HIMS

Human Resources Command Identity Management System
**Identity Management System (IMS)** ................................................................. 5

- IMS Landing Page ..................................................................................... 5

**Adding a New User** .................................................................................. 6

- UIC Query ................................................................................................. 8
- User Role .................................................................................................. 9
- Application Access .................................................................................. 9
- Comments ............................................................................................... 10
- Audit/Activity Logs .................................................................................. 10
- Security Validation .................................................................................. 11
- Add Update System Roles ...................................................................... 11
- IMS Activity Email .................................................................................. 12

**Updating an Existing User** ..................................................................... 12

- View User Access ................................................................................... 14
- Manage Sponsorship ............................................................................... 15
- Validating a User .................................................................................... 16
- Transfer User ......................................................................................... 18
- Deactivate User ..................................................................................... 20
- Work List ................................................................................................ 21
- Pick List .................................................................................................. 22

**Reports** .................................................................................................. 24

**Troubleshooting** .................................................................................... 26

- Cannot reach SPEX .................................................................................. 26
  - Using Incorrect URL ........................................................................... 26
- Unable to login to HIMS via SPEX ........................................................ 26
  - Does not have a HIMS Account ......................................................... 26
  - Does not know how to login to HIMS ............................................... 26
  - Not Using Correct Certificate to Login ............................................ 26
- Common Findings within HIMS .............................................................. 27
  - UIC Lookup on User ......................................................................... 27
- Application Access Restrictions for Users outside of HR01 .............. 28
- Work List Cleanup .................................................................................. 28
- General and Location Information ....................................................... 29

**System Support Information** .................................................................. 29
The IMS Application is available via SPEX (Secure Processing Extranet) on the Public Internet.

URL: https://spex.usaac.army.mil
From this page, click the “Continue” button to proceed.

SPEX Landing Page/IMS Access

Notice the three (3) headers on the left-hand side of your screen. You may need to click the [+] next to each header to expand the menu.

Secure Processing
- **IMS:** This link will provide you with the link to access the IMS system (it is recommended you view the Help section below prior to accessing IMS) and also download this HIMS User Manual.

Help
- **Access:** Outlines the prerequisites needed to access the IMS system
- **Logging In:** Instructions along with screenshots outlining the login sequence with your CAC. **Note:** Use DOD EMAIL Certificate when logging into IMS.
- **Support:** Email and Phone Number for support

Home
- **Home:** This link will return you back to the SPEX homepage ([https://spex.usaac.army.mil](https://spex.usaac.army.mil))
- **Logout:** Will log you out of SPEX
Under the Secure Processing Header, click the IMS link.

Click either of the two links to access IMS (either to load in a NEW browser window or the current browser window). There is no difference in the links other than opening in the current browser window or a new one.

You will then get a pop-up prompt instructing you to select your DOD EMAIL certificate, click "OK"

Click your DOD EMAIL certificate then click “OK”

If you have IMS Sponsor level Access, your IMS homepage will look like the following:
**Identity Management System (IMS)**

**IMS Landing Page**

- **Add/Update Access:** Add new users or update existing users’ access in IMS
- **View User Access:** View existing users application access, user IDs, sponsorship level, activity logs and/or user account comments
- **Manage Sponsorship:** Delegate another user as a sponsor (*Level 2 sponsors only*)
- **Transfer User:** This option is to transfer a user from sponsor to sponsor, not PSC to PSC.
- **Deactivate User:** Remove all application access from a user and place their profile in ‘deactivated’ status
- **Work List:** View listing of users that you have added access to and/or updated with quick access to Actions List (Update, View Access, Manage Sponsorship, Transfer, Deactivate)
- **Pick List:** List all users listed under your PSC code or search for user by Last name with quick access to Actions List (Update, View Access, Manage Sponsorship, Transfer, Deactivate)
- **Reports:** Run reports to view what applications your users have access to, either can be ran by PSC code or by the application. Note: The reporting feature does not guarantee the application account is active. Sponsor may need to contact the
Adding a New User

Click the “Add / Update Access” link located in the left-hand navigation.

Input the user AKO ID in the text box and click the “Fetch User” button.

You will see a note under the AKO User ID text box: New User at AKO.
All General and Location information is pulled down from AKO. If the user information is incorrect or outdated, the user must update this information in AKO. You will not be able to modify this general and location information in IMS.

If you do not know the users’ security background information and their data is located in ITAPDB, you can click the “Get/Refresh Security Clearance and UIC Data from ITAP” button.

If you have previously verified this information, you are not required to click this button.

If you are uncertain of the Security Eligibility codes, click the yellow question mark (?) next to the “Security Eligibility to Classified Information Explanation Table”.

Place a checkmark in the box to verify that CIV/CTR user has a favorable NACI or that the MIL user has a NACLC completed. By checking this box, you have verified the user meets the appropriate security clearance for access to the applications listed in IMS. You may not proceed until you have checked this box.

Knowingly permitting access to a user who does NOT meet the security requirements will result in the loss of your sponsorship privileges in IMS and could result in UCMJ. Regaining sponsorship access to IMS will be handled on an individual basis.

When you have fetched the user data from AKO, verified their security clearance and checked off the checkbox, click the “Add Access for New User” button.

First step you should take as a sponsor is to verify that the user information is correct.
**UIC Query**

Next, enter the users UIC Code.

If you already know this data, input the user UIC in the UIC text box under Additional Information and click the “Query DMSL thru ARQODA Values via UIC” button. If the UIC is valid, it will auto populate the values for DMSL, PSC, DML, MACOM and ARQODA.

If the UIC is not valid, when you click the “Get DMSL thru ARQODA Values via UIC” button, an error message will appear stating “UIC Could NOT be Found”.

You can query the available UIC Codes for your PSC Code by clicking the “UIC Lookup” link here.

---

**General Information**

- AKO User ID: gayle.donne
- Rank / Grade: M1
- First Name: Gayle
- Middle Name: Waysa
- Last Name: Thomas
- Employee Type: DA
- AKO EMAIL Address: gayle.donne@us.army.mil
- Sponsor: linda.nurse
- Sponsor Work Phone: 502-813-2138
- AKO EMAIL Sponsor: linda.nurse@us.army.mil

**Location Information**

- Street Address: 1600 Southland Dr, Ave, Dept 810
- Room #: Mail Stop: City: Fort Knox
- State / Province: Kentucky
- Postal Code: 42791
- DSN Phone: 843-7968
- Work Phone: (502) 513-7685

**User IDs**

- Legacy ID:
- EDAS ID:

**Add Update User Access**

- Query UIC:
- DMSL thru ARQODA Values via UIC

**From the UIC Search box, input the user PSC code in the PSC textbox and click the radio button if the PSC code is exactly as entered or if the PSC code starts with a certain character. Then, click the “List UIC(s) Where:” button.**

Locate the user’s UIC from the list; highlight the UIC and either hit CTRL + C or right click and select Copy.

Close out the UIC Search box and Paste the user UIC in the Query UIC textbox by either hitting CTRL + V or right click and select Paste.
Then click the “Get DMSL thru ARQODA Values via UIC” button.

If you input the wrong UIC, you can enter the correct one or query the UIC list again and update by re-clicking the “Get DMSL thru ARQODA Values via UIC” button.

Once you have set the users UIC, you may also add in the user Office Symbol and their Organization/Company if desired.

**User Role**
Next, update the users’ role.

Update the users Echelon, Duty Position and Section.

You will not be able to modify the PSC Type. This is auto populated based on the UIC/PSC information from the previous step.

**Application Access**
Check the boxes next to the applications that the user needs access to. Some of the applications listed are Human Resources Command (HRC) internal only (EPM, SEPM, ITAPDB, SEPS, OSSS, and RPAS). If you are not internal to HRC, you will not be able to check off these boxes. DO NOT request access to all applications or check everything checkbox because it is available. Only check the applications the user needs to perform their job role. If you are unsure of the
application acronym, click the yellow questions mark (?) next to “Application Access”.

If user needs AORS, RDMS or RPAS (HRC ONLY) account and you wish to have their account mirror another user, provide that users’ name in the “Mirror Account” textbox.

**Comments**
Click the “Manage IMS Account Comments” link to view previous comments for this user or to add a new comment. (Optional)

This will log the previous 10 comments on the account.

When a request is submitted, the most recent comment will be included in the email.

**Audit/Activity Logs**
Click the “View Account Activity Log” link to view a history of the account access for this user.

When ready to submit the user request, click the “Update Access and Attributes” button at the bottom of the page.
Security Validation
To the right of the Audit/Activity Log, it will show the last time the user’s security background and clearance information has been validated.

Note: It will not show the initial security validation timestamp until the request has been submitted in HIMS.

Add Update System Roles
On this page, you may select what system roles the user needs. Highlight only those roles that the user needs. For CITRIX, select the applications that the user will need access to via CITRIX (At this time, most commonly used will be PERNET and TOPMIS2). To make multiple selections, hold down the CTRL button as you left click on your mouse to make selections.

For EDAS, the roles available are Promotion Reports (C10) and View Only. You can only select one.

When completed, click the “Update and Continue” button.

Add/Update Account Results
Lastly, you will be directed to a page that shows a summary of the transaction.

Click the “Done” button.
**IMS Activity Email**

The sponsor and the user will receive an activity notification email from IMS for each application that was requested and/or updated.

Once the access has been created, the sponsor and user will be notified via email and if the access requires a user name and password, they will be supplied in that email.

---

**Updating an Existing User**

Click the “Add / Update Access” link located in the left-hand navigation.

Input the user AKO ID in the text box and click the “Fetch User” button.

You will see a note under the AKO User ID text box: Found existing user within IMS.
Click the “Get/Refresh Security Clearance and UIC Date from ITAP” button if you need to revalidate the user background investigation, check the checkbox to verify this information and then click the “Update Access for Existing User” button.

From here, you can:

Update user however needed and click the “Update Access and Attributes” button at the bottom.

You will get prompted to update the system roles. Update if needed, otherwise, click “Update and Continue” button.

Account results page will be displayed.

Note: The Request Status will only show the results of any changes in Application Access (adding/removing). If you only update the users’ profile (change UIC, Office Symbol, or Role), it will not be displayed on the Account Results page.

Click the “Done” button.
View User Access

To view a current users’ access, click on the “View User Access” link located in the left-hand navigation.

At the View User Access page, input the users AKO ID and click the “Fetch User” button.

From this page, you can view all the current information that is available for that user. This page will display the User IDs they have been assigned, sponsorship level, application access requested, most recent comment and you can click on the “View Account Activity Log” link to see all actions performed on this user.

This page is VIEW ONLY and you will not be able to modify any user information or account access. This must be done by clicking the “Add/Update Access” link in the left-hand navigation.

Note: The Application Roles only show what access the user has within the respective application. It does not state that the user has access to that application or the application listed in the box. The Application Access for that application must state it is “Active”. If the line is blank next to that application, they do not have access to it.
Manage Sponsorship

Only Level 2 sponsors and above will have the capability to delegate sponsorship to another user.

Transferring your sponsorship to another user should be done when you are leaving your duty position and transferring the users under your PSC code to the new sponsor.

Click the “Manage Sponsorship” link located in the left-hand navigation.

Input the user AKO ID in the text box and click the “Fetch User” button.

Under Manage Sponsorship, select the level of sponsorship you wish to delegate to user and then locate the users PSC code in the “Available PSC(s)” box, click on the user’s PSC code and click the “Add Selected PSC” button.

When finished, click the “Update User Sponsorship” button.
You will see a note under the AKO User ID box that the Requested Operation was Successful.

Validating a User

In order to comply with AR25-2, all sponsors will be required to validate their users in HIMS on an annual basis. This will be accomplished using the Manage Annual Renewal page.

Beginning 30 days prior to a user’s validation date, HIMS will automatically send out an e-mail every day informing the sponsor that a user needs to be validated. Once you receive this e-mail, you can go into the Manage Annual Renewals and validate their account by following these steps:
Once you click on Manage Annual Renewals you will be taken to the following screen:

If you have any users within your PSC, that has an annual renewal date, they will show up on this page. As the sponsor, you will have one of three actions to choose from:

**Renew** – you have determined that the user is still under your hierarchy, and still needs access to the HRC applications

**Disable** – the user is no longer under your hierarchy or no longer needs access to the HRC applications

**Ignore** – you are unsure of this user.

Once you have chosen what action you want to take, click the Submit button.
If no action is taken before the renewal date, the user’s account will be deactivated in HIMS automatically, and any access he/she had will be disabled.

**NOTE:** If you make any changes to a user’s account, such as add EDAS, then the user’s renewal date will automatically adjust to one year from the date of the transaction.

**Transfer User**

At this time, you can only transfer a user if they belong to one of your sponsoring PSC codes. If you try to access a user that is not in one of your PSC codes, you will receive a message stating you do not have the authority to access that user. If you need access to that user, you must contact the current sponsor for that user and request them to transfer that user to you or contact the HRC IT Helpdesk (800-272-1330) and submit a ticket to have the user transferred to you in HIMS.

There will be a procedure in HIMS to transfer users from different PSC codes in a future release.

To transfer a user, click the “Transfer” link located in the left-hand navigation.

Input the user AKO ID of the user you wish to transfer in the text box and click the “Fetch User” button.

You can keep the asterisk (*) in the “Where Last Name is Like” textbox and click the “List Sponsors” button.

---

**HIMS V.3/MAY 2014**
This will display all available sponsors for your PSC code.

Or, you may enter in the Last Name of the sponsor and click the “List Sponsors” button.

Click the “Select” link next to the sponsor’s name and the row will become highlighted in yellow.

Click the “Transfer User” button.

When processes has completed, IMS will state that the “Requested Operation was Successful” and the User’s Current Sponsor will update to the new sponsor.
**Deactivate User**

To deactivate a user, click the “Deactivate User” link located in the left-hand navigation.

Input the users AKO ID in the text box and click the “Fetch User” button.

Verify that this is the correct user you wish to deactivate and if not, click the “Cancel” button. Otherwise, click the “Deactivate User” button.

When you deactivate a user, any application access they had **will be deleted**. If the user transfers to a new unit/installation, their new IMS manager can reactivate their profile and request their application access back (if needed).

Click “OK” to confirm the deactivation of user’s access.

Confirmation that user was deactivated successfully.
Until the deactivated user is transferred out of your PSC code, their IMS profile will remain under your PSC code as a “Deactivated” user when viewing Work List, Pick List and Reports.

Regardless of transfer or deactivation, the User IDs will not change.

**Work List**
The Work List is a listing of all the users that you have added access to or have updated. From this Work List, there are up to five (5) quick action icons that you can perform on any user listed.

Click the “Work List” link located in the left-hand navigation

From the work list above, you can click on any of the icons in the Actions column for that user:
Pick List
The Pick List is similar to the Work List above but allows you to search for a specific user or to list accounts by a PSC.

Click the "Pick List" link located in the left-hand navigation.

To view users that belong to a specific PSC Code, locate the PSC Code in the dropdown box and click the radio button next to "List Accounts by PSC Selected Above".

Click the “List Users” button
Much like the Work List, the Pick List also displays the users’ Echelon, UIC, Sponsorship Level (If blank, they are not delegated as a sponsor) and their last login date to IMS.

You can also click any of the icons in the Actions column for that user.

To search for a user using the Pick List, click the radio button “Is exactly as entered above” next to “List Accounts Where Last Name is” and input the users Last Name in the text box.

Click “List Users” button.

This will search for all users under the PSC Codes you sponsor with the last name you entered in the Last Name textbox.
If you do not know the correct/full spelling of the users last name, you can input a minimum of two (2) characters of the last name and click the “Starts with characters as entered above”. The results will populate all users whose last name begins with those characters entered in the “Last Name” textbox.

Reports

Click the “Reports” link located in the left-hand navigation.

There are two types of Reports that you can run, PSC and by Application.

To run a PSC Report, select your PSC code from the PSC Code dropdown box and next to “List Account by PSC or Application” click the radio button by PSC, then click the “List Users” button.
The PSC report will display the IMS UID, Last Name, First Name, Echelon, Position, Application Access and status.

In the Application columns:

R: Access has been Requested for this application

S: Access request for this application was Successful

E: Access Request Error

To run an Application report, click the Application radio button next to “List Accounts by PSC or Application” and then select which Application you wish to check.

The Application Report will display all the users that have access to the application that was searched. The report populates the IMS UID, Title, Last Name, First Name, Echelon, Position, PSC Code, Sponsor and Status.
Troubleshooting

**Cannot reach SPEX**

**Using Incorrect URL**
- Be sure you are using the correct URL: [http://spex.ussac.army.mil](http://spex.ussac.army.mil)
- Cut and Paste the URL into the browser address bar to avoid any typographical errors

**Correct URL but still cannot access**
- Make sure the site is available using Vendor LAN or Air Card
- Check with Local IT Helpdesk for network issues

**Unable to login to HIMS via SPEX**

**Does not have a HIMS Account**
- Ensure the user trying to access HIMS is delegated as a HIMS Sponsor

**Does not know how to login to HIMS**
- Ensure the user knows the proper procedure for logging into HIMS. Direct user to Help section in HIMS. See above, pages 3-5

**Not Using Correct Certificate to Login**
- Verify that the user is selecting their DOD EMAIL Certificate when logging into HIMS.
Common Findings within HIMS

**UIC Lookup on User**

- This action is new for all users moving over from HURS
- Entering in a UIC is mandatory
- All subsequent values, (DMSL, DML, MACOM & ARQODA) are derived from the UIC and will help clean the data for all users who's values were incorrectly inputted by hand in HURS
- Copy and Paste the appropriate UIC from the lookup window

- Then click the “Query DMSL thru ARQODA Values via UIC” button to populate the remaining fields

**Application Access Restrictions for Users outside of HR01**
- Selected Applications are only available for users in HR01 and sponsors in other PSC’s will not be able to request access for their users and will not be selectable.

**Work List Cleanup**
- There is nothing that a user can do to remove a user from their Work list.
- Once a sponsor has performed an action on a user, they will be shown on the sponsors Work List.
General and Location Information

- The General and Location Information on the Add/Update User page is pulled from AKO.
- If the user’s information is incorrect, the sponsor should contact the user and have them update their General and Location information in AKO.

System Support Information

For password resets, permission issues or general questions, please contact the HRC IT Helpdesk.

USARMY Fort Knox HRC IT Helpdesk

1-502-613-7777

usarmy.knox.hrc.mbx.it-help-desk@mail.mil