

DEPARTMENT OF HEALTH & HUMAN SERVICES  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard, Mail Stop N1-19-18  
Baltimore, Maryland 21244-1850



Office of Information Services

---

# Enterprise User Administration (EUA)

## User's Guide

Version 1.5  
May 13, 2008

## Revision History:

08/12/2006	Version 1.0	
11/28/2006	Version 1.1	Added Section 7.0 Managing EUA Workflow
03/13/2007	Version 1.2	Semi-annual review
06/27/2007	Version 1.3	Semi-annual review
01/19/2008	Version 1.4	Updated Captioning for 508 Compliance
05/13/2008	Version 1.5	Added Section 8.0 Setting up Challenge Questions

## Contents

<b>1.0</b>	<b>INTRODUCTION .....</b>	<b>4</b>
<b>2.0</b>	<b>NEW USER REQUESTS.....</b>	<b>5</b>
<b>3.0</b>	<b>USER CHANGE REQUESTS .....</b>	<b>6</b>
<b>4.0</b>	<b>CMS USER ID CERTIFICATION REQUIREMENTS .....</b>	<b>7</b>
<b>5.0</b>	<b>EUA PASSPORT .....</b>	<b>8</b>
5.1	Installation of PassPort.....	8
5.2	Logging on to PassPort .....	8
5.3	PassPort Home Screen .....	9
5.4	PassPort Certification Screens.....	9
<b>6.0</b>	<b>MANAGING PASSWORDS .....</b>	<b>13</b>
6.1	Using PassPort to Manage Passwords .....	13
6.2	Setting up Challenges .....	15
6.3	Logging on to PassPort without a Password.....	16
6.4	Inactivity Revocation.....	18
<b>7.0</b>	<b>MANAGING EUA WORKFLOW .....</b>	<b>19</b>
7.1	Connect Additional Access.....	19
7.1.1	Connects for RACF Job Codes.....	21
7.2	Disconnect Job Code .....	24
7.3	IT Support Icon (Creating a trouble ticket for EUA support for CMS Employees only).....	27
<b>8.0</b>	<b>SETTING UP CHALLENGE QUESTIONS IN EUA PASSPORT .....</b>	<b>30</b>
8.1	Log into passport .....	30

## List of Figures

<b>Figure 1 — PassPort Logo.....</b>	<b>8</b>
<b>Figure 2 — PassPort Logon .....</b>	<b>8</b>
<b>Figure 3 — PassPort Home Screen.....</b>	<b>9</b>
<b>Figure 4 — PassPort Certification Screen.....</b>	<b>9</b>
<b>Figure 5 — System Access Certification Screen.....</b>	<b>10</b>
<b>Figure 6 — Privacy Act Statement.....</b>	<b>10</b>
<b>Figure 7 — Agree and Decline Buttons.....</b>	<b>11</b>
<b>Figure 8 — Confirmation Screen .....</b>	<b>11</b>
<b>Figure 9 — Certification Screen.....</b>	<b>12</b>

<b>Figure 10 — Summary of Accesses</b> .....	<b>12</b>
<b>Figure 11 — Password Screen</b> .....	<b>13</b>
<b>Figure 12 — Password Screen: Apply Changes</b> .....	<b>14</b>
<b>Figure 13 — View Status of Password Changes</b> .....	<b>14</b>
<b>Figure 14 — Challenges Tab</b> .....	<b>15</b>
<b>Figure 15 — Edit Challenge Screen</b> .....	<b>16</b>
<b>Figure 16 — Log On Without Your Password Screen</b> .....	<b>16</b>
<b>Figure 17 — Challenge 1 of 5 Randomly Selected Challenges Screen</b> .....	<b>17</b>
<b>Figure 18 — Password Tab</b> .....	<b>17</b>
<b>Figure 19 — WorkFlow Job Code – Connect Additional Access Screen</b> .....	<b>19</b>
<b>Figure 20 — WorkFlow Connect Job Code Request Tab</b> .....	<b>20</b>
<b>Figure 21—WorkFlow Connect Job Code Access</b> .....	<b>20</b>
<b>Figure 22—WorkFlow Connect Job Code Request Tab</b> .....	<b>21</b>
<b>Figure 23 — WorkFlow Connect Job Code details Tab</b> .....	<b>21</b>
<b>Figure 24—WorkFlow Connect Job Codes</b> .....	<b>21</b>
<b>Figure 25—WorkFlow Connect Job Code Requests Tab</b> .....	<b>22</b>
<b>Figure 26—WorkFlow Connect Job Code Access</b> .....	<b>22</b>
<b>Figure 27—WorkFlow Connect Job Code Request Tab</b> .....	<b>23</b>
<b>Figure 28—WorkFlow Connect Job Request Tab</b> .....	<b>24</b>
<b>Figure 29—WorkFlow Connect Job Code Details Tab</b> .....	<b>24</b>
<b>Figure 30—WorkFlow Disconnect Access</b> .....	<b>25</b>
<b>Figure 31—WorkFlow Disconnect Access Job Code Selection</b> .....	<b>25</b>
<b>Figure 32—WorkFlow Disconnect Access Job Code Selection</b> .....	<b>26</b>
<b>Figure 33—WorkFlow Disconnect Access Job Code Submission</b> .....	<b>26</b>
<b>Figure 34—IT Support Logon</b> .....	<b>27</b>
<b>Figure 35—IT Support Main Screen</b> .....	<b>27</b>
<b>Figure 36—IT Support Trouble Ticket Submission</b> .....	<b>28</b>

## 1.0 INTRODUCTION

This guide provides information on the Enterprise User Administration (EUA) system used by the Centers for Medicare & Medicaid Services (CMS) and the CMS Data Center (CMS DC). The guide discusses the role of EUA in User ID and password management, and provides instructions for installation and operation of EUA support products available to the user.

EUA is a system used by CMS to manage enterprise User IDs and passwords. It allows for centralized administration of User IDs on the entire CMS enterprise including the mainframe systems, mid-tier devices such as AIX or Sun systems, network operating systems such as Netware or Windows, and database platforms such as Oracle, Sybase, and MS SQL. The system utilizes online data to automate the approval process for access requests and provides logging and auditing support.

EUA only manages resources resident at the CMS DC and at CMS Web sites. EUA does not control remote dial-up access User IDs provided by AT&T Global Network Services (AGNS) or Health and Human Services (HHS) provided resources such as the Integrated Time and Attendance System (ITAS) and Outlook. Users need to manage those User IDs and passwords through mechanisms provided in those environments. EUA also does not manage local IDs created in application tables. It does, however, notify an application maintainer whenever a user has been granted access to the maintainer's application.

## **2.0 NEW USER REQUESTS**

The process for new users requesting access to CMS resources requires submission of a signed paper request form. For CMS employees, the new user provisioning process is handled by the agency personnel department. New contractor personnel need to complete the Application for Access to CMS Computer Systems Form available at <http://www.cms.hhs.gov/InformationSecurity/Downloads/EUAAccessform.pdf>

The contractor should forward the signed form according to the instructions provided by their CMS contact.

### **3.0 USER CHANGE REQUESTS**

All users may submit change requests by sending an e-mail to the CMS Access Administrator (CAA) responsible for their User IDs. The CAA will enter the request into EUA, where it will be routed to the appropriate approving authorities. Contractors must immediately notify CMS upon termination of any employees who hold CMS User IDs.

## **4.0 CMS USER ID CERTIFICATION REQUIREMENTS**

CMS requires everyone who has an enterprise User ID to complete an annual certification of their access needs, and to take a security Computer Based Training (CBT) course. Users who do not complete these tasks by their certification due date will have their access rights revoked.

Six weeks prior to the due date, each user receives an e-mail message notifying him/her of the need to certify and complete the CBT. The e-mail contains Web browser links to the EUA PassPort application and to the CBT Web pages. A printed letter is sent to those users who do not have e-mail addresses on file with CMS. Some external users may not be able to access the PassPort and CBT services. These services are not available from the Internet, but are accessible over the Medicare Data Communications Network (MDCN). The user notifications also include instructions on using the existing paper-based certification process and an alternate CBT process.

Beginning two weeks before the due date, a daily reminder notice is sent to those users who have not completed the certification requirements. If the users do not certify before the deadline, their access rights are revoked.

Users whose access rights have been revoked due to non-certification must request reinstatement by contacting the CMS Service Desk at 800-562-1963. Reinstatements will be granted for a two-week period. If the user does not complete the certification within the two week period, the User ID will again be revoked.

**NOTE** Both the paper and electronic certifications require approval before the user is considered certified. Please allow some time for this approval process, i.e., do not wait until the day before expiration to submit the certification request.



## 5.0 EUA PASSPORT

PassPort is a Web-based application used to provide users with an interface to EUA. The two principal uses of PassPort are for the annual user certification of access requirements and password management. Use of PassPort is encouraged by CMS, but its capabilities will simplify the User ID management process for users.

### 5.1 Installation of PassPort

Since PassPort is a Web-based application, no user installation is needed. The only software needed on the user workstation is a Web browser such as Internet Explorer or Netscape. CMS employees have an icon (Figure 1) for PassPort on their desktops. Other users can create a desktop icon for PassPort.

**Figure 1 — PassPort Logo**



### 5.2 Logging on to PassPort

PassPort is accessed by using the icon on the desktop or by entering the following URL in the Web browser: <https://158.73.79.141/passport/>. Users then enter their CMS enterprise User ID and password (Figure 2).

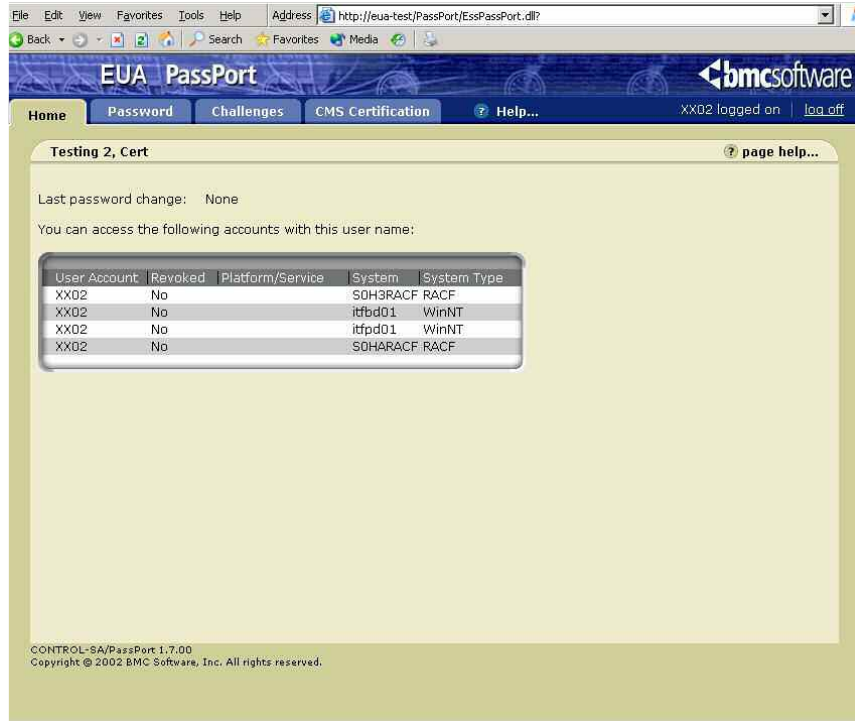
**Figure 2 — PassPort Logon**

The screenshot shows the PassPort logon interface. At the top, there is a blue header bar with "EUA PassPort" on the left and the "CMS" logo on the right. The main background is a light green color with a faint, circular seal-like pattern. In the center, there is a white rounded rectangular box with a grey border. Inside this box, the text "Log On" is at the top. Below it, the question "What is your CONTROL-SA PassPort user name and password?" is followed by two input fields: "Username:" and "Password:". Below the password field is a "Log On" button. At the bottom of the box, there are two blue hyperlinks: "Log on without your password..." and "Help with this page...".

### 5.3 PassPort Home Screen

Upon successful login to PassPort, the user is presented with the home screen (Figure 3).

**Figure 3 — PassPort Home Screen**



This screen lists the systems on which the user has accounts, and the status of those accounts.

### 5.4 PassPort Certification Screens

Selecting the CMS Certification tab brings up the screen illustrated in Figure 4.

**Figure 4 — PassPort Certification Screen**

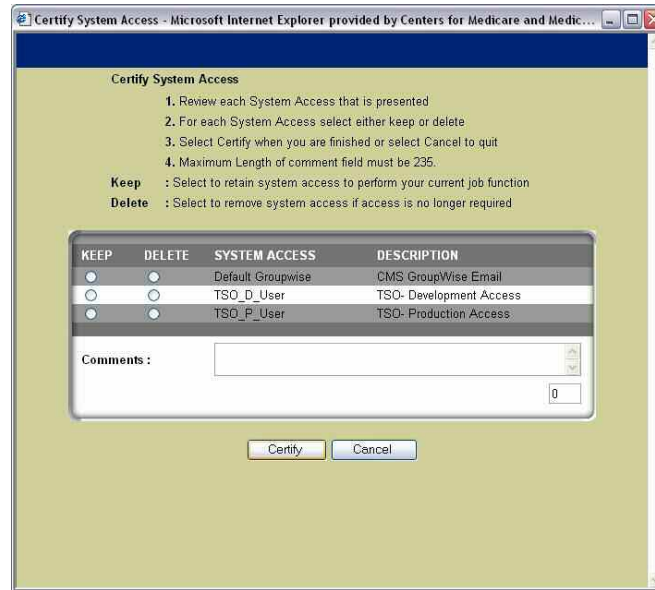


The screen has three sections. The first section presents the user details, as recorded in EUA. If any of this information is incorrect, the user’s CAA should be contacted. The link “Click here to find the RGA for your organization” is available to assist users in finding their CAA.

The second section displays the System Access Status. In this example, the user is due for certification, and the due date is 01/31/2004. The third section displays the security CBT status. The example shows this as “DUE”, with a due date of 01/31/2004.

To certify system access, the user should click on Update System Access, at which time the System Access Certification screen (Figure 5) is presented.

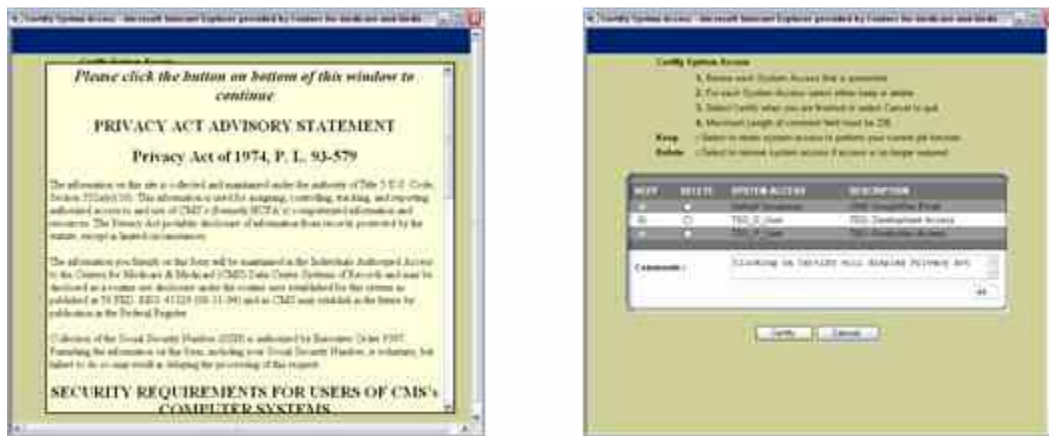
**Figure 5 — System Access Certification Screen**



This screen summarizes the accesses the user holds. The user is given the opportunity to select “KEEP” or “DELETE” for each access. The comments box may be used for any comments the user wishes to provide. Do not delete the default access at the top of the list.

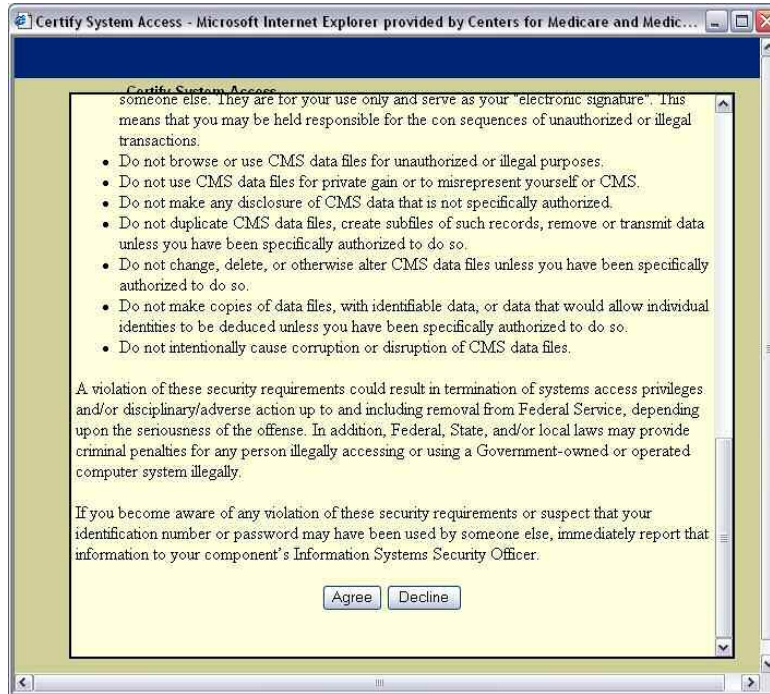
When the user has selected each access, click the Certify button. (You may need to use the scroll bar to scroll down to the button). The user is then presented with a Privacy Act statement (Figure 6).

**Figure 6 — Privacy Act Statement**



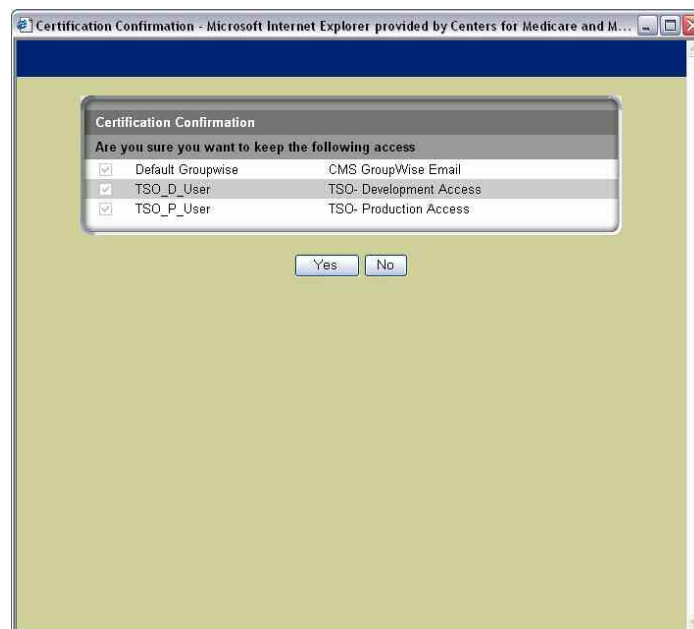
This statement is the same as the one on page 2 of the Application for Access to CMS Computer Systems Form, previously signed by the user. Scrolling down to the bottom of the screen reveals the Agree and Decline buttons, as illustrated in Figure 7.

**Figure 7 — Agree and Decline Buttons**



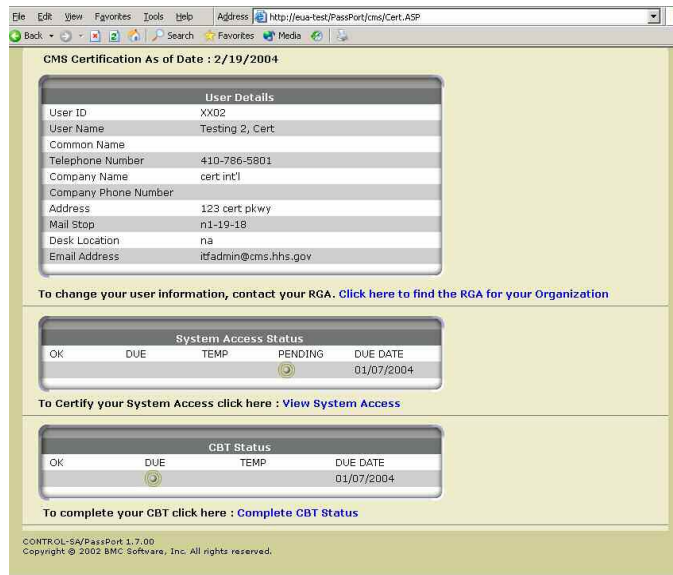
The user should click on Agree, at which time the confirmation screen (Figure 8) is displayed.

**Figure 8 — Confirmation Screen**



Selecting "Yes" completes the certification process for the user. At this time, the Certification screen changes the status to "PENDING," (Figure 9).

**Figure 9 — Certification Screen**

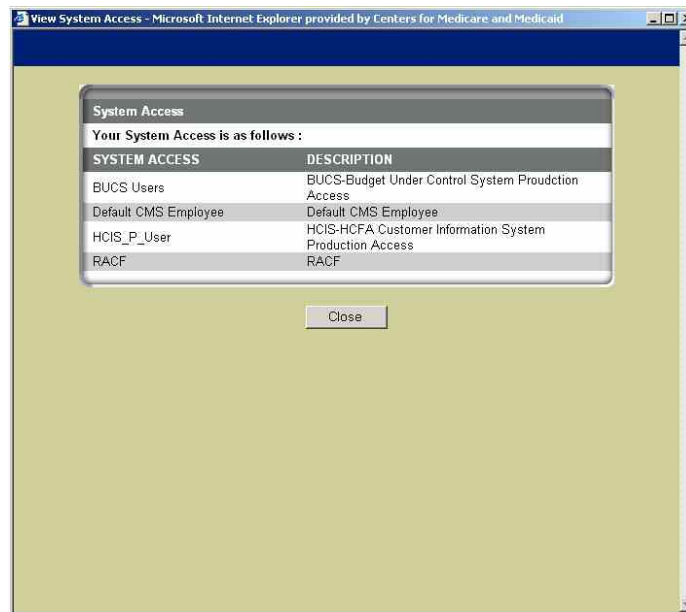


Notice that “Update System Access” has been changed to “View System Access.” The status is now set to “PENDING.” It will remain in this state until the certification has been approved by CMS, at which time the status will change to “OK.”

The “Complete CBT Status” link can be selected when the user is ready to take the security CBT. Upon completion, the status will not immediately change to “OK.” The status update process for the CBT takes 24 hours. Users are not considered completely certified until both the System Access Status and the CBT Status are set to OK.

Selecting the “View System Access” link will present the user with a summary of accesses, as illustrated in Figure 10.

**Figure 10 — Summary of Accesses**



Users can view their list of accesses at any time, not just during the certification process.

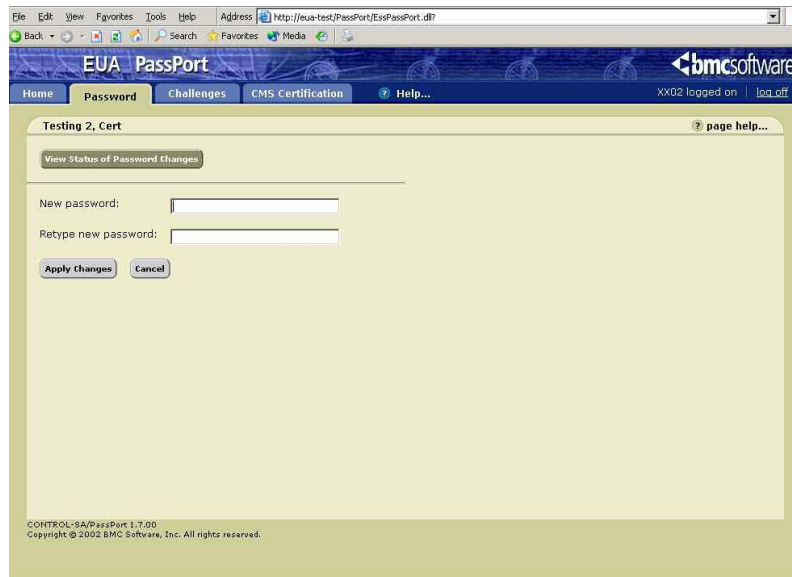
## 6.0 MANAGING PASSWORDS

The CMS processing environment is diverse. There are hundreds of applications hosted on a variety of platforms and servers. In an effort to reduce complexity for the users, CMS has instituted Password Propagation. This is not exactly the same as Password Synchronization. In synchronization, the systems ensure that passwords are the same on all accounts. With password propagation, changes are done natively on each platform, and password interception logic on some platforms causes the password change to be propagated to all others. This means that if a user changes the password on a database platform, such as Oracle or MS SQL, that change will not affect other platforms. CMS has ensured that password changes on platforms used for initial login, namely the mainframe, Windows NT and Active Directory, Remote Desktop (MetaFrame), Sun, and AIX, will be propagated to all other environments, including database platforms. As long as users change their passwords on one of these initial entry platforms, or use PassPort to change their passwords, all platforms will have the same password.

### 6.1 Using PassPort to Manage Passwords

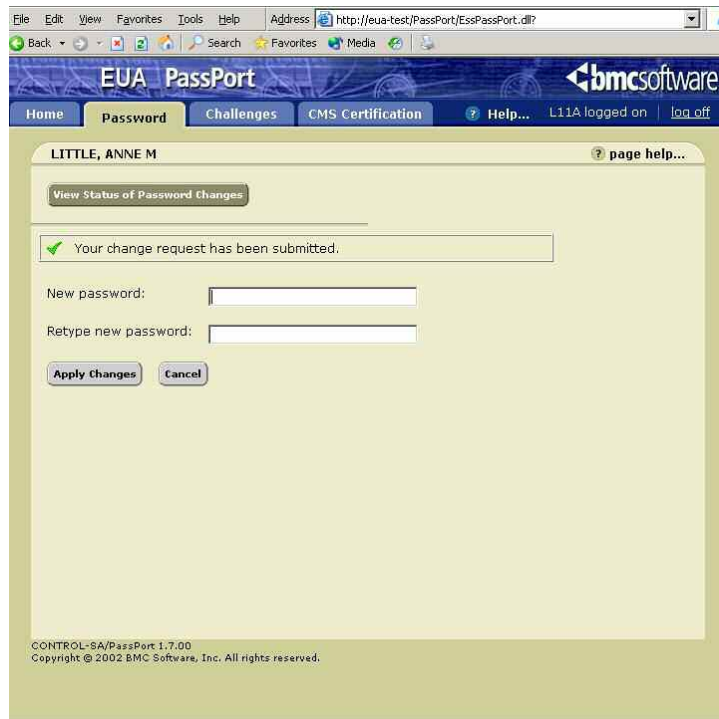
PassPort is the preferred tool for managing users' passwords. Selecting the Password tab on PassPort displays the following screen, as illustrated in Figure 11.

**Figure 11 — Password Screen**



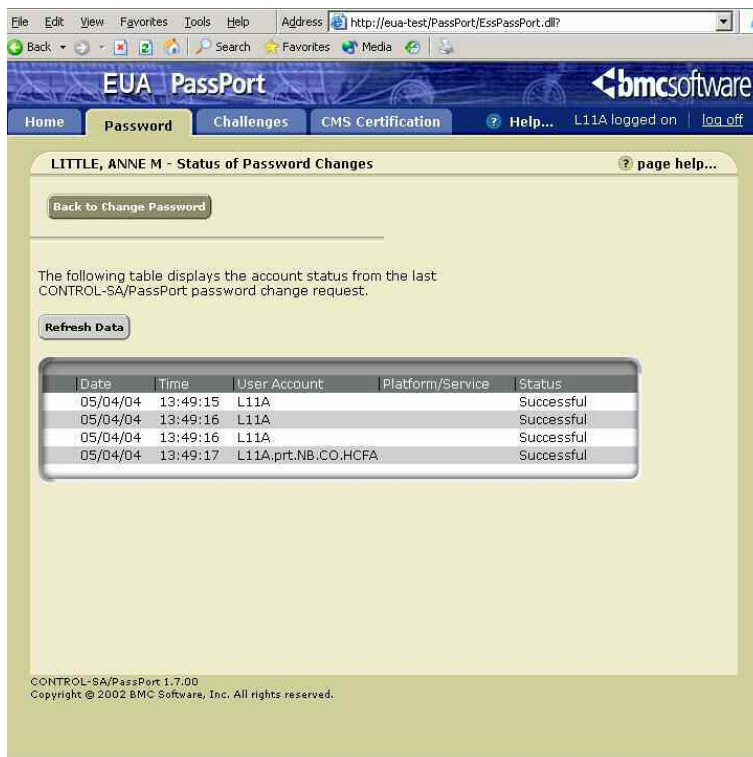
The user can then type the new password, retype it for confirmation, and select “[Apply Changes](#).” At this time, the screen will indicate the change was submitted, as illustrated in Figure 12.

**Figure 12 — Password Screen: Apply Changes**



The status of the changes on the various platforms can be viewed by selecting “View Status of Password Changes,” as illustrated in Figure 13.

**Figure 13 — View Status of Password Changes**



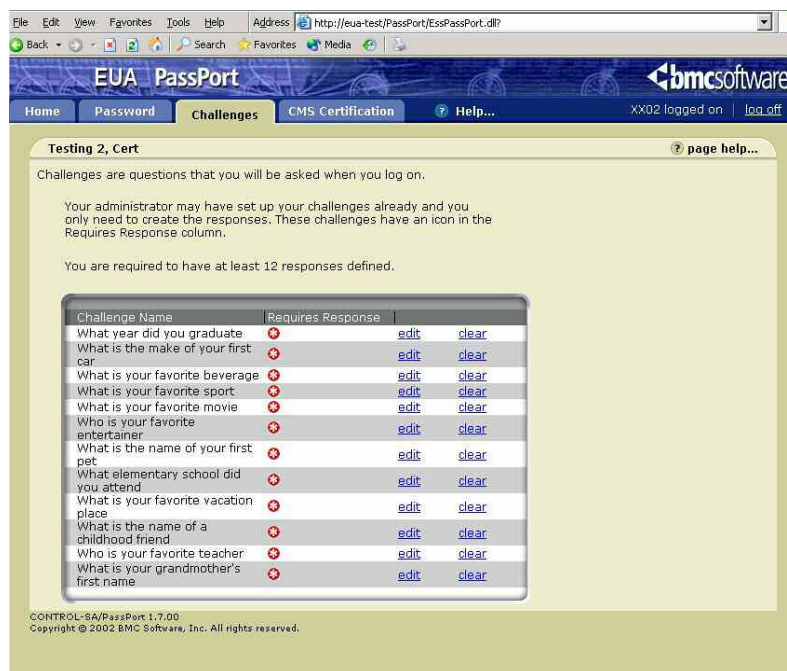
The display shows the status of the password change for all accounts. The user should wait until the status is “Successful” before attempting to log on with that account.

Use of PassPort is recommended. Users who cannot use PassPort can change their passwords when challenged by the platform and still have the change propagated to all other platforms, as long as the new password meets the CMS password standard. Some platforms may not be able to check the password for reserved words or character sequences. In this situation, the password change may work on the platform, but propagation to all other platforms will fail. The user will receive an e-mail stating that the password change only occurred on the local platform, and that propagation failed.

## 6.2 Setting up Challenges

PassPort can also be used by users who have forgotten their passwords, or who have been revoked by mistyping their passwords. In order to utilize this feature, users need to set up challenges that can be used to authenticate them prior to password reset. This is done by selecting the “Challenges” tab, as illustrated in Figure 14.

**Figure 14 — Challenges Tab**



The screen contains a list of challenges for which responses are needed. To establish a response for a given challenge select edit.

This brings up the “Edit Challenge” screen (Figure 15).



**Figure 15 — Edit Challenge Screen**

To set up the challenge, the user types and retypes the response, and selects “[Apply Changes](#).” Responses must be provided for **all** challenges. They must be a minimum of four characters, and the same response cannot be used for more than one challenge.

### 6.3 Logging on to PassPort without a Password

After the challenges and responses have been set up, the user can access PassPort without a password. This is done by selecting “[Log on without your password](#)” in the initial PassPort logon screen (Figure 16).

**Figure 16 — Log On Without Your Password Screen**

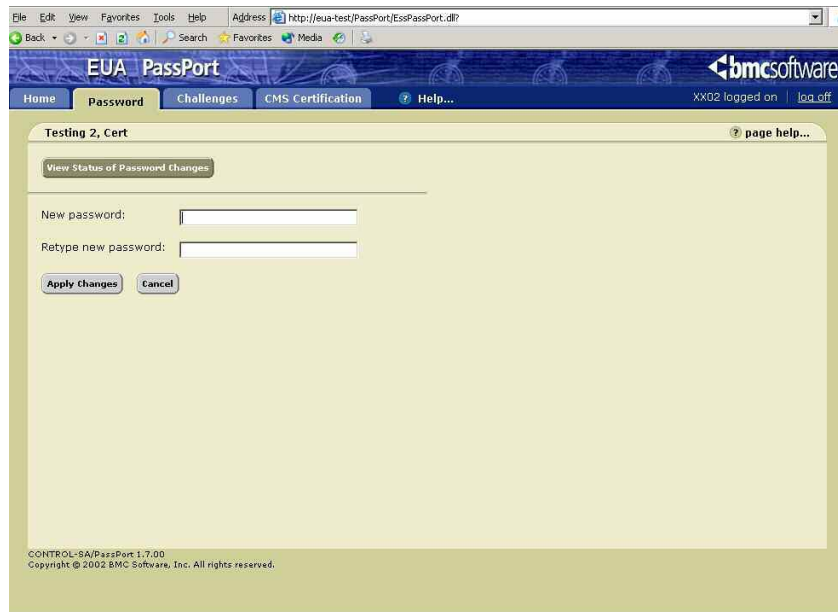
The user will be asked to provide responses to five randomly selected challenges (Figure 17).

**Figure 17 — Challenge 1 of 5 Randomly Selected Challenges Screen**



When all five are answered correctly, the user is allowed to access PassPort. At this time, the password can be changed by selecting the Password tab (Figure 18).

**Figure 18 — Password Tab**



Upon completion of the password change, all user accounts are restored with the new password, and the password is valid for 60 days.

## **6.4 Inactivity Revocation**

Users who have not changed their passwords for 120 days will have their User ID revoked. Since CMS' password policy requires a password change every 60 days, this means that some users can be revoked after 60 days of inactivity (those who used the system for 60 days after a password change and then stopped using it). On average, users will be revoked after 90 days of inactivity.

These User IDs will remain in a revoked state until the user contacts their CAA or the CMS Service Desk and requests they be reinstated. There is no limit to the number of times a User ID can be reinstated for inactivity. However, owners of CMS User IDs must perform annual certification for the User ID. If the User ID is not certified by the due date, it will be revoked, and then deleted 30 days later.

Certifying a CMS User ID does not exempt it from revocation for inactivity; conversely, inactive User IDs are not deleted unless they are not certified each year.

This policy allows infrequent and Internet-only users to retain their User IDs; it also enables purging of User IDs that no longer have a need to access CMS resources.

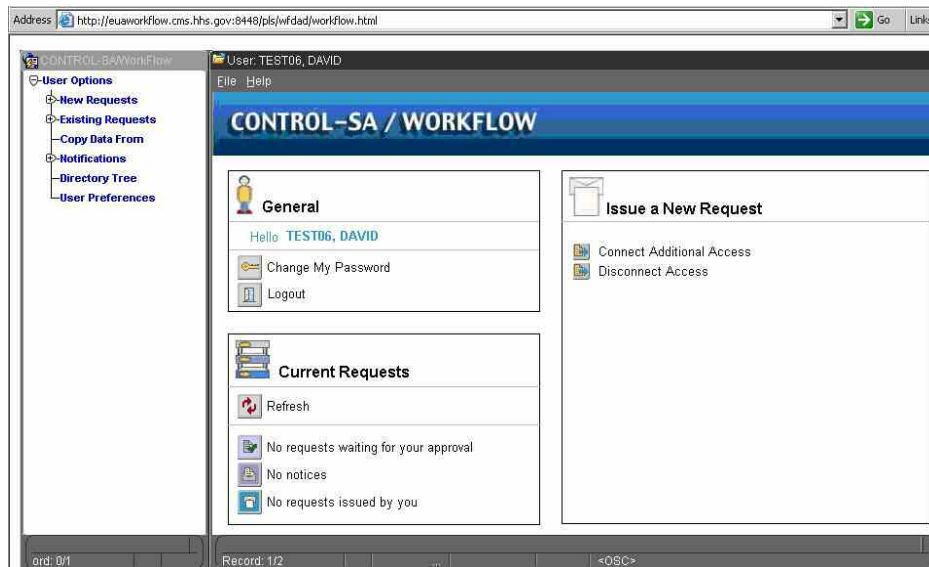
## 7.0 MANAGING EUA WORKFLOW

### 7.1 Connect Additional Access

Connect Additional Access is used when an employee or contractor has an active CMS User ID and additional access is required. You will need to have the user's first and last Name, their CMS User ID, typically a four-character alphanumeric ID, and the access they require. CMS access is defined through Job Codes.

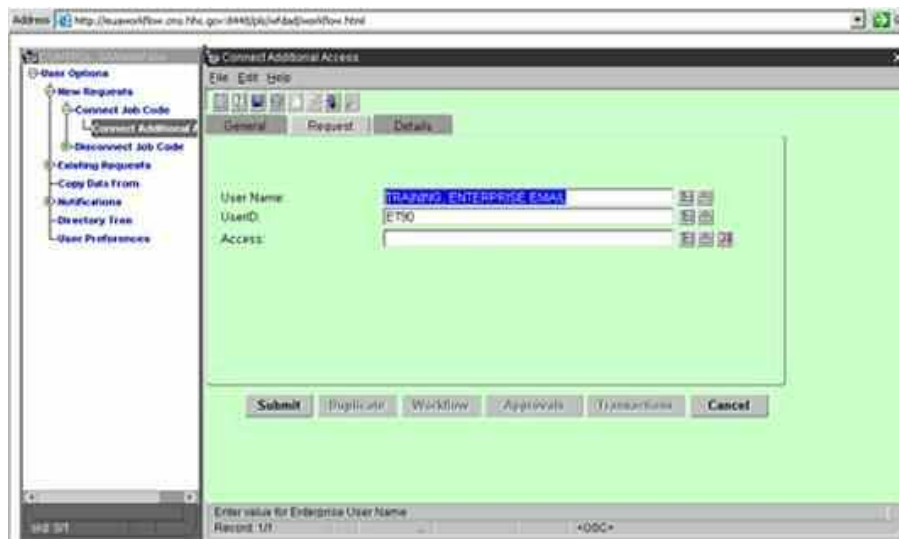
1. Sign on to WorkFlow.
2. Expand New Requests, then Connect Job Code, and click Connect Additional Access.
3. Click the Connect Additional Access icon on the Issue a New Request panel on the right of the screen (Figure 19).

**Figure 19 — WorkFlow Job Code – Connect Additional Access Screen**



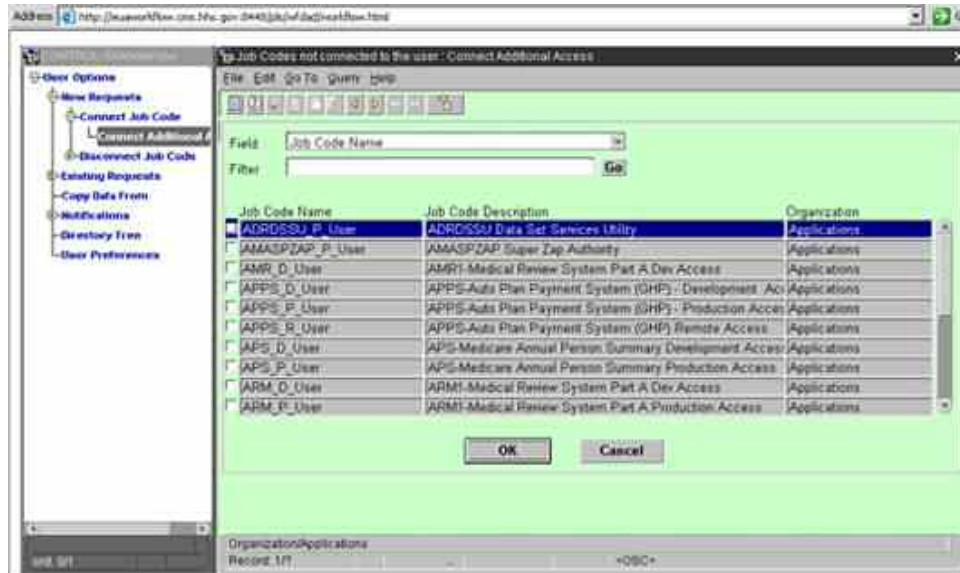
The WorkFlow Job Code Request Tab (Figure 20) is displayed.

**Figure 20 — WorkFlow Connect Job Code Request Tab**



4. Key in the four-character CMS User ID in CAPS in the User ID field then hit ENTER.
5. Verify the user's name.
6. Click the far right drop down box in the Access field to select Job Codes not connected to the user.

**Figure 21—WorkFlow Connect Job Code Access**



7. Enter all or part of a Job Code name representing the access the user requires (see list of links in section 3.13) followed by a percent sign (the % is a wild card character in WorkFlow) in the Filter field.
8. Click the Go box to the right of the Filter field.
9. Click in the far left box of the required Job Code displayed; a check mark will appear.
10. When more than one Job Code is required, repeat steps 7 through 9. There is a limit of nine Job Codes per request.
11. Click OK when all accesses are checked.
12. Job Codes will automatically populate the Access field.

**Figure 22—WorkFlow Connect Job Code Request Tab**

13. Click on the detail tab and enter the Contract Number and Justification (Figure 23).

**Figure 23 — WorkFlow Connect Job Code details Tab**

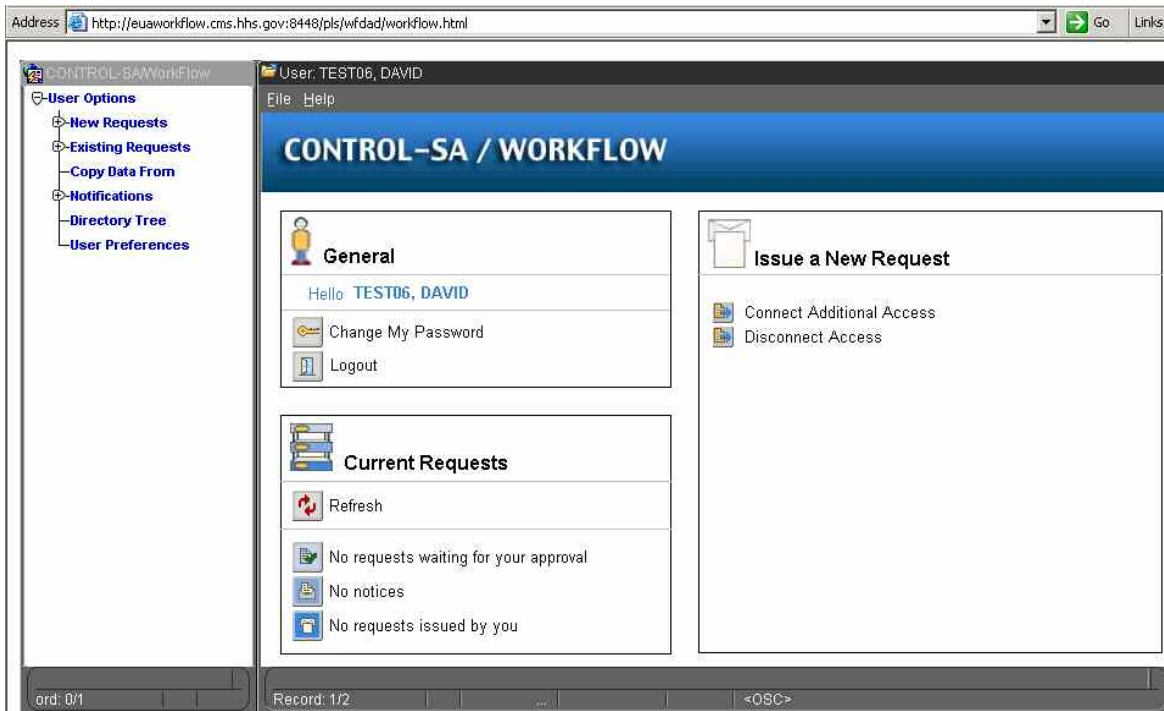
14. Submit request. A WorkFlow request number will be generated for your request. The request is routed to the designated approver. On approval, the access is granted.

### 7.1.1 Connects for RACF Job Codes

1. Sign on to WorkFlow
2. Expand New Requests
3. Expand Connect Job Code
4. Click Connect Additional Access

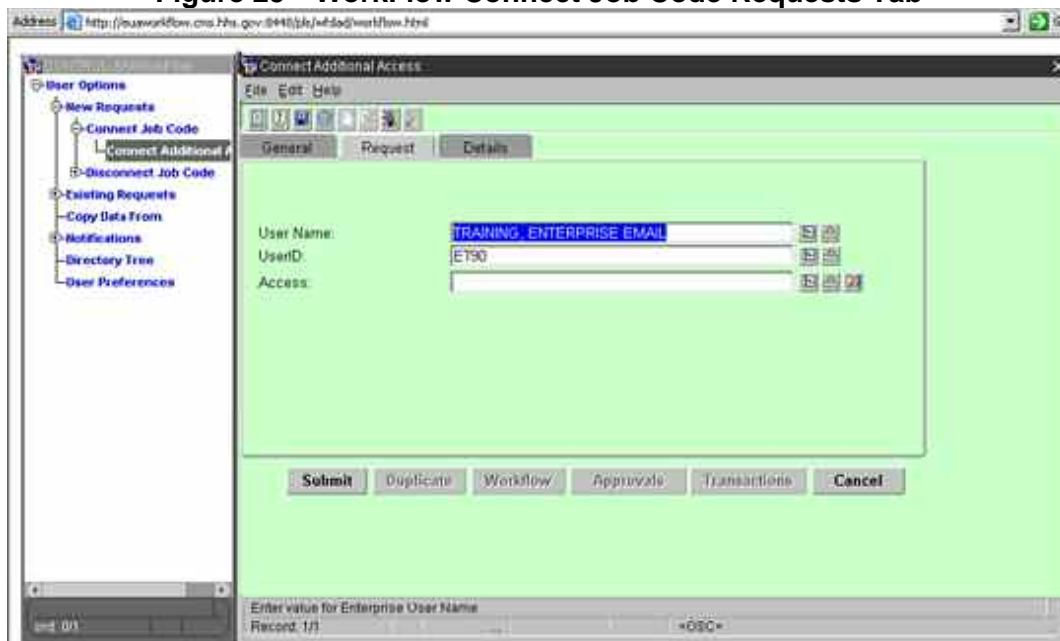
Scroll to the bottom of the Issue a New Request panel on the right and click the Connect Additional Access icon.

**Figure 24—WorkFlow Connect Job Codes**



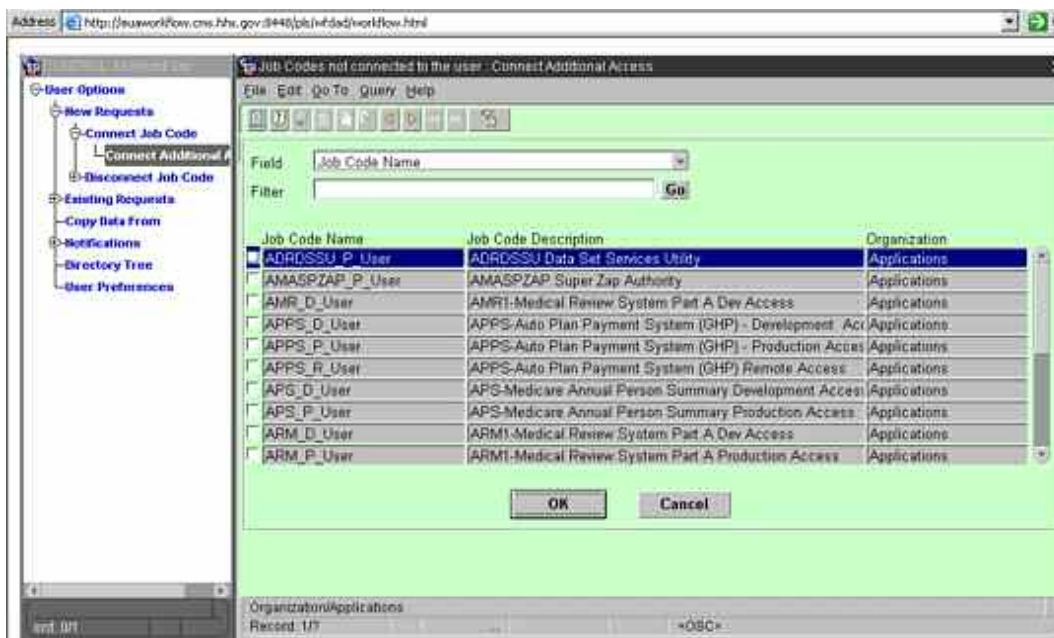
The screen, as illustrated in Figure 25, is displayed.

**Figure 25—WorkFlow Connect Job Code Requests Tab**



5. Key in the four-character CMS User ID in CAPS in the User ID field then type ENTER.
6. Verify the user's name.
7. Click the far right drop down box in the Access field to select Job Codes not connected to the user.

**Figure 26—WorkFlow Connect Job Code Access**

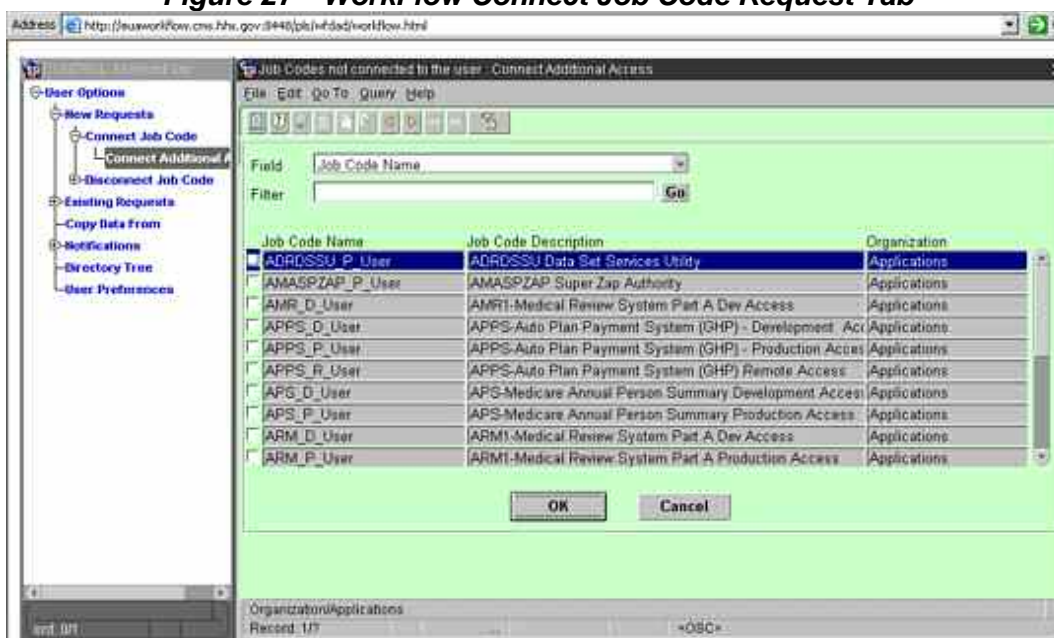


8. Enter all or part of a Job Code name representing the access the user requires (see list of Job Codes) followed by a percent sign (the % is a wild card character in WorkFlow) in the Filter field.

NOTE For Mainframe HLQ access, the Job Code is always 'HLQ\_XXX', Where 'XXX' is the three character application.

9. Click the Go box to the right of the Filter field.
10. Click in the far left box of the required Job Code displayed; a check mark will appear.
11. When more than one Job Code is required, repeat steps 1 through 3. There is a limit of nine Job Codes per request.
12. Click OK when all accesses are checked.
13. Job Codes will automatically populate the Access field.

**Figure 27—WorkFlow Connect Job Code Request Tab**





**Figure 28—WorkFlow Connect Job Request Tab**

The screenshot shows a web browser window with the URL <http://euaworkflow.cml.hhi.gov:9443/ps-afad3/workflow.html>. The main content area is a dialog box titled "Connect Additional Access" with a menu bar (File, Edit, Utilities, Help) and a toolbar. The "Request" tab is selected, showing three input fields: "User Name" with the value "TEST06, DAVID", "UserID" with "TEST06", and "Access" with "HLQ\_MRD". Below the fields are buttons for "Submit", "Duplicate", "Workflow", "Approvals", "Transactions", and "Cancel". A status bar at the bottom indicates "Record: 1/1".

14. Click on the **Detail** tab and enter the justification and Contract Number.
15. Enter the contract number.
16. In the **Justification** field, enter the specific dataset(s) requested, followed by the type of access, read, alter, update. Separate each dataset with a comma.

**Figure 29—WorkFlow Connect Job Code Details Tab**

The screenshot shows the same "Connect Additional Access" dialog box, but with the "Details" tab selected. The "Request" tab is now disabled. The "Contract/Grant Number" and "Justification" fields are visible. The "Submit" button is highlighted. The status bar at the bottom indicates "Record: 1/1".

17. Submit request. A WorkFlow request number will be generated for your request.

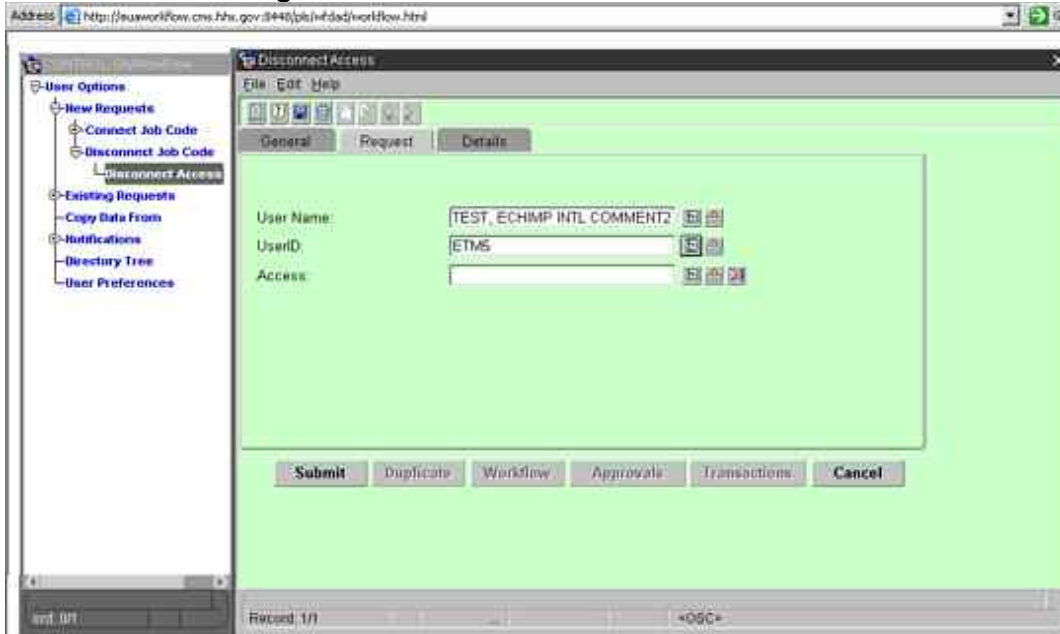
## 7.2 Disconnect Job Code

Expand Disconnect Job Code in the pane on the left. Select Disconnect Access.

OR simply scroll to the bottom of the Issues New Request panel on the right and click the Disconnect Access icon.

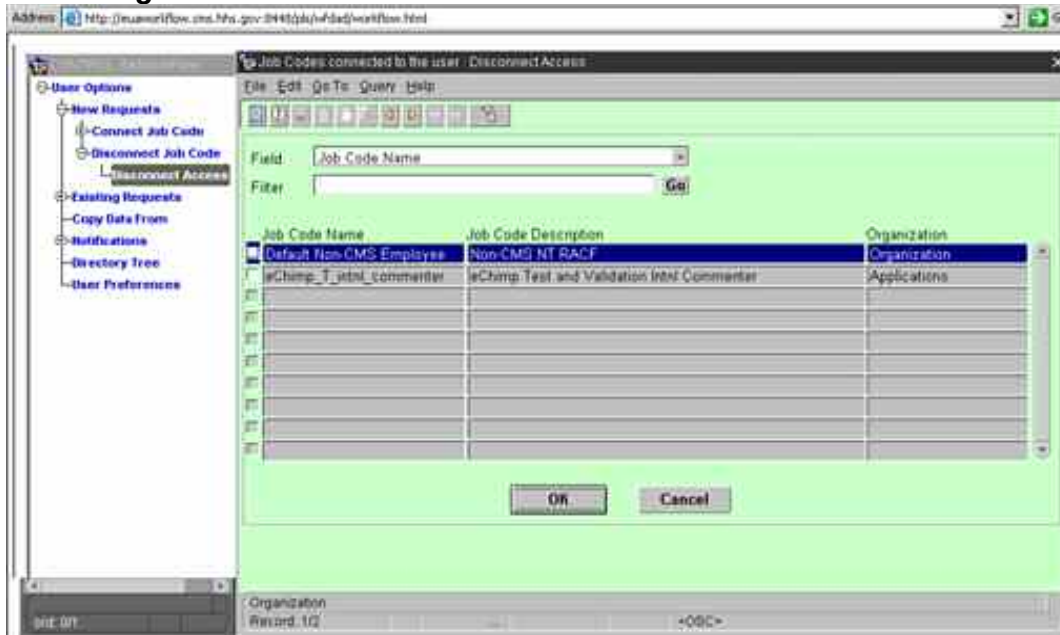
The Disconnect Access screen is displayed. Using the same procedure as used for Connect Additional Access, find the desired user, as illustrated in Figure 30.

**Figure 30—WorkFlow Disconnect Access**



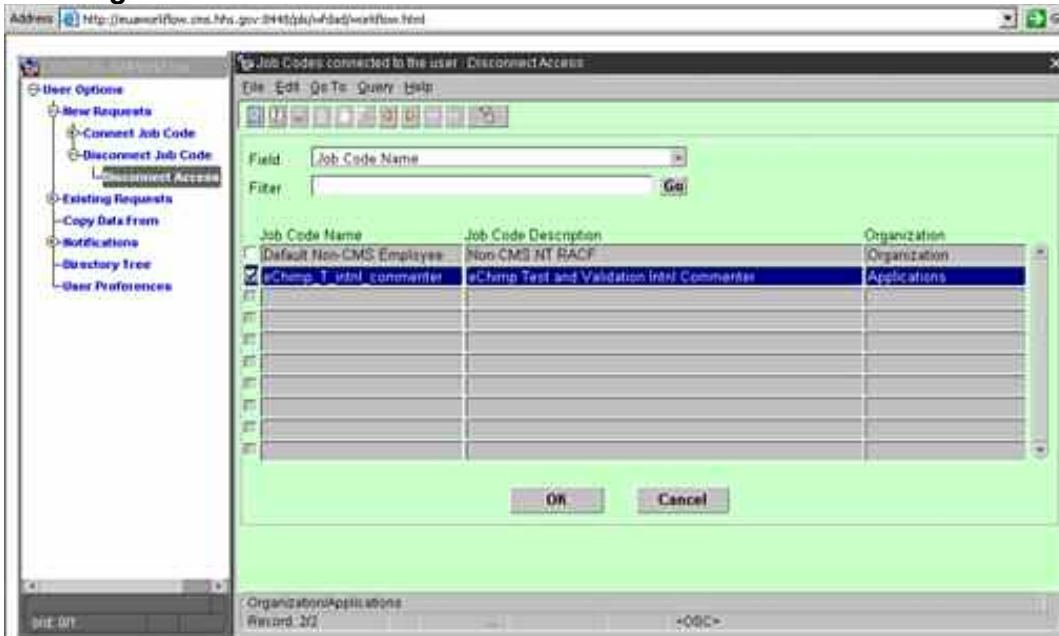
Click the far right drop down box in the Access field to list all Job Codes connected to the user.

**Figure 31—WorkFlow Disconnect Access Job Code Selection**



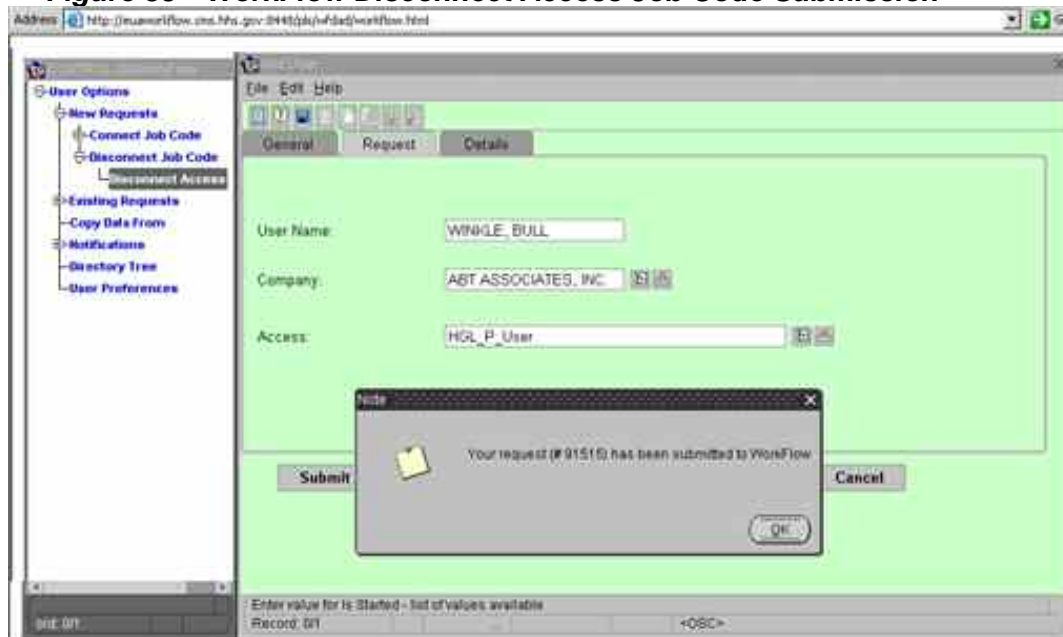
The screen lists the Job Codes connected to the user. Click far left box next to the Job Code or access no longer required; a check mark will appear.

**Figure 32—WorkFlow Disconnect Access Job Code Selection**



1. Click OK. The Job Code to be disconnected will automatically populate in the Access field.
2. Click on the Details tab and enter the justification and Contract Number.

**Figure 33—WorkFlow Disconnect Access Job Code Submission**



Submit the request in the Disconnect Access screen. A WorkFlow request number will be generated for your request.

The request is routed to the designated approver. On approval, the access is removed.

### 7.3 IT Support Icon (Creating a trouble ticket for EUA support for CMS Employees only)

EUA support is handled through the trouble ticket process. In lieu of contacting the CMS IT Service Desk to open a trouble ticket for you, you can open your own by utilizing the IT SUPPORT icon found on your workstation.


To open a trouble ticket, follow the few steps below.

Double-click the IT SUPPORT icon found on your workstation and satisfy the security alerts.



Log in using your CMS four-character User ID and current password.

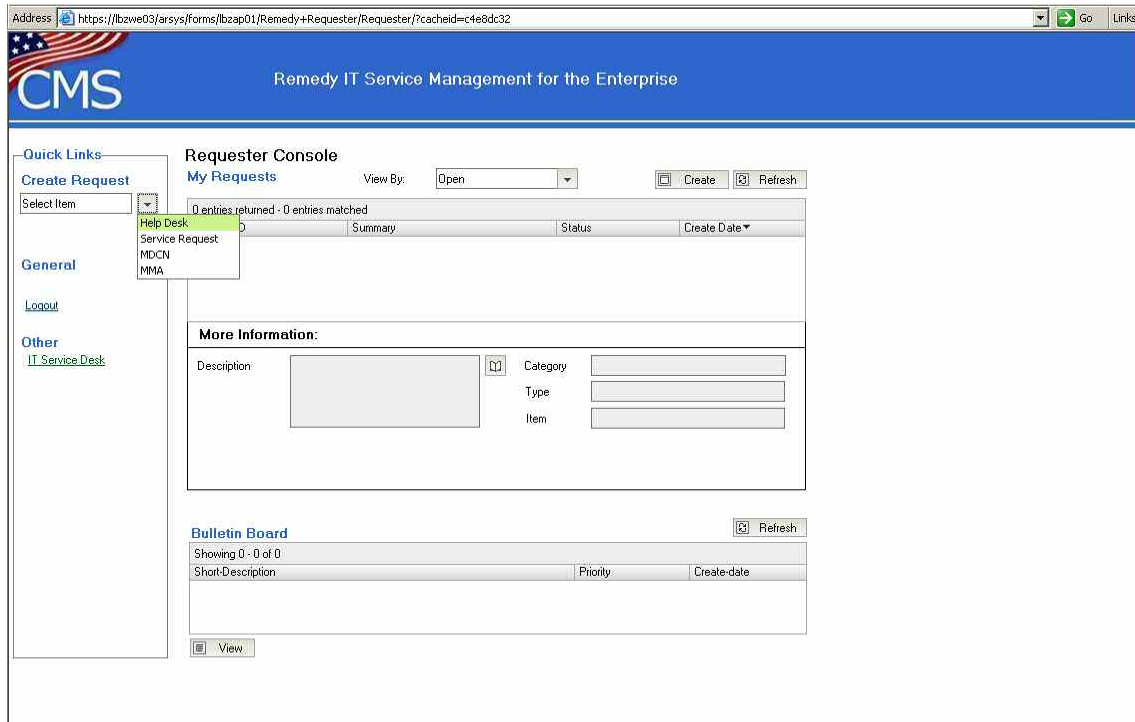
**Figure 34—IT Support Logon**



The screenshot shows a web browser window with the address bar containing `https://lbzwe03/arsys/shared/login.jsp`. The page title is "CMS IT Support Online - Login Page". The CMS logo is visible in the top left corner. A message states: "Pop-ups must be enabled for the web page to work properly." Below this is a "Welcome" heading and a login form with the following fields: "User Name\*" (text input), "Password" (text input), and "Authentication" (dropdown menu set to "HCFA.GOV"). There are "Login" and "Clear" buttons below the form. At the bottom, there is a note: "If you are having problems logging in or would rather speak directly with a Service Desk Analyst, please contact the CMS IT Service Desk at 410-786-2580 or 1-800-562-1963."

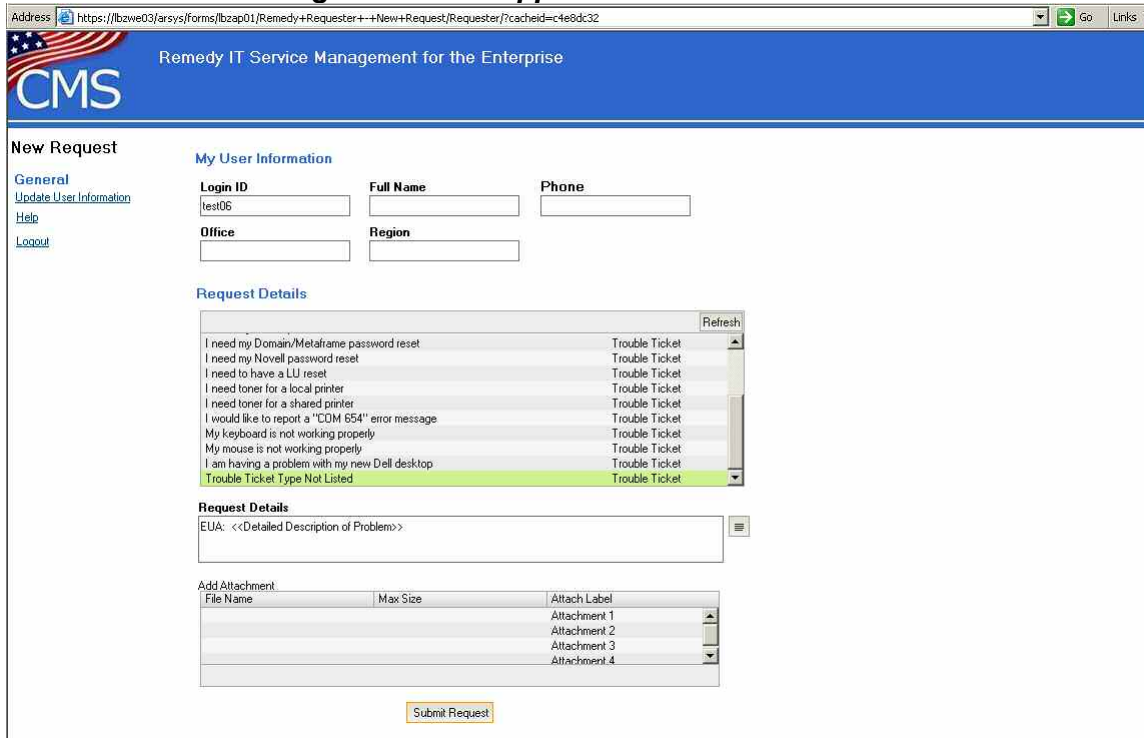
After you have logged in, you will see the window, as illustrated in Figure 35.

**Figure 35—IT Support Main Screen**



Click on the downward arrow under Create Request on the far left of your screen. Select Help Desk. This screen will pop up. Make sure the information in My User Information is correct before proceeding.

**Figure 36—IT Support Trouble Ticket Submission**



1. In the first box underneath Request Details, scroll down to the bottom of the list and select the last item, Trouble Ticket Type Not Listed.

2. In the next box, prefix your problem or question with **EUA:** Give a detailed description of problem or a specified question. Attach files if needed.
3. Click the **Submit Request** button.

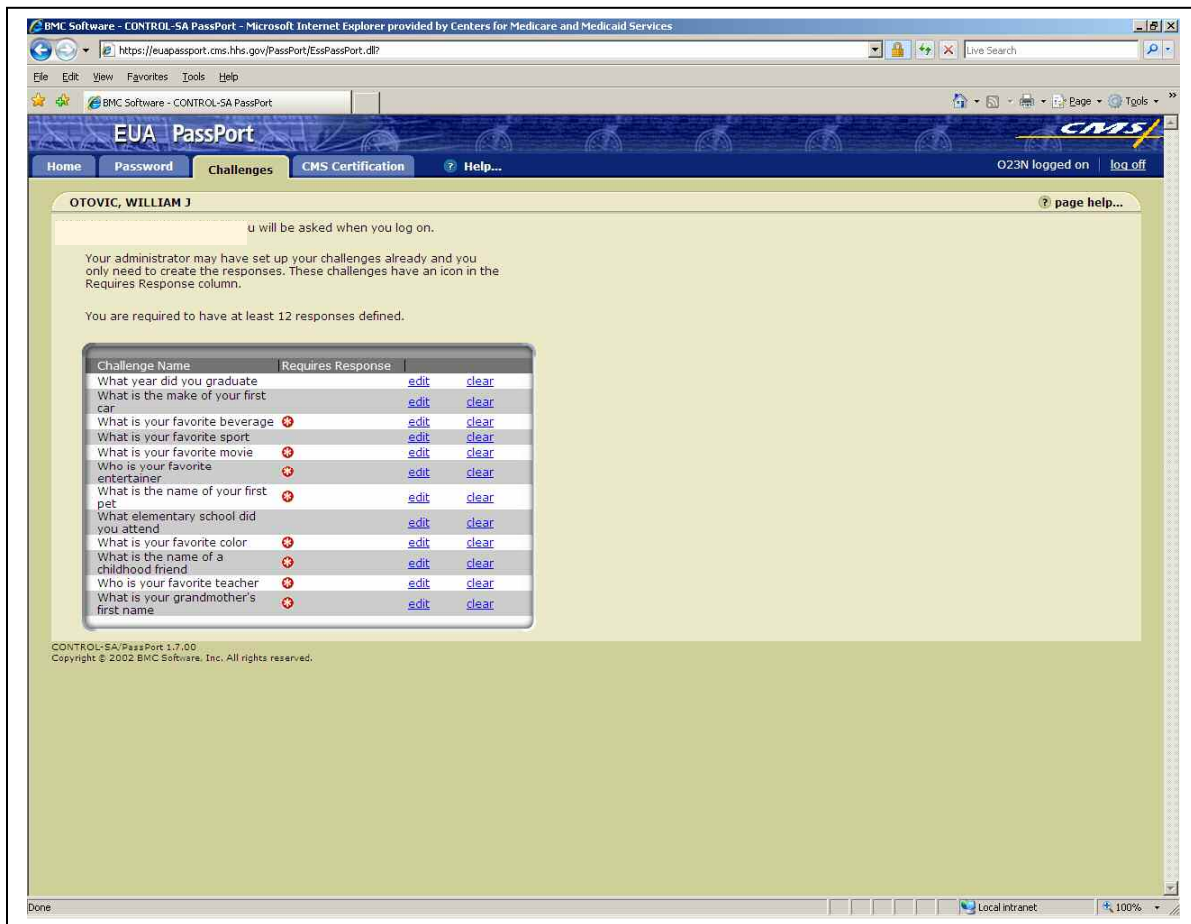
This window will close and the Remedy Console will now have your trouble ticket as being open.

## 8.0 SETTING UP CHALLENGE QUESTIONS IN EUA PASSPORT

### 8.1 Log into passport

Challenge Question are used when an employee or contractor has forgot their password. You will need to have the challenge questions completed in order to be able to log on without your password.

1. Sign on to Passport
2. Click on the Challenges Tab
3. Ensure that all questions are answered. Once this is complete you will have no more RED “X”’s



**Figure 37—Passport Challenge Questions**