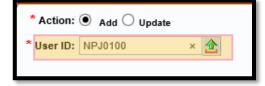# Create and Update User Security with UDOC

This document walks through establishing new eMARS users security and modifying or removing existing users with a User Maintenance Document (UDOC). UDOCS are created in the Administrative application of eMARS.

All security assignments should be completed by the agencies delegated Security Officer per FAP-120-22-00. The Security Officer will be responsible for approving the agency's automated Workflow setup within the Commonwealth's central accounting system. The Security Officer will work with the Fiscal Officer to ensure that agency security settings create proper internal control structure.

Create a UDOC for a New eMARS User

1. Log into eMARS and navigate to the UDOC document in the Document Catalog
   a. Enter UDOC in the Jump to field and select "Go" OR;
   b. Use the Secondary Navigation panel, select Search> Document Catalog>Create
2. Create UDOC
   a. Select Create
   b. Enter UDOC in the Code field
   c. Enter your Department and Unit code
   d. Enter a unique Document ID
      I. Use the naming convention "USER ID-1". For example **ABC1234-1**, the "-1" signifies this is a new user. The User ID should be capital letters.
      II. Any modifications made to this user should also use the same naming convention with the next number in sequence. For example ABC1234-2
   e. DO NOT check the Automatic Numbering option
   f. Select Create again
3. *Header Section*
   a. Select "Add" radio button
   b. Enter User ID (eMARS ID using all capital letters)

c. Directory Information tab
    i. Enter User's Last Name and First Name (using Title Case: Smith, not smith or
        SMITH), Email Address, and Phone Number
    IMPORTANT: Email address must be correct; email notification will used to notify
    users of their User ID and Password once the UDOC is approved

| Directory Information | Home Organization | Account Options | Password Maintenance | Applications | External Directory ID |

* Last Name: Smith	Locality:	Phone Number: 502-564-1234 ✕
* First Name: Jane	Room Number:	Ext.:
	Email Address: Jane.Smith@ky.gov	Fax Number:

d. Home Organization tab
    i. Enter User's three digit Department code
    ii. Enter "CTPL" in the Bureau field (used for central security purposes)

| Directory Information | Home Organization | Account Options | Password Maintenance | Applications | External Directory ID |

Government Branch:	Division:	District:
Cabinet:	Group:	Bureau: CPTL
Department: 758	Section:	Unit:

e. Password Maintenance tab
    i. For New Users only, select check boxes for *Reset Password*, *Generate New
        Password* and *Expire New Password*. These options will create the users initial
        password and allow the user to reset/maintain their eMARS password.

| Directory Information | Home Organization | Account Options | Password Maintenance | Applications | External Directory ID |

Reset Password: ✔	Password:
Generate New Password: ✔	Email Password:
Expire New Password: ✔	

f. Applications tab
    i. Check the ADVANTAGE Financial box, this allows access to eMARS
    ii. Check the PASSWORD RESET box, this allows the user to reset their password

| Directory Information | Home Organization | Account Options | Password Maintenance | Applications | External Directory ID |

ADVANTAGE Financial: ✔	ADVANTAGE Administrator: ☐	ADVANTAGE MSS Mobile: ☐
ADVANTAGE HR: ☐	ADVANTAGE ESS: ☐	ADVANTAGE ESS Mobile: ☐
ADVANTAGE VSS: ☐	PASSWORD RESET: ✔	ADVANTAGE Procurement: ☐
VSS Password Reset: ☐	ADVANTAGE MSS: ☐	User Security Realm: ☑
		Existing LDAP User: ☐

4. *Security Role Section*
   a. Select "Insert New Line" at the bottom of the section
   b. Select "Add" radio button (Defaults to Add)
   c. Select the required Security Role ID for User using the pick list
   d. Enter a unique number as Precedence for the role (eMARS does not use Precedence, but it must be unique. Use sequential numbers 1, 2, 3, etc. for each new role you add
   e. Repeat steps to assign multiple security roles to a user

5. *Workflow Approver Section* (complete <u>only</u> if user has been identified to have a Workflow Approver role)

   a. Select "Insert New Line"
   b. Select "Add" radio button (Defaults to Add)
   c. Select Role ID for this manager using the pick list
   d. Check Manager box, if needed, this will allow the User to Return Tasks (documents) to the Group Worklist from other users in their absence
   e. Display Sequence is required, but has no function within eMARS; you can leave the default at 1 for all Workflow Roles
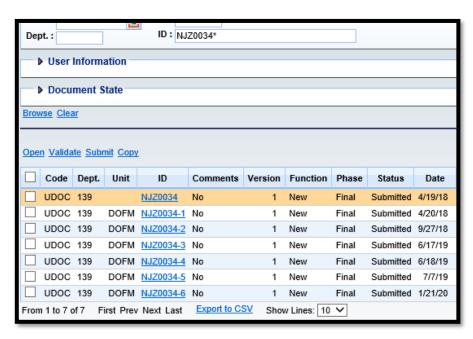   f. Repeat steps to assign multiple workflow roles to an approver

6. Select "Validate" to check for errors. Fix any errors that display, such as missing values in required fields
7. Select "Validate"again. If validation is successful, a message displays, "Document validated successfully."
8. Select "Submit" The UDOC will submit into workflow for approval. Confirm the document s in a Pending phase.

The Office of the Controller will approve all UDOCS. If there is a rush for approval, please email the Head Security Lead in the Office of the Controller, otherwise all UDOCS are approved by close of business the same day. If approval is needed in the Historical application, please email the Head Security lead in the office of the Controller.

Note: New users who will be creating Payable/Procurement documents will need to be added to the USER table in the eMARS Production application.

Updating User Permissions

1. Log into eMARS and navigate to the UDOC page
   a. Enter UDOC in the Jump to field and select "Go" OR;
   b. Use the Secondary Navigation panel, select Search> Document Catalog
   c. Enter the User ID and (*) wildcard, select "Browse" (ei. ABC123*)
   d. Take note of the most recent *Final* document. For example, below the last Final document is NJZ0034-6.

   e. Select Create
   f. Enter UDOC in the Code field

g. Enter your Department and Unit code

h. Enter a unique Document ID

    I. To be consistent, use the same naming convention when creating another UDOC for a user. In this scenario, the new document ID would be NJZ0034-7.

i. DO NOT check the Automatic Numbering option

j. Select Create again

1. *Header Section*

    a. Select "Update" radio button

    b. Enter User ID or use the pick list to locate the User ID

    c. Select "Populate from Existing User", this will fill in the current security access for the user

2. *Complete Security Roles section*

To **ADD** a Security Role:

    a. Select "Insert New Line" (Insert line after the last established security role)

    b. Select "Add" radio button (Defaults to Add)

    c. Select Security Role from the pick list

    d. Add a unique Precedence number

To **REMOVE** a Security Role:

    a. Select the line with the Security Role you want to delete

    b. Select "Delete" radio button (not the Trash icon; see Helpful Hints)

Never UPDATE a Security Role! Add needed Security Roles; Delete unneeded Security Roles Quick

3. *Workflow Approver Section* (complete only if user has been identified to have a Workflow Approver role)

To **ADD** a Workflow Role:

    a. Select "Insert New Line" (Insert line after the last established workflow role)

    b. Select "Add" radio button (Defaults to Add)

    c. Select Role ID for this manager using the pick list

    d. Check the Manager, if needed, this will allow the User to Return Tasks (documents) to the Group Worklist

    e. Display Sequence is required; you can leave the default at 1

    f. Repeat steps to assign multiple workflow roles to an approver.

To **REMOVE** a Workflow Role:

    a. Select the line with the Workflow Role you want to delete

    b. Select "Delete" radio button (not the Trash icon; see Helpful Hints below)

To **UPDATE** a Workflow Role (for changing the Manager setting)

    a. Select line with the Workflow Role you want to update

    b. Select "Update" radio button

    c. Check or uncheck the **Manager** box

4. Select "Validate" to check it for errors, fix any errors that display, such as missing values in required fields
5. Select "Validate" again, if validation is successful, a message displays "Document validated successfully"
6. Select "Submit," The UDOC will submit into workflow for approval. Confirm the document s in a Pending phase.

Helpful Hints

Use Delete Radio Button, not the Trash Can Icon on each line to remove a Role

UDOCS created for a new user, have a *Copy Line* and *Delete Line* icon available on the lines you added. The Delete Line icon is used to remove a line inserted in error, removing the unnecessary line will prevent updating the User's profile.

When creating a UDOC to update user security, selecting the trash can icon to delete a role only removes the line from the document. It **does not** delete the actual Security or Workflow Role from the User's Permissions. To delete a role from the User's Permissions, you must select "Delete" from the **Add/Update/Delete** radio button options.

Exit a User

When a User leaves the agency, the security officer is responsible for inactivating the user's eMARS account. To do this create a UDOC and complete the following Header fields.

- Locality: ACCESS REVOKED
- Locked Out: DISABLED
- Applications: Remove all ions

Note: If the user was assigned to any worklists, please navigate to the Workflow Rules and delete any security assignments. This prohibits emails from being sent for workflow assignments, for employees who are no longer with the agency.

Requesting a New Reporting User

New eMARS User who will be using eMARS Reporting have additional requirements that will need to be requested to the Office of the Controller, as well as, creation of UDOC for security roles. In order for users to be able to run or create reports in MARS Reporting, they will require an EBI account to be created by COT. The COT request must come from the Office of the Controller, Head Security Lead.

Users, who need an eMARS reporting account, should submit the following information to the Office of the Controller. There is no need to submit an F181 form to request access for eMARS reporting.

- User Name
- User ID
- User phone
- User email
- User home department
- Any query folders in addition to User Home Department and Statewide or Agency folders
- eMARS Template (where COT will charge for the EBI account quarterly)
- Developer or non-developer status

Requesting an account for a Contractor/Temporary Employee

If your agency is in need of a contract or temporary employee to perform eMARS functions, the office of the Controller, can be provide a User ID. Please contact the Head Security Lead for a temporary ID.

Check Writer Additional Access

New eMARS Users who will be running and processing Checkwriter files have additional requirements that will need to be requested to the Office of the Controller, as well as, creation of UDOC for security roles.

To request user access to process Check Writer files please submit the following information to the Office of the Controller:

- User Name
- Check Writer File ID's the user will need access to.

Common Mistakes

Common mistakes that cause Approvers to reject a UDOC'

- Not selecting "Populate From Existing User" when updating a current users account
- Forgetting to check the Manager checkbox for the assigned workflow roles
- Using the trash can icon to delete a user's role, you should use the "Delete" radio button
- Typing over an existing record to add a role, you should use "Insert Line"