but it is not all inclusive. You can reference this section as you are performing the steps below.

Notes before you begin:

- If a PHA has more than one coordinator, a coordinator cannot assign rights to another coordinator.
- When a coordinator is assigning rights to a user, the user should not be logged in when these steps are performed.
- If you need to assign rights to your auditor, ask them if they have the CPA Verification role already assigned to their user ID (usually an I ID since they do not work for a PHA but older ones may begin with M). The CPA Verification role is the only role they should have – they should not have the PHA Submitter or PHA Director roles.
    - If they do have the CPA Verification role, you can follow steps 13-18 below.
    - If they are unsure if they already have this role assigned, you can check by using steps 1-3 and 9-12. If you find it is assigned, use steps 13-18. If you find it is not assigned, while on the Assign/Unassign Roles page check the box for this role and continue with steps 10-18.
    - If you cannot see the FASPHA subsystem when you are checking for the role, you either do not have access to this subsystem yourself or possibly the action for the subsystem needs to be assigned to the auditor first. To assign the action, you will need to use the cancel button to go back to the user details and use steps 4-8 to assign the AUV Auditor Verification action, then continue starting with step 9. If you cannot see FASPHA on the Assign/Unassign Actions page it means you do not have access to the FASPHA subsystem and will need to give yourself access to it first using the steps below.

1. Login to Secure System (REAC) by going to http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/online and single click on the Login Here link.
    - Note: If the user logging in cannot remember the password they chose OR they have two failed login attempts (user receives the "invalid credentials" error) they will need to ask for a password reset from REAC at https://hudapps.hud.gov/reac/wass/resetPwd.html or by calling REAC at 1-888-245-4860.
2. On the Main Menu page find the heading System Administration. Under this heading single click on the User Maintenance link.
3. On the User Maintenance page enter the user ID of the user that rights will be assigned to. *This may be the user that is logged in if they are a coordinator or the user ID of a staff person registered as a user*. Single click on the Search By User button.
4. The page will refresh show the name and other details for the user ID entered. From the Choose a Function drop down box select the Maintain User Profile – Actions option and single click on the Submit button.
5. On the Assign/Unassign Actions page select the actions that correspond to the subsystem/systems that the user needs access to. **You only need to select one action per subsystem/system.** A list of the most common actions is provided in the appendix in this document.

6. After all of the actions have been selected single click on the Assign/Unassign Actions button at the bottom of the page.
7. The page will refresh and display a message that says you have successfully assigned/unassigned action(s) for the user. Single click on the OK button.
8. The page that shows the user's information will appear. From the Choose a Function drop down box select the Maintain User Profile – Roles option and single click on the Submit button.
9. On the Assign/Unassign Roles page select the roles that correspond to the subsystems/systems that the user needs access to. **Do not check all available roles since this may cause a conflict when attempting to perform tasks in a subsystem.** A list of the most common roles is provided in the appendix in this document.
10. After all of the roles have been selected single click on the Assign/Unassign Roles button at the bottom of the page.
11. A page will appear that asks you to confirm the roles you have just assigned. Single click on the Confirm button if it looks correct.
12. The page will refresh and display a message that says you have successfully assigned/unassigned role(s) for the user. Single click on the OK button. The page that shows the user's information will appear.
13. On the left side of the page find the System Administration heading. Single click on the PHA Assignment Maintenance link.
    - If you are a coordinator assigning rights to yourself and do not see this link you may need to log out of the system, close your web browser, wait 30 seconds, and then use the link in step 1 to log back in again. Once you have logged back in you can continue with this step.
14. On the PHA Assignment Maintenance page enter the user ID that you just completed assigning actions and roles to in the User ID box. Enter the PHA code that you need to assign access to in the PHA ID box. Single click on the Submit button.
15. On the Assign PHA to User page select the role(s) you need to assign a PHA to from the Role Description box. To select all of the roles listed you can single click on the first role in the list so that it is highlighted in blue, then use the scroll bar on the right side of the Role Description box to scroll to the button of the list. Hold down the Shift key on your keyboard and single click on the last role listed—all of the roles should now be highlighted in blue. To select only some of the roles you can use your CTRL key and single click on each role you want to select.
16. Single click on your PHA code in the PHA ID box so that it is highlighted in blue. Single click on the Submit button.
17. A page will appear that asks you to confirm that you want to assign the selected PHA to the selected roles. If it looks correct single click on the Confirm button.
18. The page will refresh and display a message that says you have successfully assigned the PHA to the user. Single click on the OK button. You will be taken back to the PHA Assignment Maintenance page.
19. The user that was assigned rights should verify they can see the links on their Main Menu page.
    - If you assigned rights to yourself, you will need to log out for all of the changes to take effect. Single click on the Logout link in the upper right hand part of the page. Close the window when prompted. Wait for about 30 seconds after you close the window before attempting to login again.
    - If rights were assigned to a user, that user can login once the steps above have been completed. They should be able to see the links on the Main Menu page for all of the systems that were selected.

Removing a PHA Assignment in Secure Systems

A PHA assignment may need to be removed if you need to unassign a role from a user or are in the process of terminating a user's access to all systems. Coordinators can only unassign a PHA code if they have access to that subsystem/system, otherwise it will not be visible.

1. Login to Secure System (REAC) by going to http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/online and single click on the Login Here link.
    - Note: If the user cannot remember the password they chose OR they have two failed login attempts (user receives the "invalid credentials" error) they will need to ask for a password reset from REAC at https://hudapps.hud.gov/reac/wass/resetPwd.html or by calling REAC at 1-888-245-4860.
2. Once on the Main Menu page, on the left side of the page find the System Administration heading. Single click on the PHA Assignment Maintenance link.
3. On the PHA Assignment Maintenance page enter the user ID for the user that you need to remove access for in the User ID box. Select View or Unassign PHA from the Choose a Function drop down box. Single click on the Submit button.
4. On the View/Unassign PHA for User page select the role(s) that are assigned to the user for your PHA that you would like to remove. To select all of the roles listed you can single click on the Select/Deselect All checkbox. All of the role(s) that you want to remove the PHA assignment from should now have checkmarks next to them.
5. Single click on the Submit button. You will get a page that confirms that you have unassigned the PHA from the user. Single click on the OK button. You will be taken back to the PHA Assignment Maintenance page.

Follow up items after a PHA assignment is removed:

- If the staff person is going to remain a systems user but their job duties have changed you will need to go to User Maintenance and first unassign the role(s) and then unassign the action(s) that are associated with the subsystem(s) that they no longer need access to so that the links will no longer show up on their Secure Systems Main Menu page.
- If the staff person has left the PHA's employment or no longer requires any systems access you will also need to terminate the user in any applicable systems that have separate access/security administration requirements from the REAC subsystems. Most notably these would include eLOCCS, PIC, and EIV. The following guidelines should be used to mitigate possible issues.
    - Users should be terminated in EIV prior to being terminated in PIC. Making a user inactive in PIC first will cause issues in terminating EIV access and could cause the user to be "stuck" in the user list for that PHA, which can cause confusion later.
    - Access to eLOCCS is terminated using the HUD-27054 form. Failure to do this will mean that the user will continue to have access until the next recertification period, at which time if the approving official does not recertify the user it will be terminated at that time. Good security procedures dictate that access should be terminated as soon as it is no longer needed.
    - Once all PHA assignments are removed and access has been terminated in all other systems (or is in the process of being terminated) the user ID needs to be terminated in Secure Systems. This can be done by the PHA's Secure Systems coordinator or via a request to the REAC Technical Assistance Center (TAC).

Terminating a User in Secure Systems

Before a user ID can be terminated by the REAC TAC the items below need to be performed the Secure Systems coordinator in the order listed below.

- If the user had EIV access that it was terminated.
- If the user had PIC access, even just to facilitate EIV access, that access has been made inactive.
- If the user had eLOCCS access that the OCFO User Support Branch has been provided the documentation to terminate this access.
- All PHA assignments have been removed under PHA Assignment Maintenance.
- If the user had access any multifamily housing systems that access has been removed under Property Assignment Maintenance. *If you are unable to complete this and/or need assistance, please contact the REAC Technical Assistance Center (TAC) at 1-888-245-4860.*

Once the items above have been completed the executive director or individual user can submit a request directly to the REAC TAC to have the user ID terminated. Information about this can be found in the Requesting Additional Updates/Changes to a User ID section of this document.

Reactivating a User in Secure Systems

Users must access Secure Systems at least once every 90 days. If this does not occur the user ID will be terminated automatically. If a user tries to log in at this point they will receive an error about the status of their user ID. The user will need to contact the REAC Technical Assistance Center (TAC) to confirm the issue. If the user ID is in terminated status, then the user can follow the information found in the Requesting Additional Updates/Changes to a User ID section of this document to request that REAC reactivate their user ID.

Updating a User's Email Address in Secure Systems

The email address in a user's profile in Secure Systems is used to communicate with the user. The most common communication is in the event of a password reset request. If the user changes email addresses but their profile is not updated, then they will not receive those email notifications. The Secure Systems coordinator will need to perform these steps for users at their PHA but can also make the update for their own user ID. If for some reason the coordinator is unable to make the update the user should contact the REAC Technical Assistance Center (TAC) at 1-888-245-4860 to inquire about how to complete this.

1. Login to Secure System (REAC) by going to http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/online and single click on the Login Here link.
    - Note: If the user cannot remember the password they chose OR they have two failed login attempts (user receives the "invalid credentials" error) they will need to ask for a password reset from REAC at https://hudapps.hud.gov/reac/wass/resetPwd.html or by calling REAC at 1-888-245-4860.
2. On the Main Menu page find the heading System Administration. Under this heading single click on the User Maintenance link.
3. On the User Maintenance page enter the user ID of the user that you need to update the email address for. *This may be the user that is logged in if they are a coordinator or the user ID of a staff person registered as a user.* Single click on the Search By User button.
4. The page will refresh show the name and other details for the user ID entered. By default, the Choose a Function drop down box is set to Maintain User Information. Single click on the Submit button.
5. On the Edit User Information page look for the email address textbox. Enter the new email address in this box and single click the Save button.
6. The page will refresh and display a message that confirms that the change was made.

Requesting Additional Updates/Changes to a Secure Systems User ID

There are some changes that do not occur very often and/or cannot be done at the PHA. These requests need to be requested through the REAC Technical Assistance Center (TAC). These changes may include:

- User ID terminations. This request can be made by the following individuals:
  - The PHA executive director
  - The user

    Note: The PHA's Secure Systems Coordinator can terminate the user without a TAC request by removing all roles and then terminating the user.
- User ID reactivation
- User ID upgrades and downgrades
- Manual activations
- Deactivations
- Re-attachments
- Detachments
- User ID information corrections and changes

Information on how to make these requests can be found in the document titled "WASS Online Systems Request Instructions" at the end of this document.

Appendix: List of Commonly Accessed Systems and Access Rights

This section lists the most common systems that a PHA will access but is not all inclusive. The roles that are assigned to a user should correlate to their job duties. Access can always be adjusted at a later time meaning that users should not have access to more than they need. This helps protect the integrity of the data in the systems. The realm of online systems is constantly changing, which includes adding and removing of systems. If a system is not listed below, please contact the REAC Technical Assistance Center (TAC) or local field office for further information.

Below are common "Actions" and "Roles" that, depending on job duties, may be assigned to someone registered as a coordinator. This may include an executive director or other individual that needs a high level of access. Whether someone is a coordinator or a user they may or may not need all system that are available. If a lower level of access is needed, please reference what you see in the system and the WASS user manual located at http://portal.hud.gov/hudportal/HUD/program_offices/public_indian_housing/reac/products/wass/wass_user_manual

Do not automatically give access to any of the examples below unless the user needs it for their job duties!

Actions – you only need to pick one per subsystem or system:

Subsystem / System	Action
EIV - Enterprise Income Verification	COR - Coordinator
FASPHA - Financial Assessment Subsystem – PHA	COR - Coordinator
FHSEC3 – FHEO Section 3 60002 Reporting Form (also known as SPEARS)	COR - Coordinator
LOCCS - Line of Credit Control System	COR - Coordinator
NASS - Integrated Assessment Subsystem	COR - Coordinator
PASS - Physical Assessment Subsystem	COR - Coordinator
PIC – PIC system	COR - Coordinator
VMS – Voucher Management System (only for PHAs with a Section 8 program)	COR – Coordinator

Roles – you only need to pick one per subsystem or system unless noted:

Subsystem / System	Role(s)
EIV - Enterprise Income Verification	EIV – PIH - EIV - External User
FASPHA - Financial Assessment Subsystem – PHA	PID – PHA Director
FHSEC3 – FHEO Section 3 60002 Reporting Form (also known as SPEARS)	S3P – 60002 Reporting – Participant
LOCCS - Line of Credit Control System	ADM - Administration QRY - Query
NASS - Integrated Assessment Subsystem	PHC - PHA Coordinator
PASS - Physical Assessment Subsystem	EEE - EHS Edit External EHC – Mitigation Reviewer PIV - Physical Inspection Viewer
PIC – PIC system	COR - Coordinator
VMS – Voucher Management System (only for PHAs with a Section 8 program)	UDE - Utilization and Expense Data Submitter

PIH-REAC

WASS ONLINE SYSTEMS REQUEST INSTRUCTIONS

INSTRUCTIONS

ID requests must be submitted in writing on letterhead and signed and titled by the original owner of the entity or by the management company of the entity (as listed in iREMS) for one of the following request types:

- Manual activations
- Deactivations
- Re-attachments
- Detachments
- ID terminations and re-activations
- ID termination by user*
- ID upgrades and downgrades
- User ID information corrections and changes*

Your official letter request must contain:

- WASS Secure System ID number
- Name on the ID
- Tax ID(s) (if applicable)
- FHA number or contract number or project number (if applicable)
- PHA Code (if applicable)
- Mother's maiden name (if applicable)
- Last 4 of SSN (if applicable)
- Name of the entity
- Signature and title of the Owner, Executive Director, President, CEO, or Board member
- Contact information (i.e. name, address, phone, email address)

For manual activations, a letter can be submitted only after you have submitted your request for activation keys electronically and then waited 7-10 business days. If you have not received the activation key code letter by U.S. Mail after 7-10 business days, then you may request manual activation.

Submit your *official letter* as an attachment in an email to: **reac_tac@hud.gov**.

Notes:

- To validate the identity of the individual making the request, staff with Technical Assistance Center (TAC) may ask for additional information.
- *A User or Coordinator can submit their own letter to terminate their own ID or have a name change on their ID:
    - Indicate your request

Created: 7/30/2012 WBA

Updated: 6/19/2017 WBA

- Include ID number, MMN and last 4 of SSN
- Include contact information (address, phone, email)
- Sign the letter

REMINDER: **It is your duty and responsibility to safely and securely transmit Personally Identifiable Information (PII) of organizations and individuals.**
Placing Social Security Numbers, Mother's maiden name and Tax ID Numbers in the body of an email is not a secure way to transfer this information.
We suggest submitting your request in a password-protected zip file. **Use password:** **TACSecurity1***