

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)

Users Guide

Version 1.7
February 4, 2010

Revision History

Date	Version	Description of Changes
08/12/2006	1.0	Initial document
11/28/2006	1.1	Added Section 7.0 Managing EUA Workflow
03/13/2007	1.2	Semi-annual review
06/27/2007	1.3	Semi-annual review
01/19/2008	1.4	Update Captioning for 508 Compliance
03/13/2008	1.5	Added Section 8.0 Setting up Challenge Questions
12/28/2009	1/6	Added Section 5.2 Access EUA PassPort from the Internet
02/04/2010	1.7	Review and Update

Contents

1.0	INTRODUCTION	5
2.0	NEW USER REQUESTS.....	6
3.0	USER CHANGE REQUESTS	7
4.0	CMS USER ID CERTIFICATION REQUIREMENTS	8
5.0	EUA PASSPORT	9
5.1	Installation of PassPort	9
5.2	Accessing EUA PassPort from the Internet.....	9
5.3	Accessing EUA Passport from the CMS Network	11
5.4	PassPort Home Screen	12
5.5	PassPort Certification Screens	13
6.0	MANAGING PASSWORDS	20
6.1	Using PassPort to Manage Passwords	20
6.2	Setting up Challenge Questions in EUA PassPort	22
6.3	Logging on to PassPort without a Password	24
6.4	Inactivity Revocation.....	27
7.0	MANAGING EUA WORKFLOW	28
7.1	Connect Additional Access.....	28
7.1.1	Connects for RACF Job Codes	31
7.2	Disconnect Job Code.....	35
7.3	IT Support Icon (Creating a trouble ticket for EUA support for CMS Employees only)	38

List of Figures

Figure 1 – PassPort Logo	9
Figure 2 — CMS SSLVPN Logon	10
Figure 3 — CMS Security Notice.....	10
Figure 4 — EUA PassPort Log On Page	11
Figure 5 — PassPort Log On	12
Figure 6 — PassPort Home Screen.....	13
Figure 7 — PassPort Certification Screen.....	14
Figure 8 — System Access Certification Screen.....	15
Figure 9 — Privacy Act Statement.....	16

Figure 10 — Agree and Decline Buttons.....	16
Figure 11 — Confirmation Screen	17
Figure 12 — Certification Screen.....	18
Figure 13 — Summary of Accesses	19
Figure 14 — Password Screen	20
Figure 15 — Password Screen: Apply Changes.....	21
Figure 16 — View Status of Password Changes	22
Figure 17 — Challenges Tab	23
Figure 18 — Edit Challenge Screen	24
Figure 19 — Log On Without Your Password Screen.....	25
Figure 20 — Five Randomly Selected Challenges Screen.....	26
Figure 21 — Passwords Tab	27
Figure 22 — WorkFlow Connect Job Code	28
Figure 23 — WorkFlow Connect Job Code Request Tab	29
Figure 24 — WorkFlow Connect Job Code Access	29
Figure 25 — WorkFlow Connect Job Code Request Tab	30
Figure 26 — WorkFlow Connect Job Code Details Tab.....	31
Figure 27 —WorkFlow Connect Job Codes	32
Figure 28 — WorkFlow Connect Job Code Requests Tab.....	32
Figure 29 — WorkFlow Connect Job Code Access	33
Figure 30 — WorkFlow Connect Job Code Request Tab	34
Figure 31 — WorkFlow Connect Job Request Tab	34
Figure 32 — WorkFlow Connect Job Code Details Tab.....	35
Figure 33 — WorkFlow Disconnect Access.....	36
Figure 34 — WorkFlow Disconnect Access Job Code Selection.....	36
Figure 35 — WorkFlow Disconnect Access Job Code Selection.....	37
Figure 36 — WorkFlow Disconnect Access Job Code Submission.....	37
Figure 37 — IT Support Icon	38
Figure 38 — IT Support Logon	38
Figure 39 — IT Support Main Screen.....	39

Figure 40 — IT Support Trouble Ticket Submission.....39

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. Therefore, it 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. 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 Accessing EUA PassPort from the Internet

EUA Passport can be accessed from any internet connection by using the CMS Secure Socket Layer (SSL) Virtual Private Network (VPN) at <https://vpnext.cms.hhs.gov/EUA>.

The CMS SSL VPN provides a secure means of using EUA Passport services via the internet, including self-service password resets and submitting System Access Certification requests.

NOTE The CMS SSL VPN cannot be used while connected to the CMS network (intranet/extranet/MDCN/WAN).

To use EUA Passport from the internet:

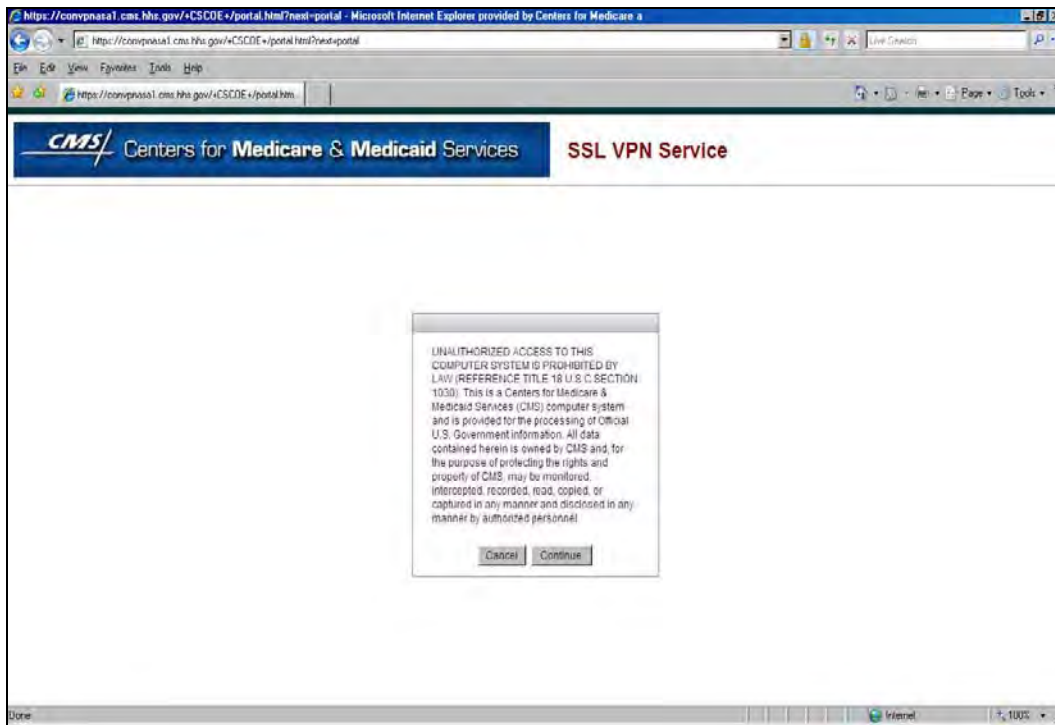
1. Logon to the CMS SSL VPN at <https://vpnext.cms.hhs.gov/EUA> using your CMS User Id and password and group as EUA (Figure 2).

Figure 2 — CMS SSLVPN Logon



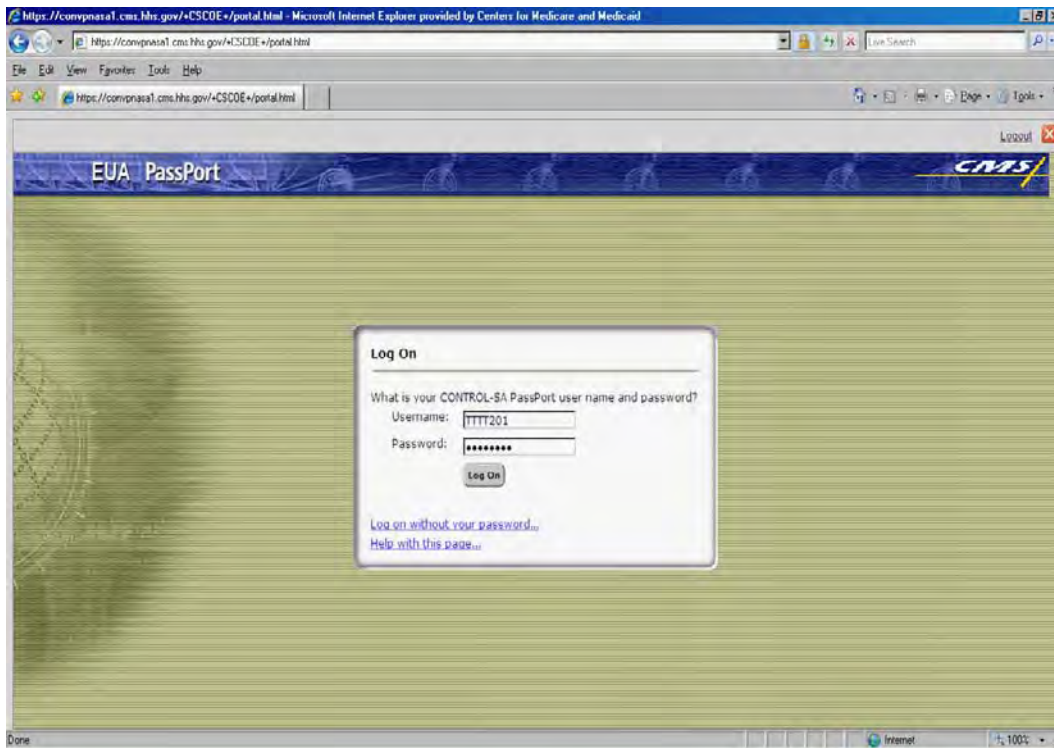
2. After verification of your User Id, password, and acknowledgement of the security notice (Figure 3), the EUA Passport logon page will be displayed.


Figure 3 — CMS Security Notice



3. Logon to the EUA Passport using your CMS User Id and password (Figure 4).

Figure 4 — EUA PassPort Log On Page



The Section 5.3 describes how to use EUA passport. After you logout of passport, you have to logout from CMS SSL VPN by clicking the logout icon  on top right hand corner of the page. Moving the mouse pointer over the top right hand page will show you the SSL VPN toolbar.

5.3 Accessing EUA Passport from the CMS Network

PassPort is accessed by entering the following URL in the Web browser:

<https://euapassport.cms.hhs.gov/passport/> or <https://158.73.79.141/passport>

Users then enter their CMS enterprise User ID and password illustrated in Figure 5.

Figure 5 — PassPort Log On

EJA PassPort **CMS**

Log On

What is your CONTROL-SA PassPort user name and password?

Username:

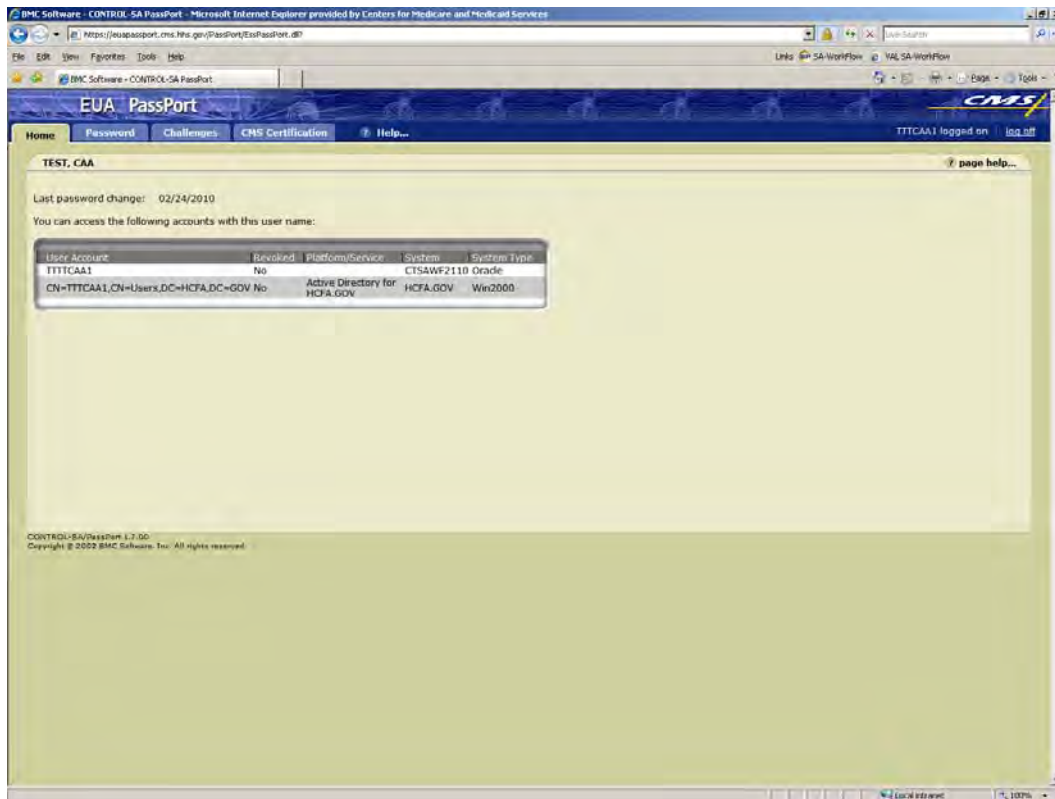
Password:

[Log on without your password...](#)

[Help with this page...](#)

5.4 PassPort Home Screen

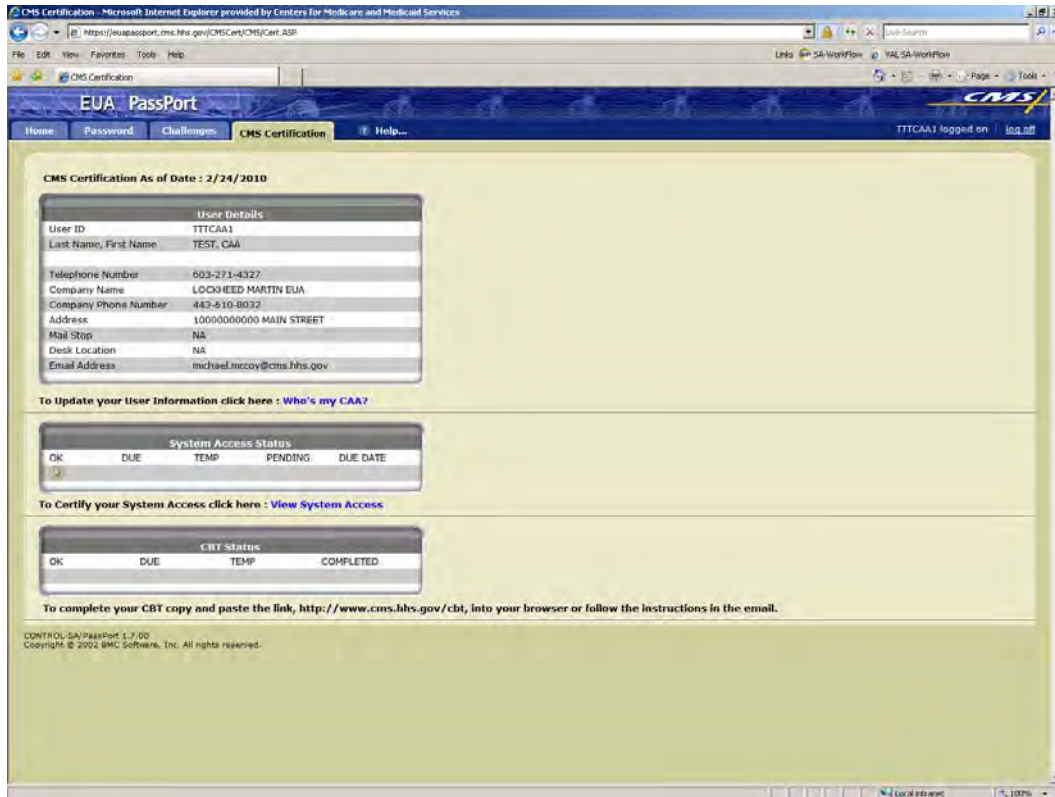
Upon successful login to PassPort, the user is presented with the home screen illustrated in Figure 6.

Figure 6 — PassPort Home Screen

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

5.5 PassPort Certification Screens

Selecting the CMS Certification tab brings up the following screen, illustrated in Figure 7.

Figure 7 — 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 "Who's my CAA?" is available to assist users in finding their CAA.

The second section displays the System Access Status. In this example, the user status is OK. The third section displays the security CBT status. The example shows the status is OK.

To certify system access, the user should click on Update System Access, at which time the following screen illustrated in Figure 8 is presented.

Figure 8 — System Access Certification Screen

Certify System Access

1. Review each System Access that is presented
2. For each System Access select either keep or delete
3. Select Certify when you are finished or select Cancel to quit
4. Maximum Length of comment field must be 235.

Keep : Select to retain system access to perform your current job function
Delete : Select to remove system access if access is no longer required

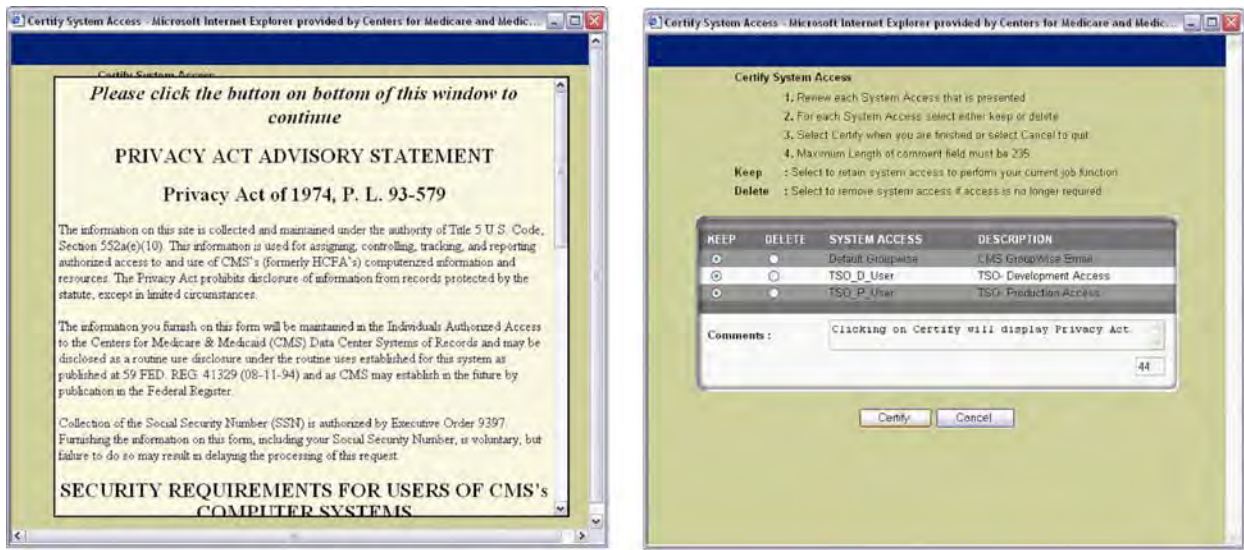
KEEP	DELETE	SYSTEM ACCESS	DESCRIPTION
<input type="radio"/>	<input type="radio"/>	Default Groupwise	CMS GroupWise Email
<input type="radio"/>	<input type="radio"/>	TSO_D_User	TSO- Development Access
<input type="radio"/>	<input type="radio"/>	TSO_P_User	TSO- Production Access

Comments :

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.

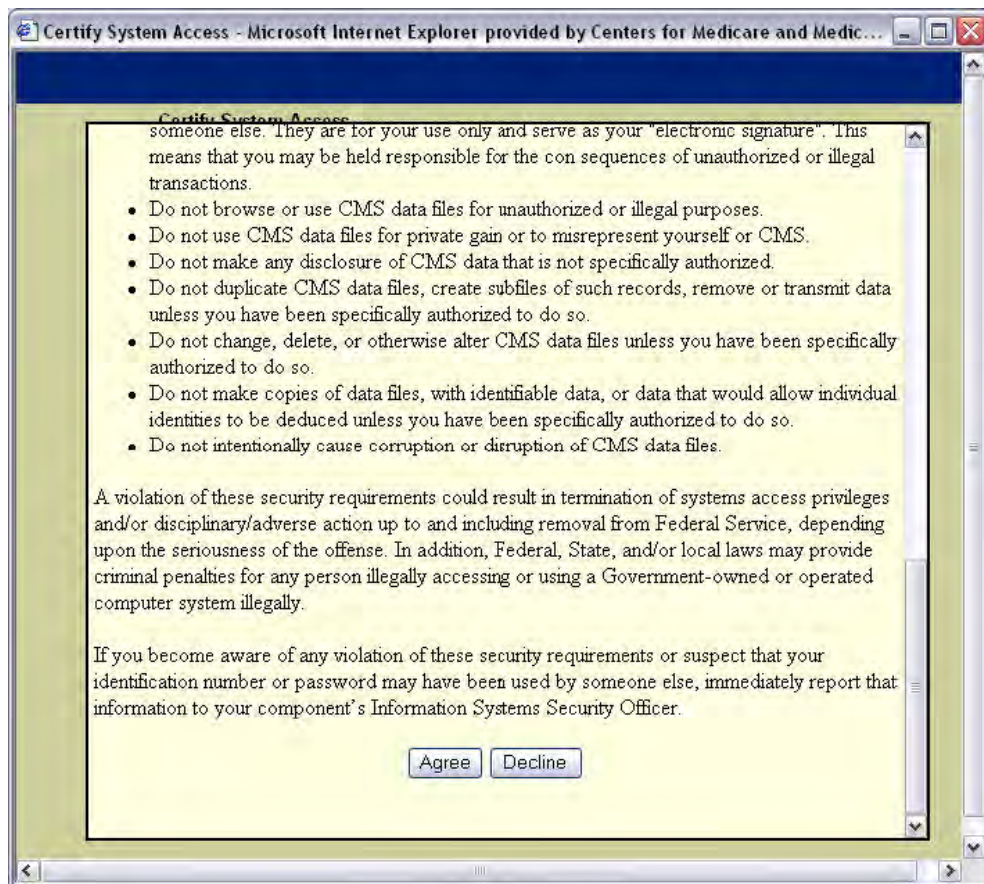
When the user has made a selection for each access, “Certify” is selected. (You may need to use the scroll bar to scroll down to the button). The user is then presented with a Privacy Act statement, illustrated in Figure 9.

Figure 9 — Privacy Act Statement



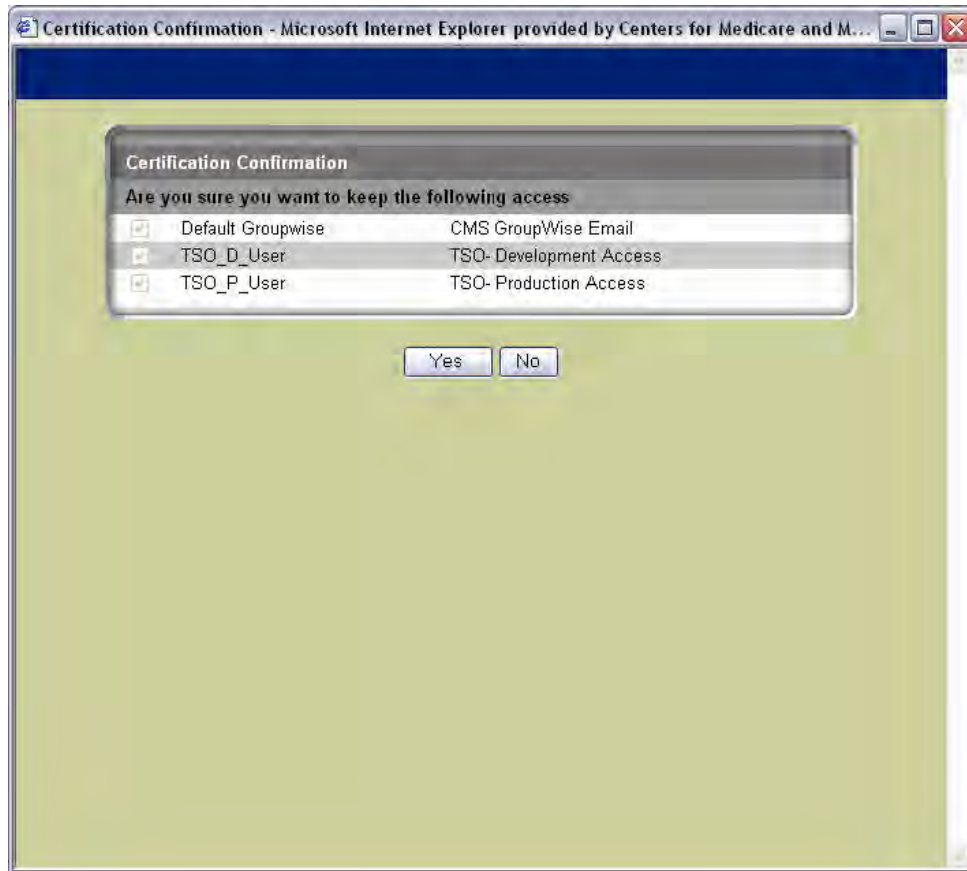
This statement is the same as the one on page 2 of the Application for Access to CMS Computer Systems Form, previously signed by the user. Scrolling down to the bottom of the screen reveals the Agree and Decline buttons, as illustrated in Figure 10.

Figure 10 — Agree and Decline Buttons



The user should click on Agree, at which time the following confirmation screen is displayed, as illustrated in Figure 11.

Figure 11 — Confirmation Screen



Selecting “Yes” completes the certification process for the user. At this time, the Certification screen changes the status to “PENDING,” as illustrated in Figure 12.

Figure 12 — Certification Screen

The screenshot shows a web browser window with the address bar displaying `http://eua-test/PassPort/cms/Cert.ASP`. The page title is "CMS Certification As of Date : 2/19/2004".

User Details

User ID	XX02
User Name	Testing 2, Cert
Common Name	
Telephone Number	410-786-5801
Company Name	cert int'l
Company Phone Number	
Address	123 cert pkwy
Mail Stop	n1-19-18
Desk Location	na
Email Address	itfadmin@cms.hhs.gov

To change your user information, contact your RGA. [Click here to find the RGA for your Organization](#)

System Access Status

OK	DUE	TEMP	PENDING	DUE DATE
			<input checked="" type="radio"/>	01/07/2004

To Certify your System Access click here : [View System Access](#)

CBT Status

OK	DUE	TEMP	DUE DATE
	<input checked="" type="radio"/>		01/07/2004

To complete your CBT click here : [Complete CBT Status](#)

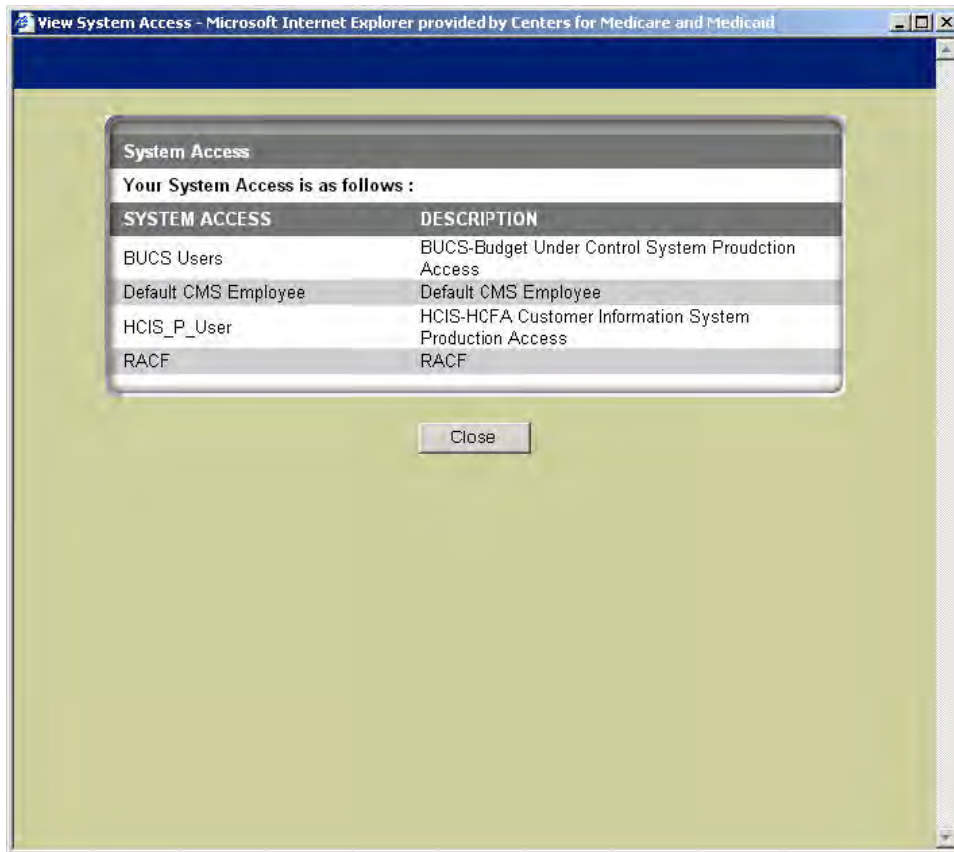
CONTROL-SA/PassPort 1.7.00
Copyright © 2002 BMC Software, Inc. All rights reserved.

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 13.

Figure 13 — 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.

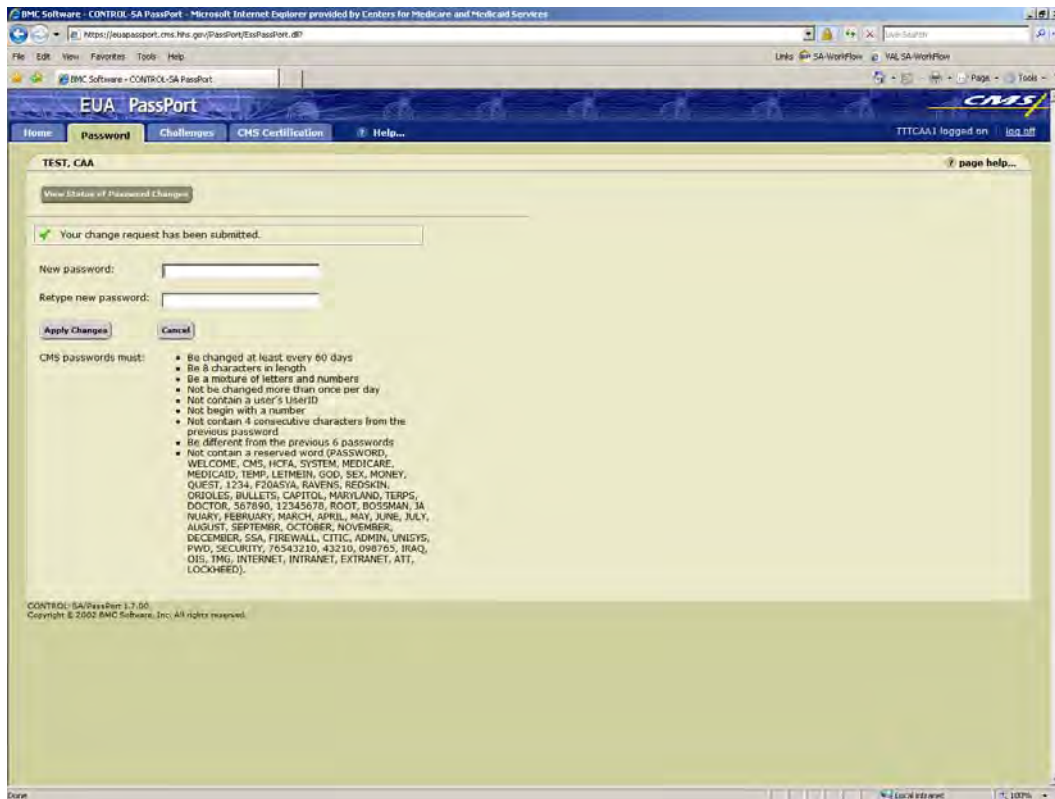
6.1 Using PassPort to Manage Passwords

PassPort is the preferred tool for managing users' passwords. Selecting the Password tab on PassPort displays the following screen, as illustrated in Figure 14.

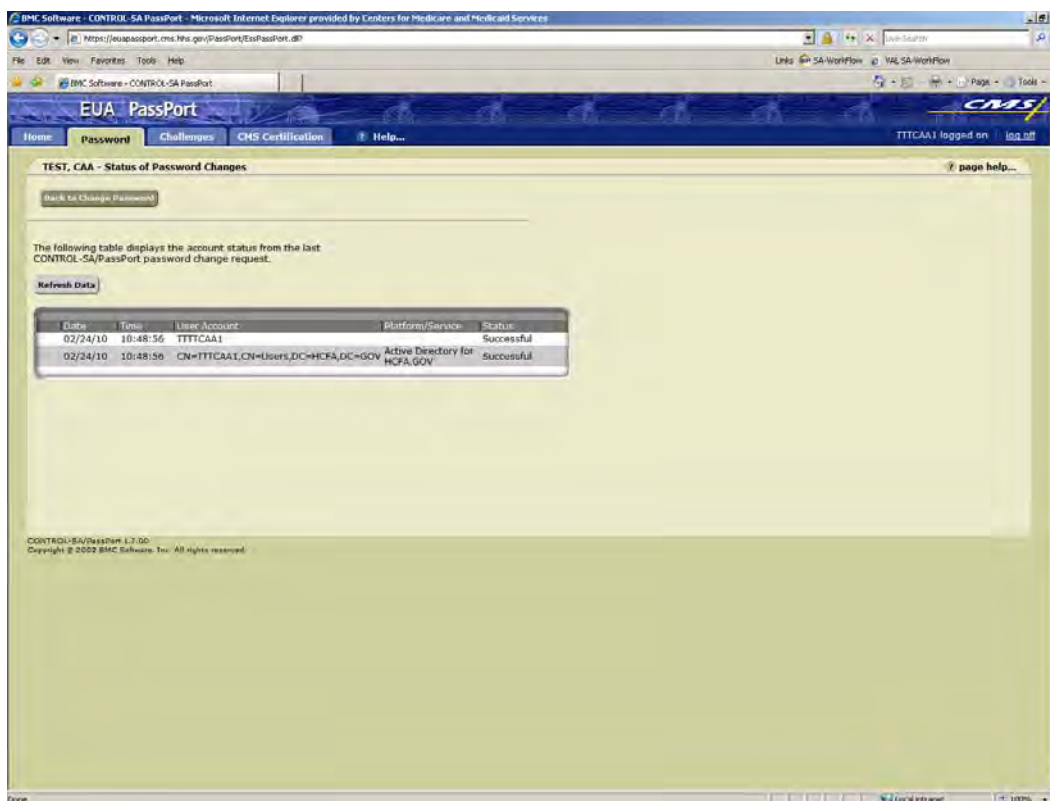
Figure 14 — Password Screen

The user can then type the new password, retype it for confirmation, and select “[Apply Changes.](#)” At this time, the screen will show the following, as illustrated in Figure 15.

Figure 15 — 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 16.

Figure 16 — View Status of Password Changes

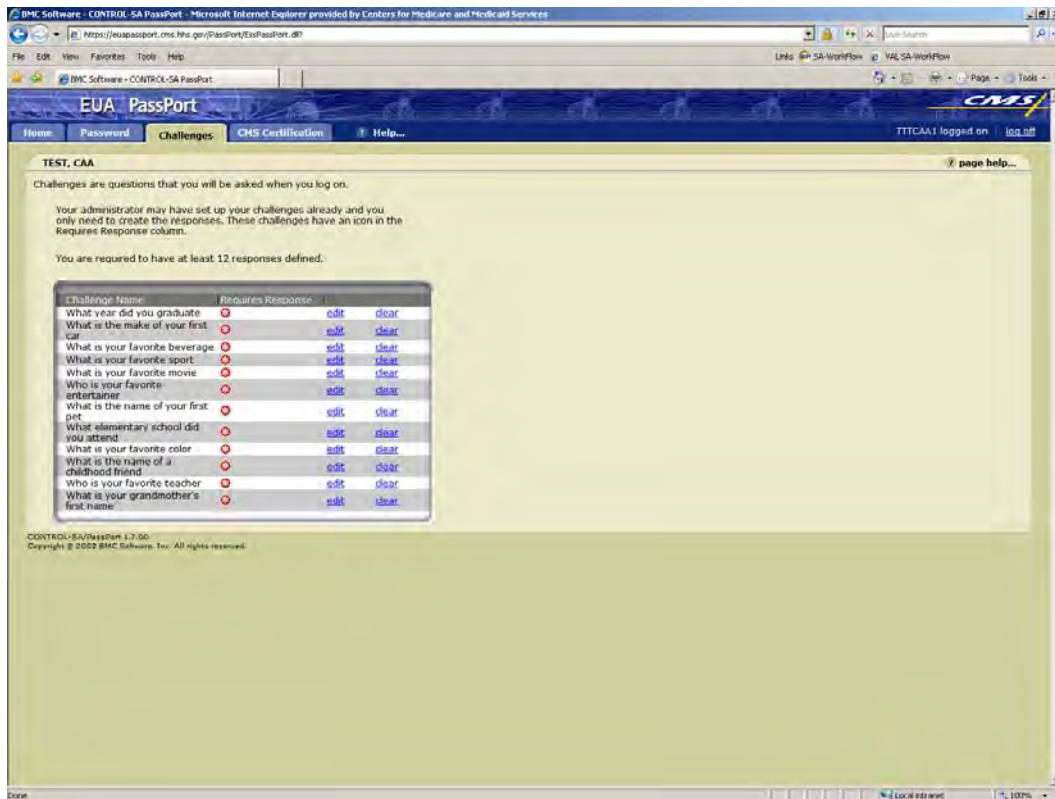
The display shows the status of the password change for all accounts. The user should wait until the status is “Successful” before attempting to log on with that account.

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 Challenge Questions in EUA PassPort

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 17.

Figure 17 — Challenges Tab



The screen contains a list of challenges for which responses are needed. To establish a response for a given challenge, the user selects “[edit](#)”.

This brings up the “[Edit Challenge](#)” screen, as illustrated in Figure 18.

Figure 18 — Edit Challenge Screen

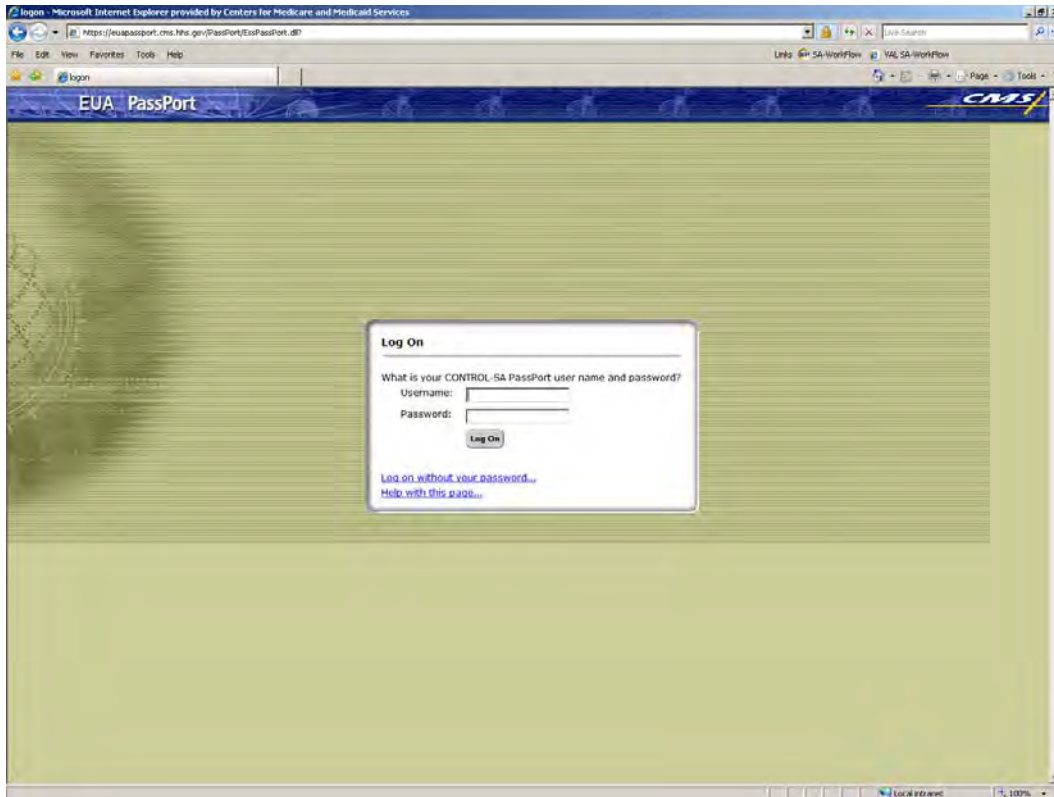
The screenshot displays the 'Edit Challenge' interface within a web browser. The browser's address bar shows the URL <https://eua.passport.cms.hhs.gov/PassPort/EsPassPort.do?>. The page title is 'TEST, CAA - Edit Challenge'. The interface includes a navigation menu with 'Home', 'Password', 'Challenges', 'CMS Certification', and 'Help...'. A 'Back to Challenges' button is located at the top left. Below it, a text block explains: 'Challenges are questions that you will be asked when you log on. To create or change your response to this challenge, type the response to the question, then click the "Apply Changes" button. Your response will be updated in the list below.' The challenge question is 'What year did you graduate'. The 'Response' field contains a masked input (seven asterisks). The 'Retype Response' field also contains a masked input (seven asterisks) with a note '(minimum 4 characters)'. At the bottom of the form are 'Apply Changes' and 'Cancel' buttons. The footer text reads 'CONTROL-SA/PassPort 1.7.00 Copyright © 2001 BMC Software, Inc.'

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

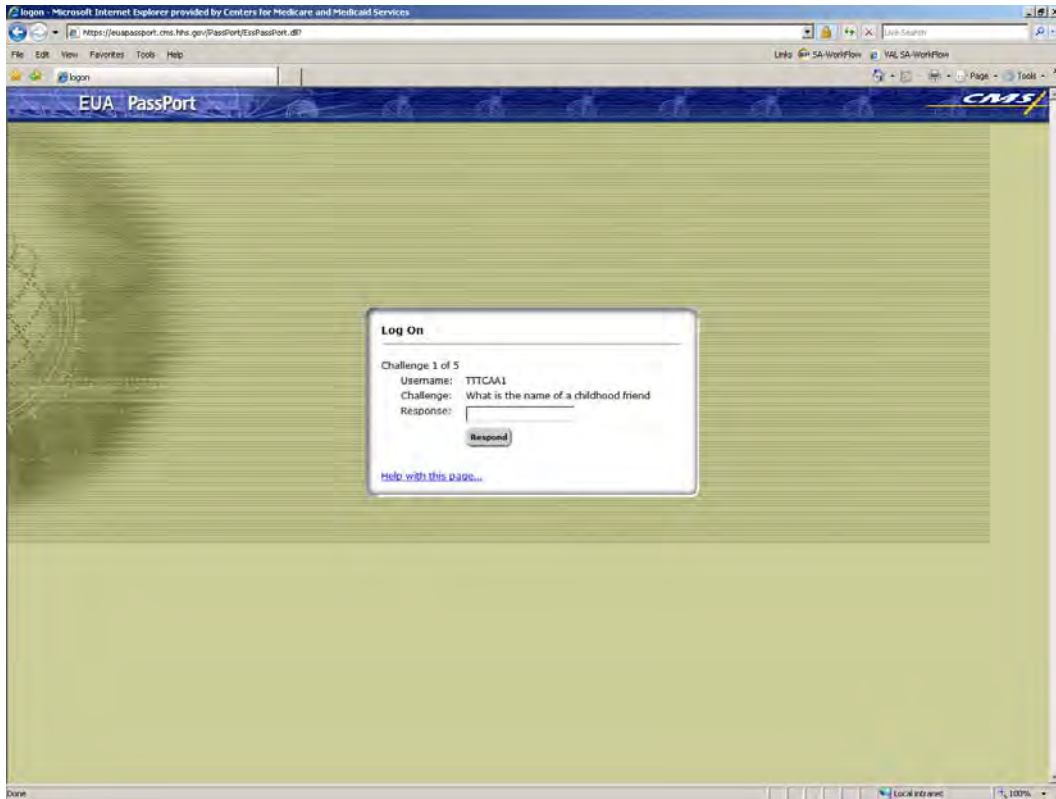
After the challenges and responses have been set up, the user can access PassPort without a password. This is done by selecting “[Log on without your password](#)” in the initial PassPort logon screen, as illustrated in Figure 19.

Figure 19 — Log On Without Your Password Screen

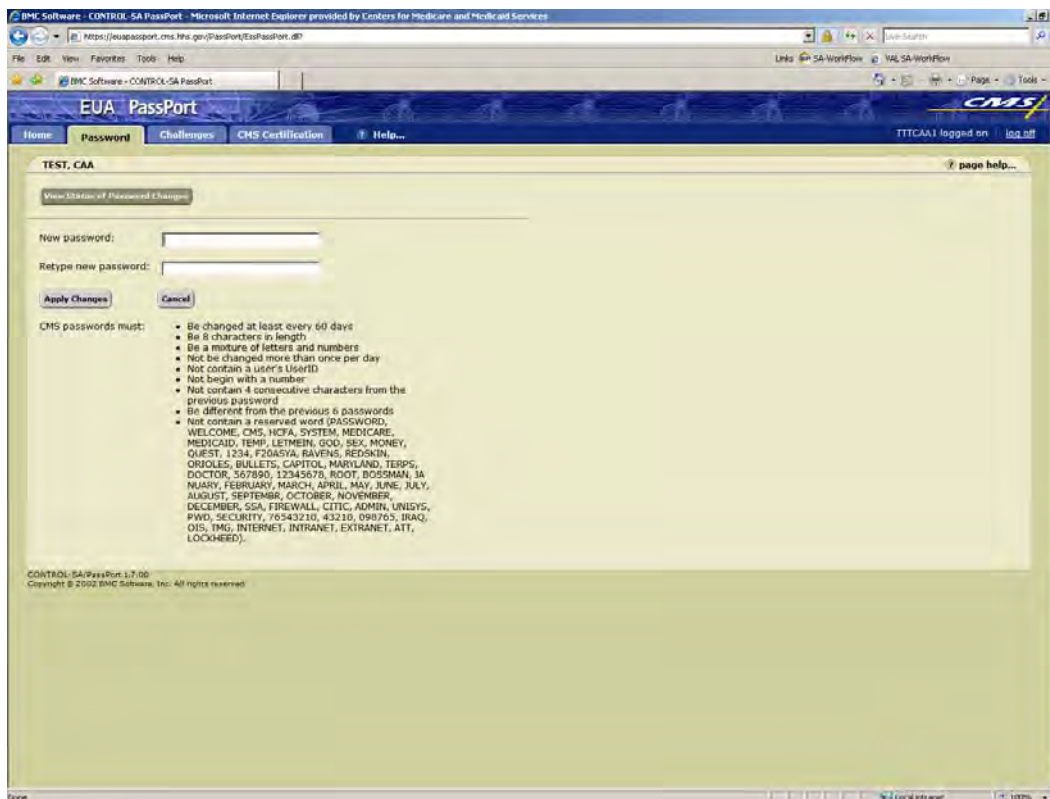


The user will be asked to provide responses to five randomly selected challenges, as illustrated in Figure 20.

Figure 20 — Five 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, as illustrated in Figure 21.

Figure 21 — 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 90 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

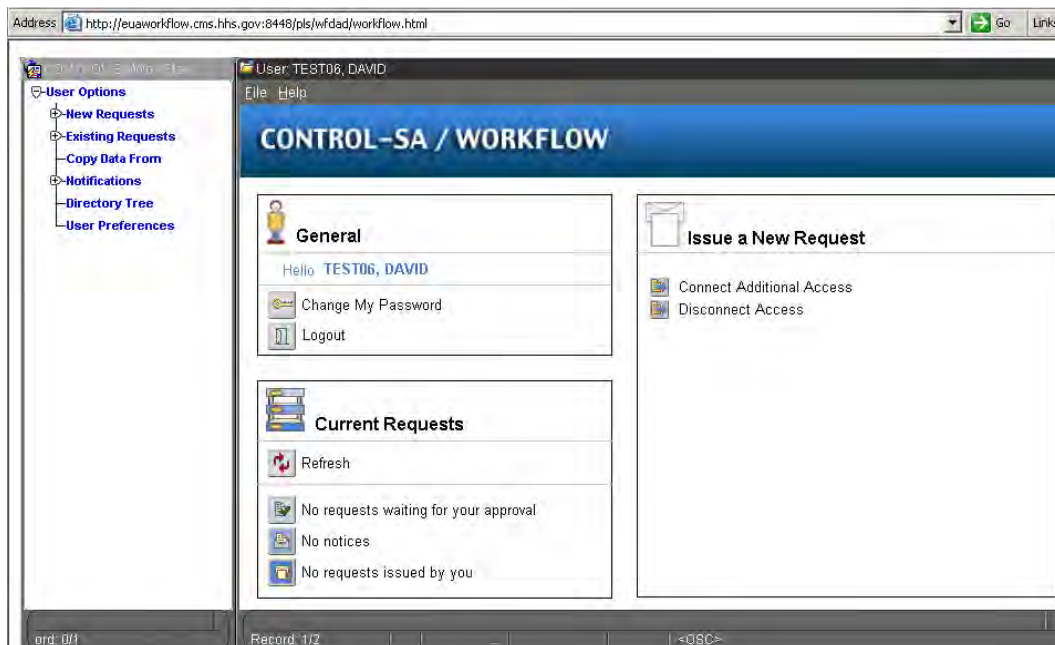
7.1 Connect Additional Access

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 (Figure 22)
2. Expand New Requests
3. Expand Connect Job Code
4. Click Connect Additional Access

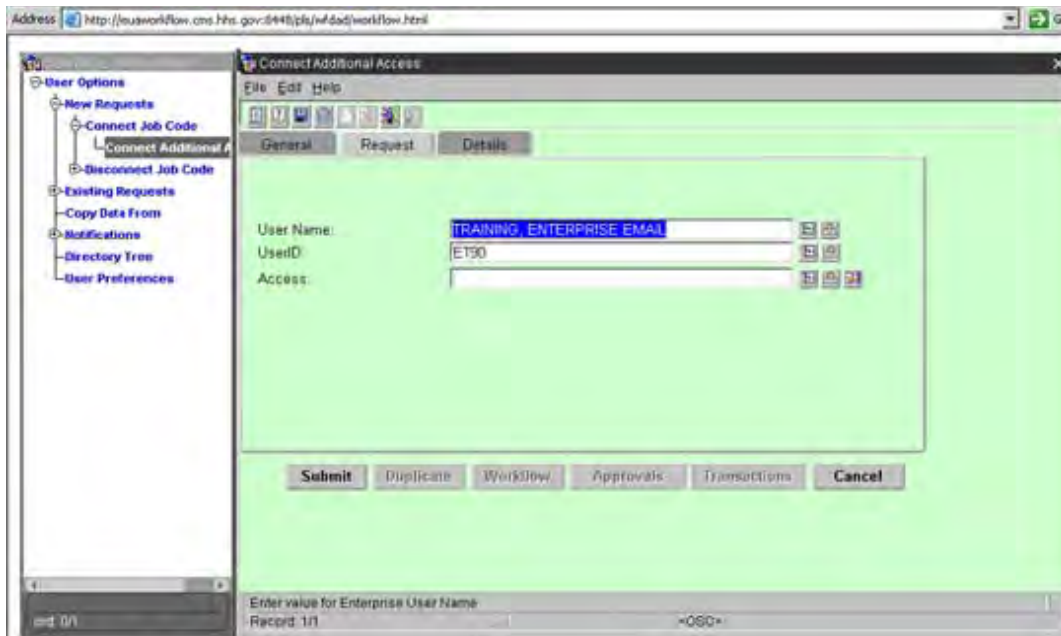
OR simply scroll to the bottom of the Issue a New Request panel on the right and click the Connect Additional Access icon.

Figure 22 — WorkFlow Connect Job Code



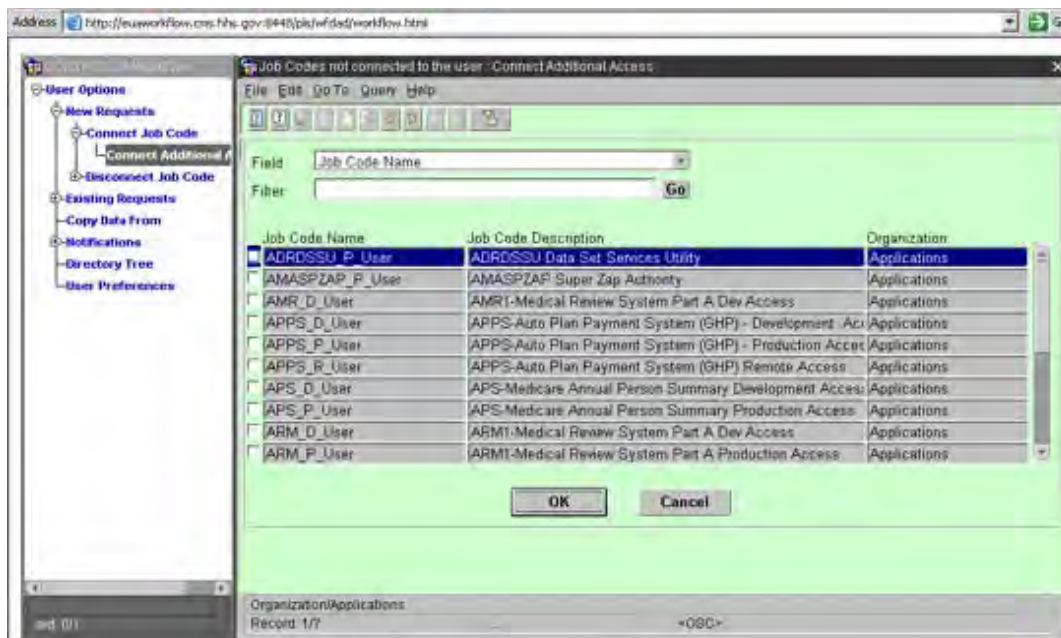
5. Figure 23 is displayed.

Figure 23 — WorkFlow Connect Job Code Request Tab



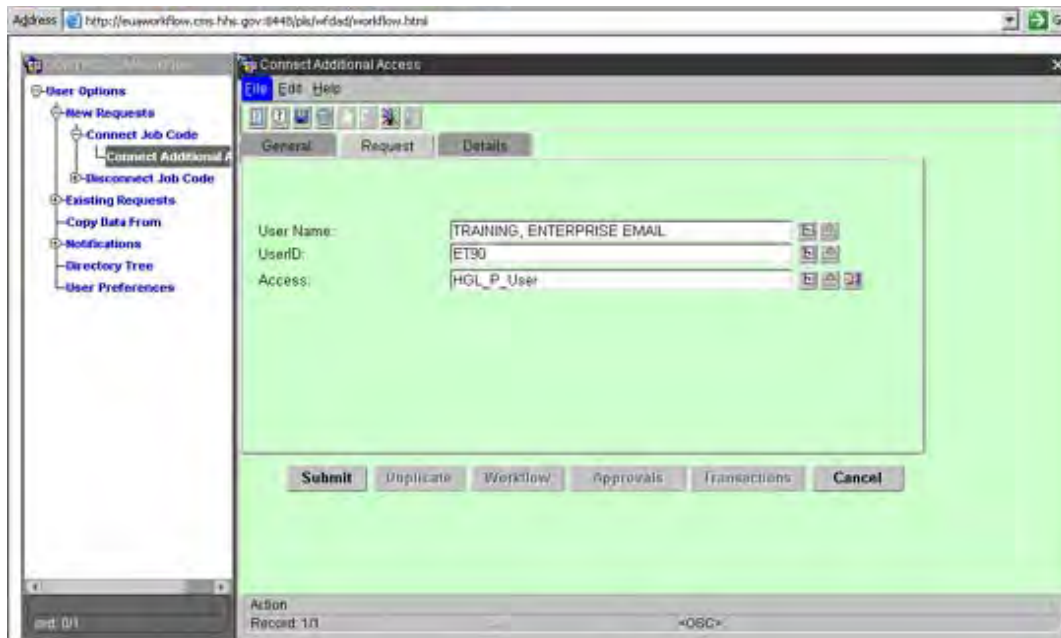
6. Type in the four-character CMS User ID in CAPS in the User ID field then type ENTER.
7. Verify the user's name.
8. Click the far right drop down box in the Access field to select Job Codes not connected to the user. The Job Code Access screen (Figure 24) displays.

Figure 24 — WorkFlow Connect Job Code Access



9. 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.
10. Click the Go box to the right of the Filter field.
11. Click in the far left box of the required Job Code displayed; a check mark will appear.
12. When more than one Job Code is required, repeat steps 1 through 3. There is a limit of nine Job Codes per request.
13. Click OK when all accesses are checked.
14. Job Codes will automatically populate the Access field (Figure 25).

Figure 25 — WorkFlow Connect Job Code Request Tab



15. Click on the Details tab (Figure 26) and enter the justification and Contract Number.

Figure 26 — WorkFlow Connect Job Code Details Tab

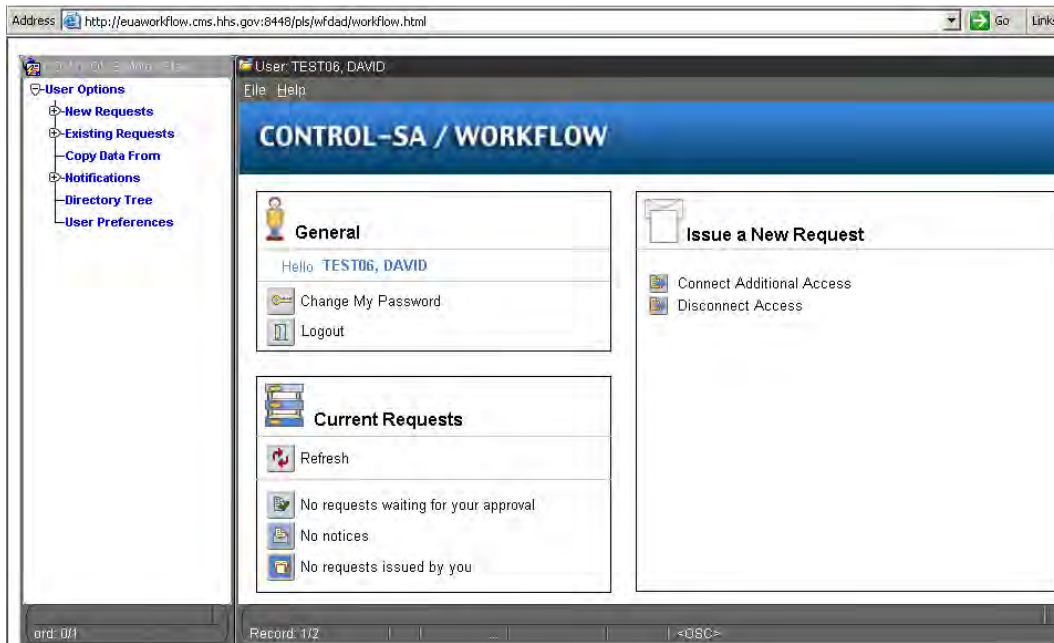
The screenshot shows a software window titled "Connect Additional Access". On the left is a navigation tree with "Connect Additional Access" selected. The main area has tabs for "General", "Request", and "Details". The "Details" tab contains two text boxes labeled "Contract/Grant Number" and "Justification". At the bottom are buttons for "Submit", "Duplicate", "Workflow", "Approvals", "Transactions", and "Cancel". The status bar at the bottom indicates "Record: 1/1" and "<<QSC>".

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.

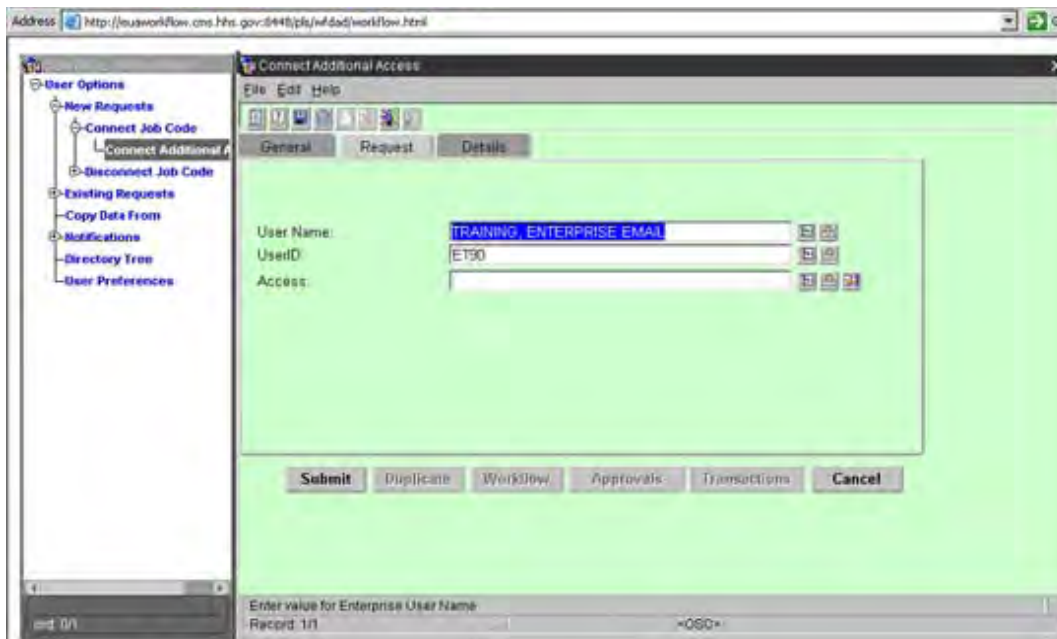
7.1.1 Connects for RACF Job Codes

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

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

Figure 27 — Workflow Connect Job Codes

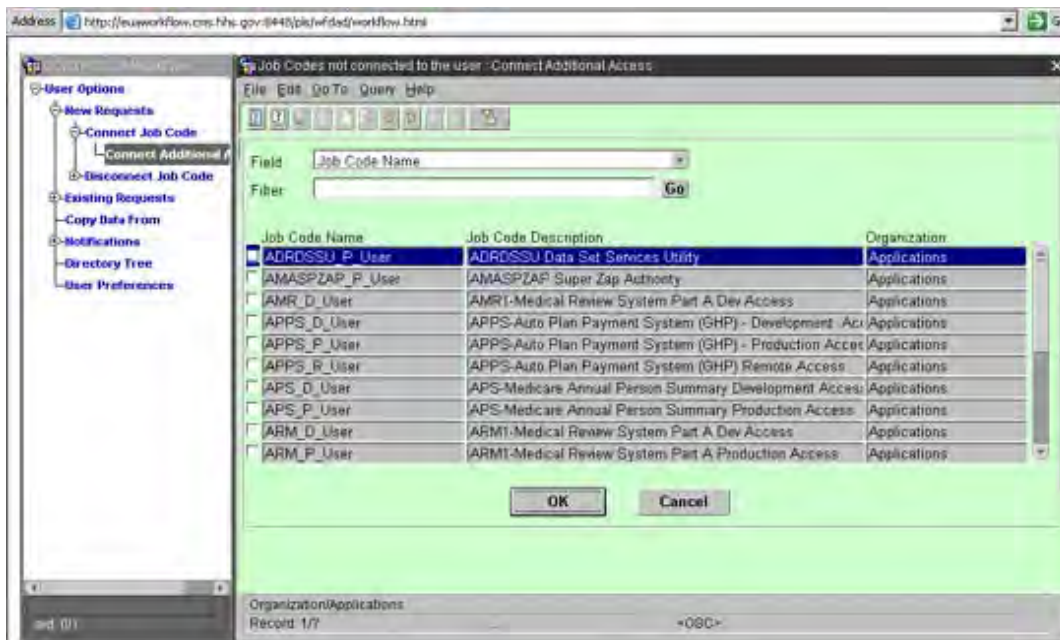
- The screen, as illustrated in Figure 27, is displayed.

Figure 28 — Workflow Connect Job Code Requests Tab

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

9. The Job Code Access screen (Figure 29) displays.

Figure 29 — WorkFlow Connect Job Code Access

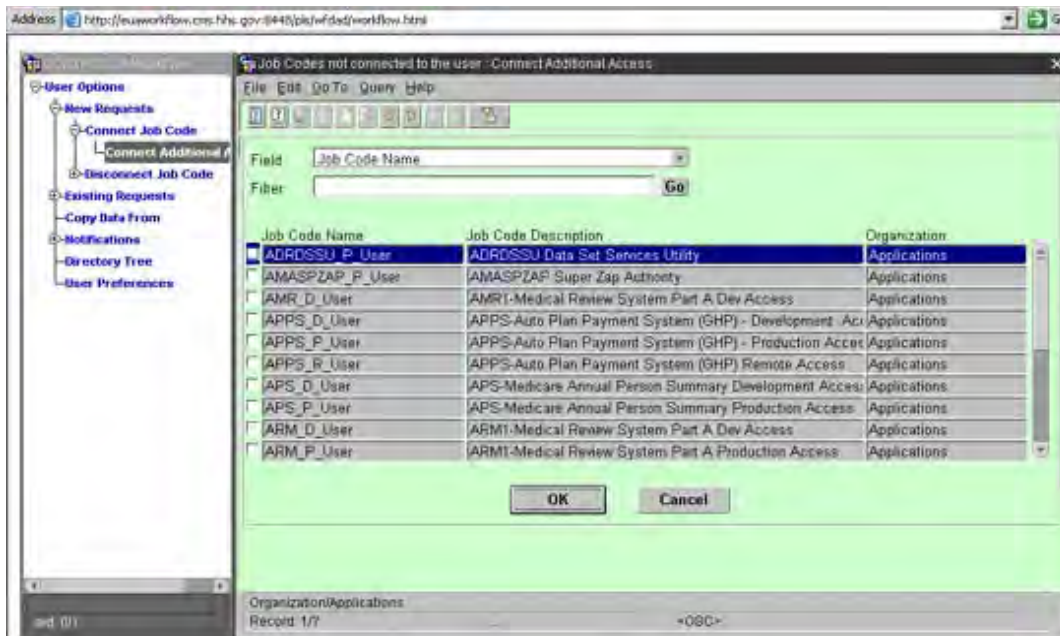


10. Enter all or part of a Job Code name representing the access the user requires (see list of Job Codes) followed by a percent sign (the % is a wild card character in WorkFlow) in the Filter field.

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

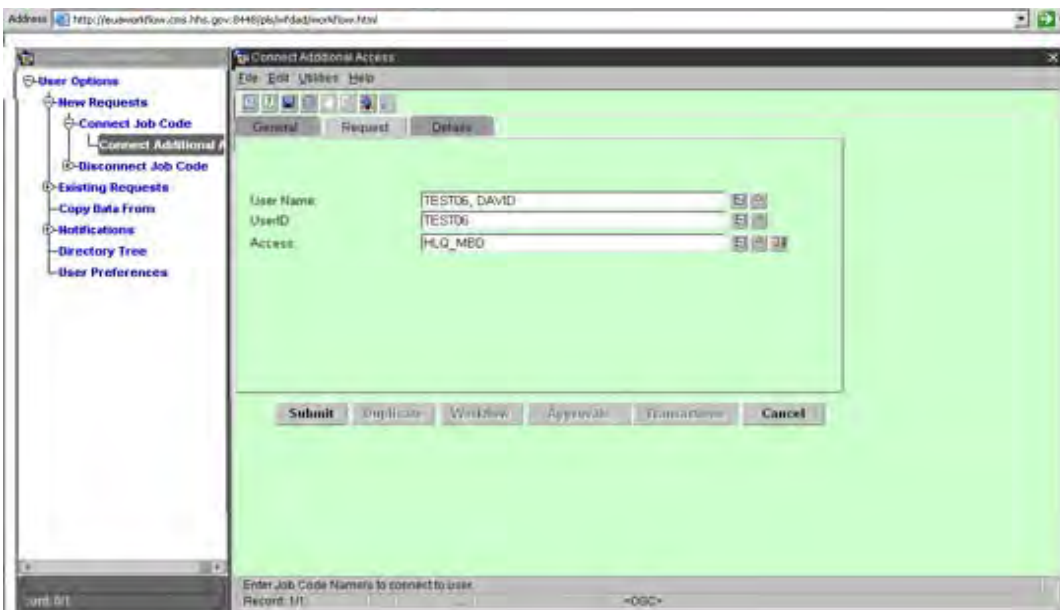
11. Click the Go box to the right of the Filter field.
12. Click in the far left box of the required Job Code displayed; a check mark will appear.
13. When more than one Job Code is required, repeat steps 1 through 3. There is a limit of nine Job Codes per request.
14. Click OK when all accesses are checked (Figure 30).

Figure 30 — WorkFlow Connect Job Code Request Tab



15. Job Codes will automatically populate the Access field (Figure 31).

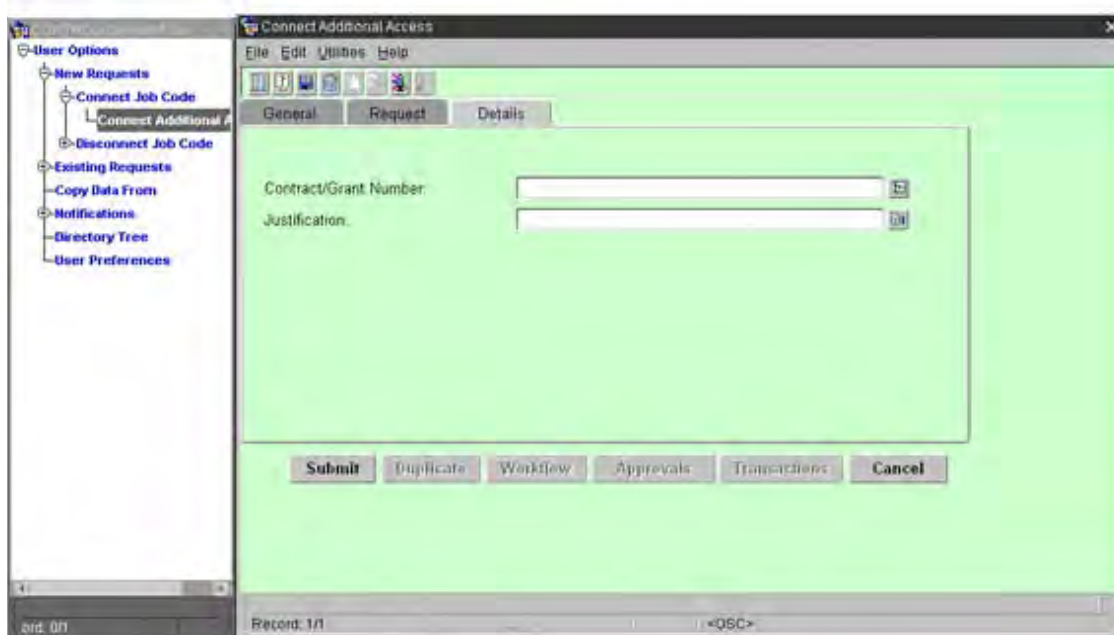
Figure 31 — WorkFlow Connect Job Request Tab



16. Click on the **Details** tab (Figure 32) and enter the justification and Contract Number.

17. Enter the contract number.

18. 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 32 — WorkFlow Connect Job Code Details Tab

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

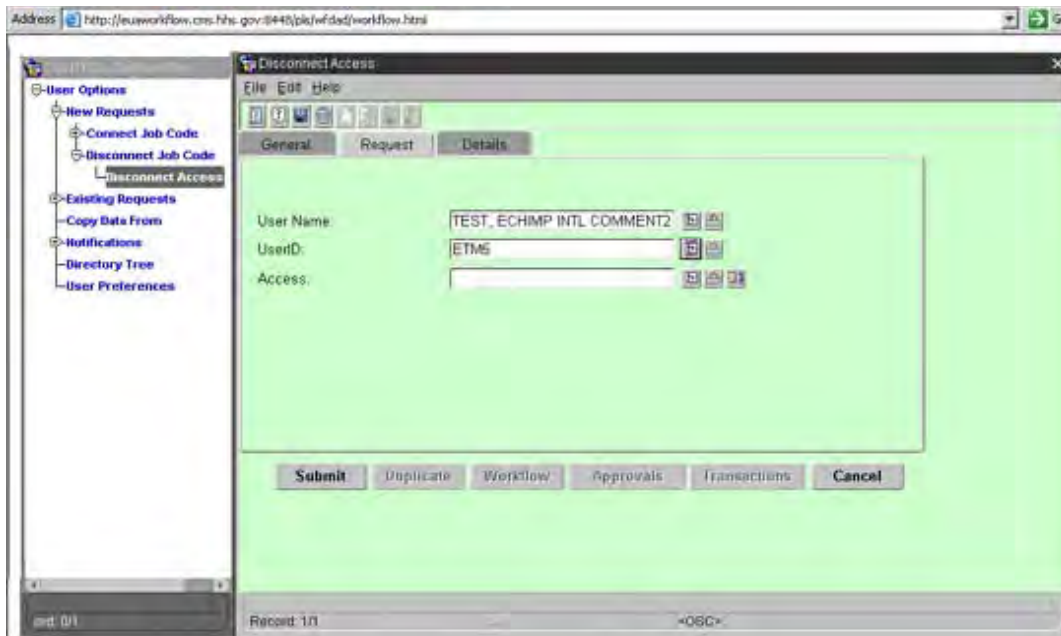
7.2 Disconnect Job Code

1. 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.

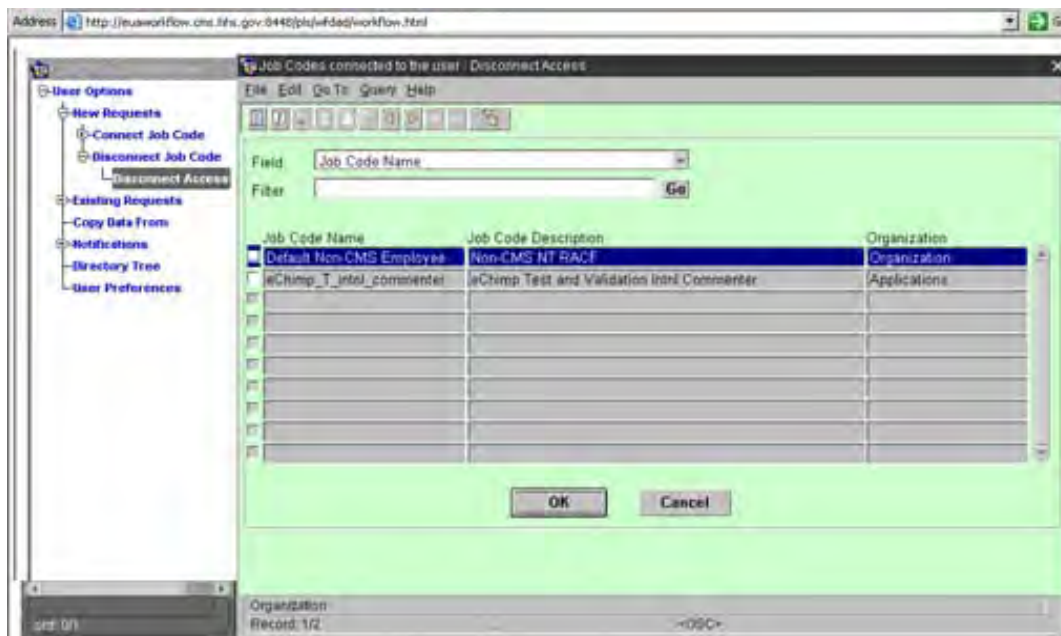
2. The Disconnect Access screen (Figure 33) displays. Using the same procedure for Connect Additional Access, find the desired user.

Figure 33 — WorkFlow Disconnect Access



3. Click the far right drop down box in the Access field to list all Job Codes connected to the user (Figure 34).

Figure 34 — WorkFlow Disconnect Access Job Code Selection



4. 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 35).

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.

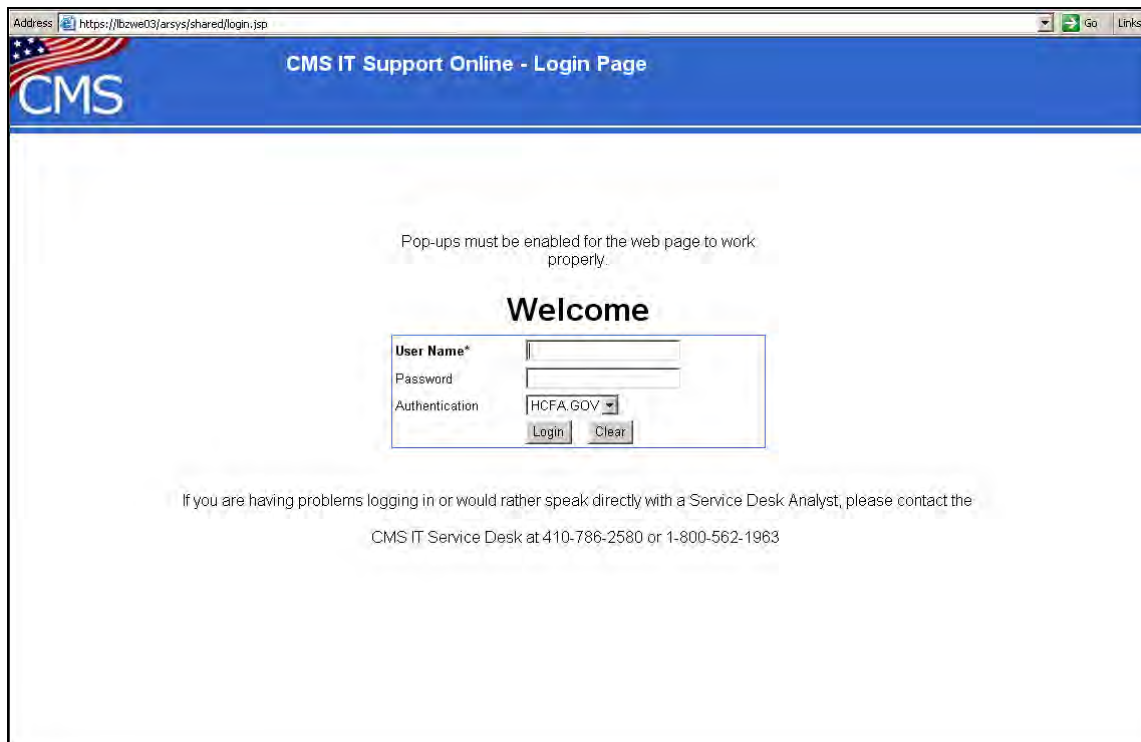
1. Double-click the IT SUPPORT icon (Figure 37) found on your workstation and satisfy the security alerts.

Figure 37 — IT Support Icon



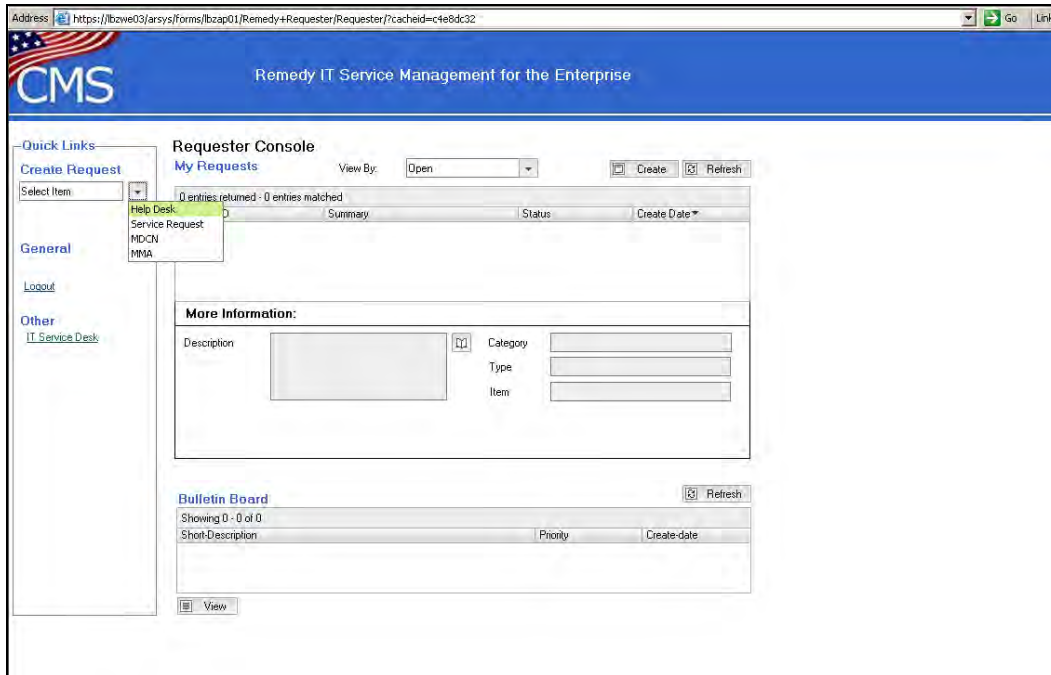
2. Log in using your CMS four-character User ID and current password (Figure 38).

Figure 38 — IT Support Logon

A screenshot of a web browser window showing the 'CMS IT Support Online - Login Page'. The browser's address bar contains 'https://lbzwe03/arsys/shared/login.jsp'. The page has a blue header with the 'CMS' logo and the text 'CMS IT Support Online - Login Page'. Below the header, there is a message: 'Pop-ups must be enabled for the web page to work properly.' Underneath this is a 'Welcome' section with a login form. The form includes fields for 'User Name*', 'Password', and 'Authentication' (set to 'HCFA.GOV'). There are 'Login' and 'Clear' buttons at the bottom of the form. At the bottom of the page, 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.'

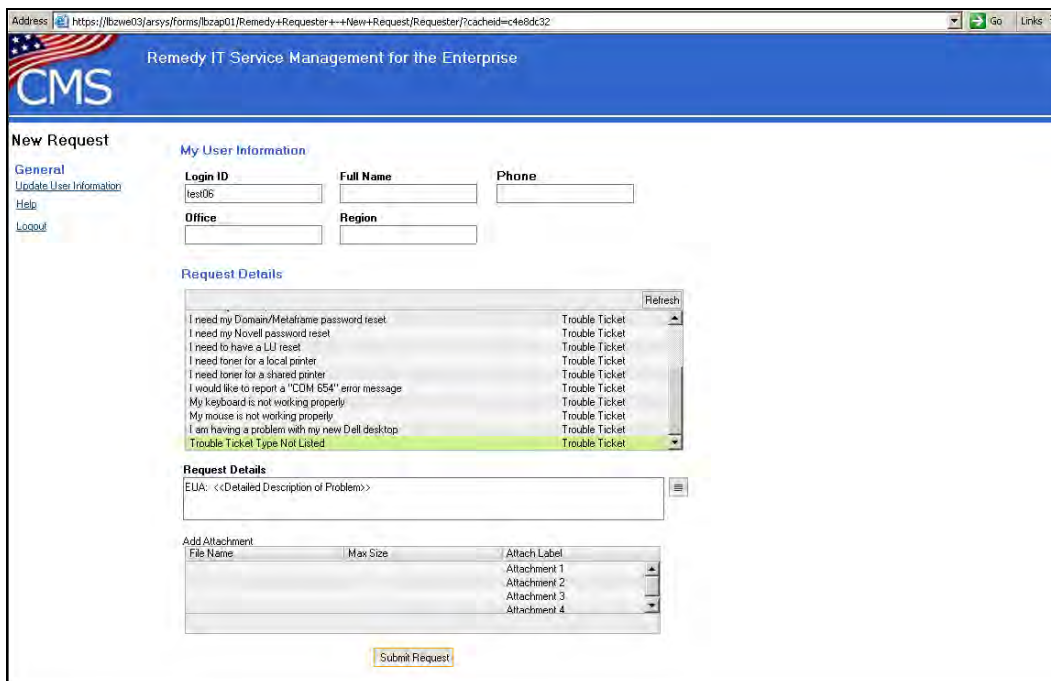
3. After you have logged in, you will IT Support Main screen, as illustrated in Figure 39.

Figure 39 — IT Support Main Screen



4. Click on the downward arrow under Create Request on the far left of your screen. Select Help Desk.
5. The IT Support Trouble Ticket Submission screen (Figure 40) displays. Make sure the information in My User Information is correct before proceeding.

Figure 40 — 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.