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

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Office of Information Services

Enterprise User Administration (EUA)

Users Guide

Version 1.3
June 27, 2007

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

Contents

1.0 INTRODUCTION 1

2.0 NEW USER REQUESTS 1

3.0 USER CHANGE REQUESTS 1

4.0 CMS USER ID CERTIFICATION REQUIREMENTS 1

5.0 EUA PASSPORT 2

5.1 Installation of PassPort 2
5.2 Logging on to PassPort 2
5.3 PassPort Home Screen 3
5.4 PassPort Certification Screens 4

6.0 MANAGING PASSWORDS 8

6.1 Using PassPort to Manage Passwords 8
6.2 Setting Up Challenges 10
6.3 Logging on to PassPort Without a Password 12
6.4 Inactivity Revocation 14

7.0 MANAGING EUA WORKFLOW 15

7.1 Connect Additional Access 15
7.1.1 Connects for RACF Job Codes 19
7.2 Disconnect Job Code 24
7.3 IT Support Icon (Creating a trouble ticket for EUA support for CMS Employees only) 28

List of Figures

Figure 1—PassPort Logo 2
Figure 2—PassPort LogOn 3
Figure 3—PassPort Home Screen 4
Figure 4—“PassPort Certification” Screen 4
Figure 5—“System Access Certification” Screen 5
Figure 6—Privacy Act Statement 6
Figure 7—Agree and Decline Buttons 6
Figure 8—“Confirmation” Screen 7
Figure 9—Certification Screen 7
Figure 10—Summary of Accesses 8
Figure 11—“Password” Screen 9
Figure 12—“Password” Screen: Apply Changes 9
Figure 13—View Status of Password Changes 9
Figure 14—“Challenges” Tab 11
Figure 15—“Edit Challenge” Screen 12
Figure 16—“Log On Without Your Password” Screen 13
Figure 17—“Five Randomly Selected Challenges” Screen 13
Figure 18—“Passwords” Tab 14
Figure 19—WorkFlow Connect Job Code 15
Figure 20—WorkFlow Connect Job Code Request Tab 16
Figure 21—WorkFlow Connect Job Code Access 17
Figure 22—WorkFlow Connect Job Code Request Tab 18
Figure 23—WorkFlow Connect Job Code details Tab 18
Figure 24—WorkFlow Connect Job Codes 19
Figure 25—WorkFlow Connect Job Code Requests Tab 20
Figure 26—WorkFlow Connect Job Code Access 21
Figure 27—WorkFlow Connect Job Code Request Tab 22
Figure 28—WorkFlow Connect Job Request Tab 23

Figure 29—WorkFlow Connect Job Code Details Tab..24

Figure 30—WorkFlow Disconnect Access..25

Figure 31—WorkFlow Disconnect Access Job Code Selection.................................26

Figure 32—WorkFlow Disconnect Access Job Code Selection.................................27

Figure 33—WorkFlow Disconnect Access Job Code Submission............................28

Figure 34—IT Support Logon 29

Figure 35—IT Support Main Screen 30

Figure 36—IT Support Trouble Ticket Submission..31

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 (CMSDC). 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 CMSDC and at CMS Web sites. Therefore, it does not control remote dialup 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 email 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 email message notifying him/her of the need to certify and complete the CBT. The email 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 email 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 for PassPort on their desktops. The icon contains the PassPort logo illustrated in Figure 1. Other users can create a desktop icon for PassPort.

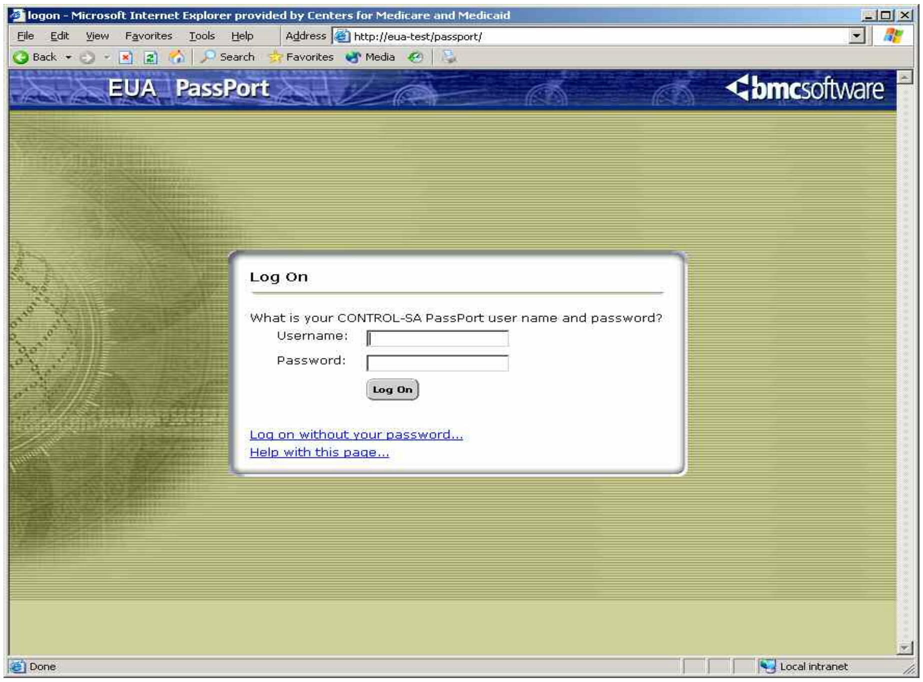
Figure 1—PassPort Logo

5.2 Logging on to PassPort

PassPort is accessed 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 illustrated in Figure 2.

Figure 2—PassPort LogOn



logon - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/passport/
Back Search Favorites Media
EUA PassPort
bmcsoftware
Done
Local intranet

Log On

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

Username:

Password:

Log On

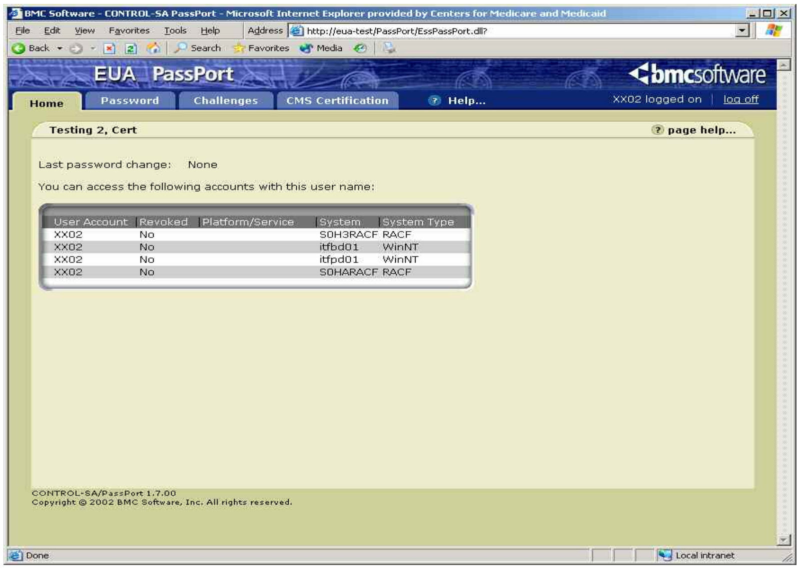
Log on without your password...

Help with this page...

5.3 PassPort Home Screen

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

Figure 3—PassPort Home Screen


BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home
Password
Challenges
CMS Certification
Help...
XX02 logged on | log off
page help...
Done
Local intranet

Testing 2, Cert

Last password change: None

You can access the following accounts with this user name:

User Account	Revoked	Platform/Service	System	System Type
XX02	No		S0H3RACF	RACF
XX02	No		itfbd01	WinNT
XX02	No		itfpd01	WinNT
XX02	No		S0HARACF	RACF

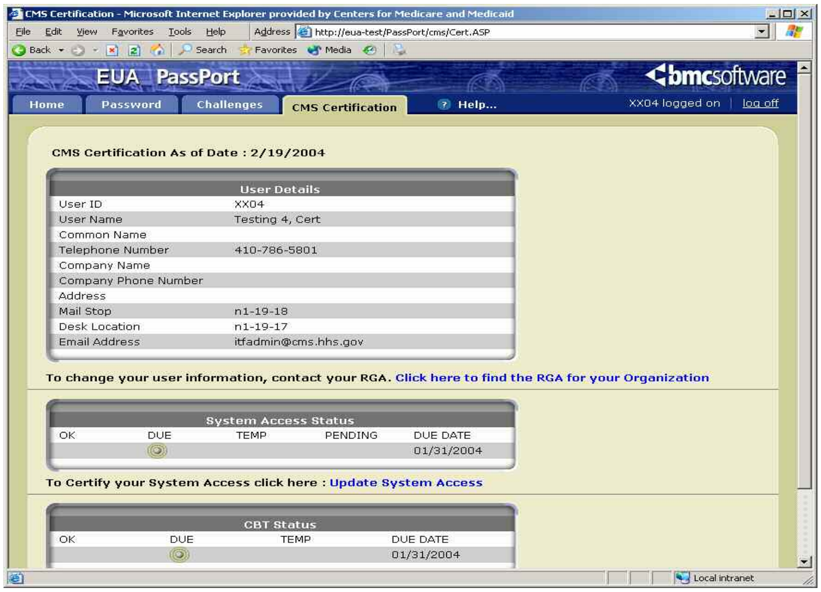
CONTROL-SA/PassPort 1.7.00
Copyright © 2002 BMC Software, Inc. All rights reserved.

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 following screen, illustrated in Figure 4.

Figure 4—"PassPort Certification" Screen


CMS Certification - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/cms/Cert.ASP
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home
Password
Challenges
CMS Certification
Help...
XX04 logged on | log off
Local intranet

CMS Certification As of Date : 2/19/2004

User Details	
User ID	XX04
User Name	Testing 4, Cert
Common Name	
Telephone Number	410-786-5801
Company Name	
Company Phone Number	
Address	
Mail Stop	n1-19-18
Desk Location	n1-19-17
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
	●			01/31/2004

To Certify your System Access click here : Update System Access

CBT Status

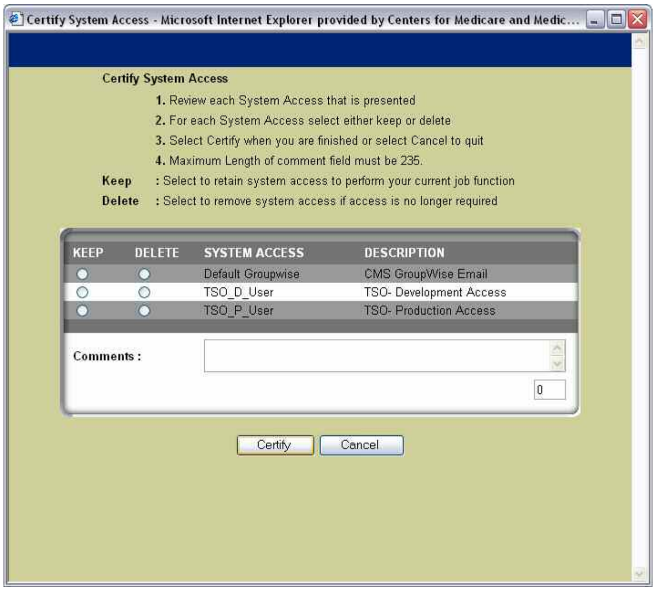
OK	DUE	TEMP	DUE DATE
	●		01/31/2004

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 following screen illustrated in Figure 5 is presented.

Figure 5—"System Access Certification" Screen



Certify System Access - Microsoft Internet Explorer provided by Centers for Medicare and Medic...

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
○	○	Default Groupwise	CMS GroupWise Email
○	○	TSO_D_User	TSO- Development Access
○	○	TSO_P_User	TSO- Production Access

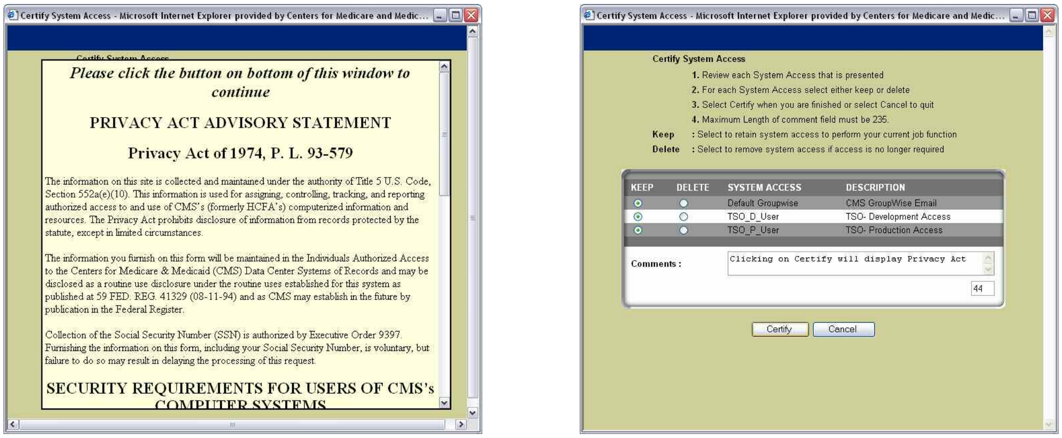
Comments :

0

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 6.

Figure 6—Privacy Act Statement


Certify System Access - Microsoft Internet Explorer provided by Centers for Medicare and Medic...
Certify System Access

Please click the button on bottom of this window to continue

PRIVACY ACT ADVISORY STATEMENT

Privacy Act of 1974, P. L. 93-579

The information on this site is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's (formerly HCFA's) computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnish on this form will be maintained in the Individuals Authorized Access to the Centers for Medicare & Medicaid (CMS) Data Center Systems of Records and may be disclosed as a routine use disclosure under the routine uses established for this system as published at 59 FED. REG. 41329 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

Collection of the Social Security Number (SSN) is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in delaying the processing of this request.

SECURITY REQUIREMENTS FOR USERS OF CMS's COMPUTER SYSTEMS

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.

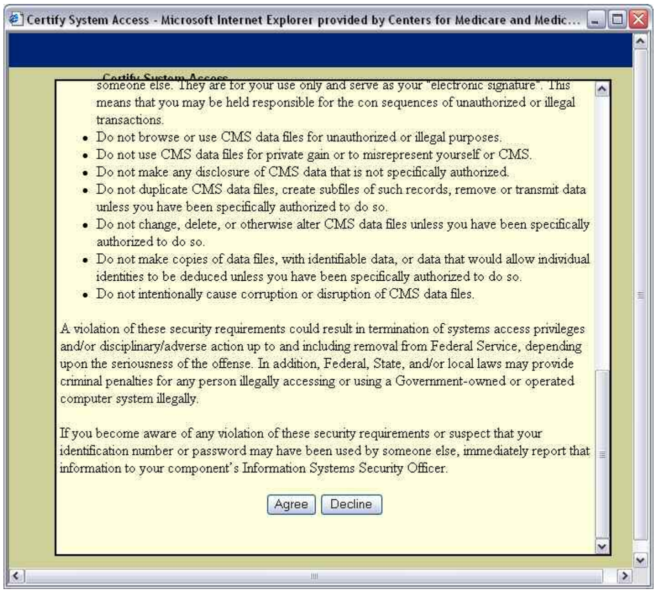
Keep : Select to retain system access to perform your current job function
Delete : Select to remove system access if access is no longer required

KEEP	DELETE	SYSTEM ACCESS	DESCRIPTION
●	○	Default Groupwise	CMS GroupWise Email
●	○	TSO_D_User	TSO- Development Access
●	○	TSO_P_User	TSO- Production Access

Comments : Clicking on Certify will display Privacy Act
44

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


Certify System Access - Microsoft Internet Explorer provided by Centers for Medicare and Medic...
Certify System Access

someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the con sequences of unauthorized or illegal transactions.

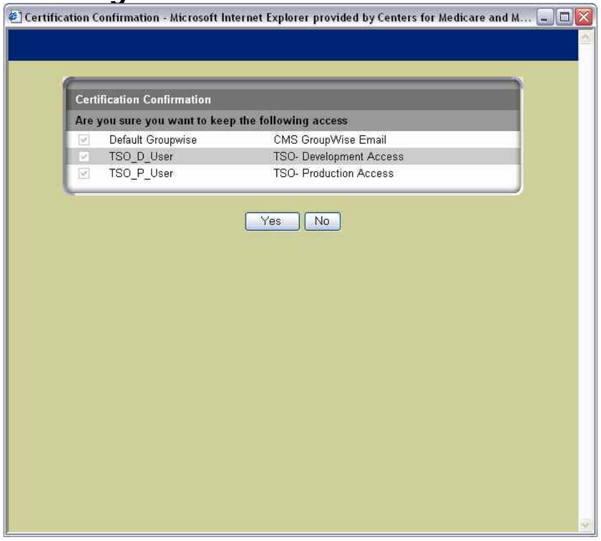
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to your component's Information Systems Security Officer.

The user should click on Agree, at which time the following confirmation screen is displayed, as illustrated in Figure 8.

Figure 8—"Confirmation" Screen



Certification Confirmation - Microsoft Internet Explorer provided by Centers for Medicare and M...

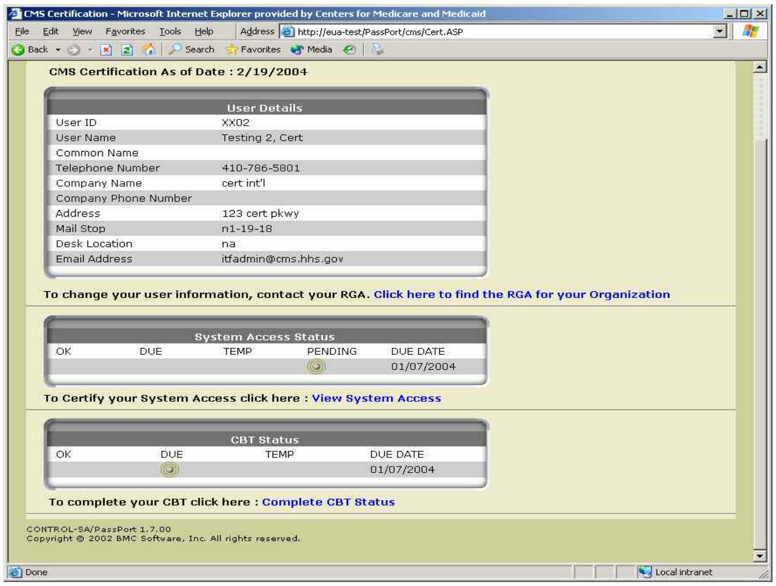
Certification Confirmation

Are you sure you want to keep the following access

☑	Default Groupwise	CMS GroupWise Email
☑	TSO_D_User	TSO- Development Access
☑	TSO_P_User	TSO- Production Access

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

Figure 9—Certification Screen



CMS Certification - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid

Address http://eua-test/PassPort/cms/Cert.ASP

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
			◉	01/07/2004

To Certify your System Access click here : View System Access

CBT Status

OK	DUE	TEMP	DUE DATE
	◉		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.

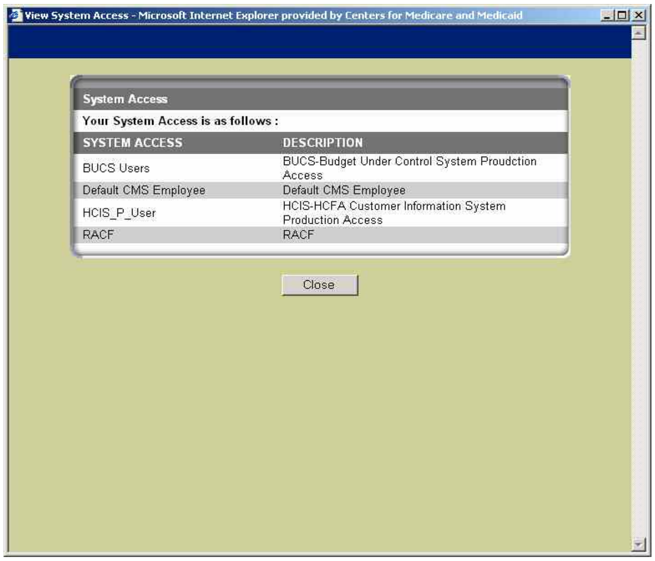
Notice that "Update System Access" has been changed to "View System Access." The status is now set to "PENDING." It will remain in this state until the certification has been approved by CMS, at which time the status will change to "OK."

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 10.

Figure 10—Summary of Accesses



View System Access - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid

System Access

Your System Access is as follows :

SYSTEM ACCESS	DESCRIPTION
BUCS Users	BUCS-Budget Under Control System Proudction Access
Default CMS Employee	Default CMS Employee
HCIS_P_User	HCIS-HCFA Customer Information System Production Access
RACF	RACF

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

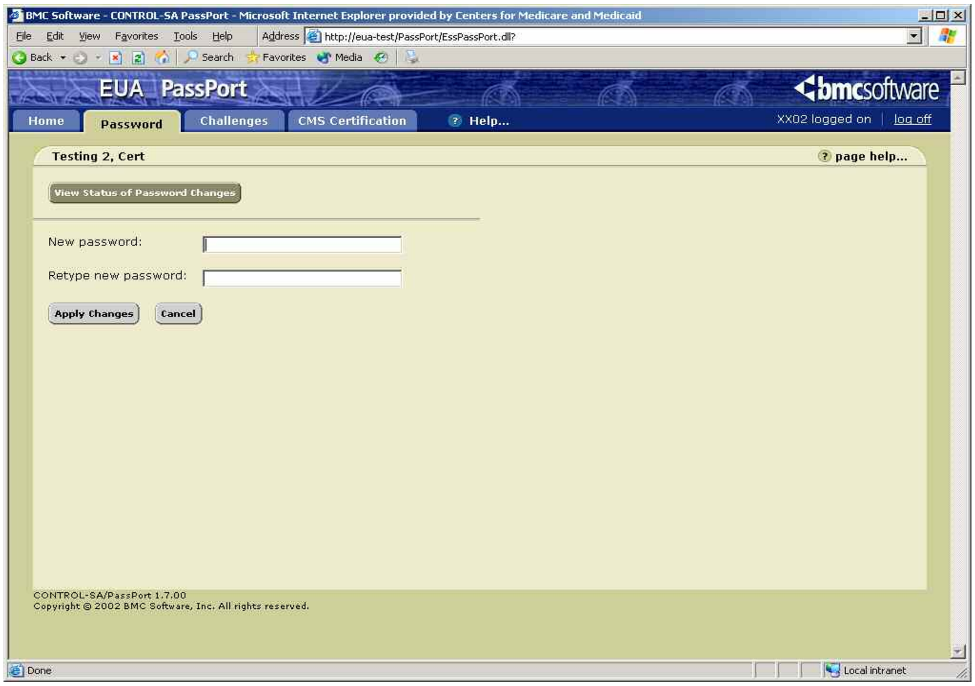
6.0 MANAGING PASSWORDS

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


BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home
Password
Challenges
CMS Certification
Help...
XX02 logged on
log off
page help...
View Status of Password Changes
Apply Changes
Cancel
Done
Local intranet

Testing 2, Cert

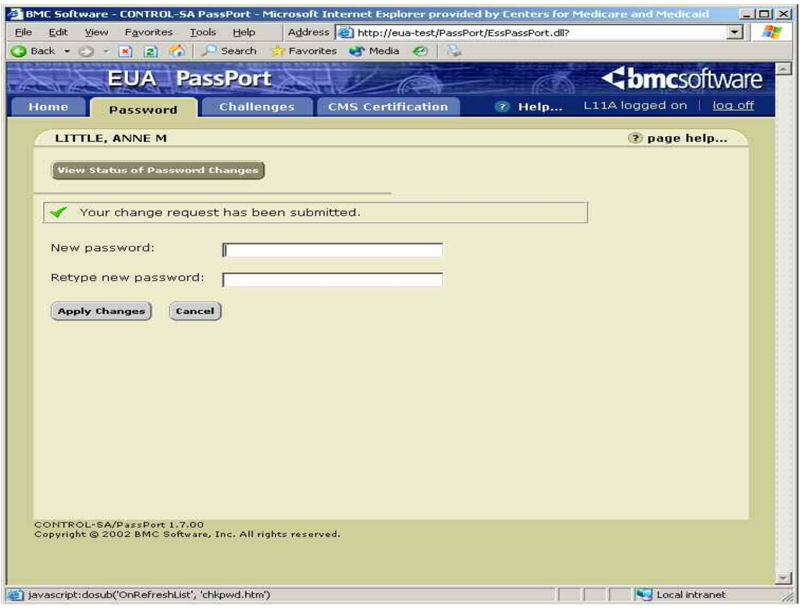
New password:

Retype new password:

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

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 12.

Figure 12—"Password" Screen: Apply Changes


BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home
Password
Challenges
CMS Certification
Help...
L11A logged on
log off
page help...
View Status of Password Changes
Apply Changes
Cancel
Local intranet

LITTLE, ANNE M

✓ Your change request has been submitted.

New password:

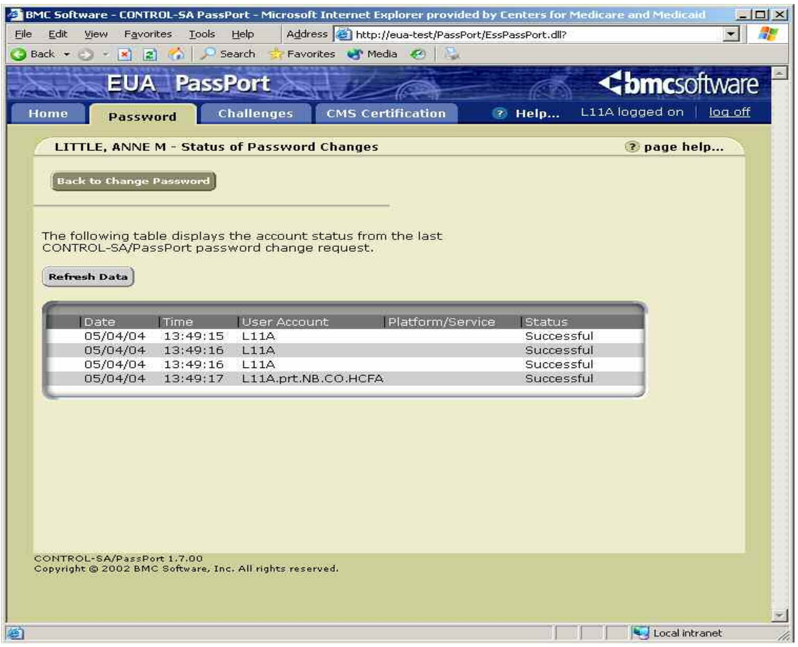
Retype new password:

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

javascript:dosub('OnRefreshList', 'chkpwd.htm')

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



BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home
Password
Challenges
CMS Certification
Help...
L11A logged on
log off
page help...
Back to Change Password
Refresh Data
Local intranet

LITTLE, ANNE M - Status of Password Changes

The following table displays the account status from the last CONTROL-SA/PassPort password change request.

Date	Time	User Account	Platform/Service	Status
05/04/04	13:49:15	L11A		Successful
05/04/04	13:49:16	L11A		Successful
05/04/04	13:49:16	L11A		Successful
05/04/04	13:49:17	L11A.prt.NB.CO.HCFA		Successful

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

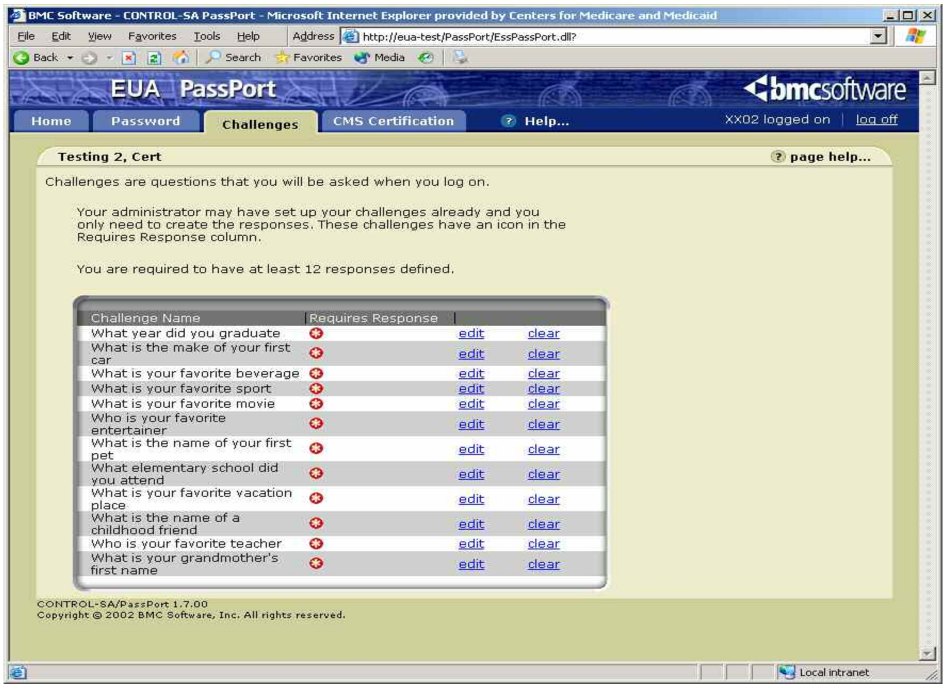
The display shows the status of the password change for all accounts. The user should wait until the status is "Successful" before attempting to log on with that account.

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 email 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


BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home Password Challenges CMS Certification Help...
XX02 logged on | log off
Local intranet

Testing 2, Cert

page help...

Challenges are questions that you will be asked when you log on.

Your administrator may have set up your challenges already and you only need to create the responses. These challenges have an icon in the Requires Response column.

You are required to have at least 12 responses defined.

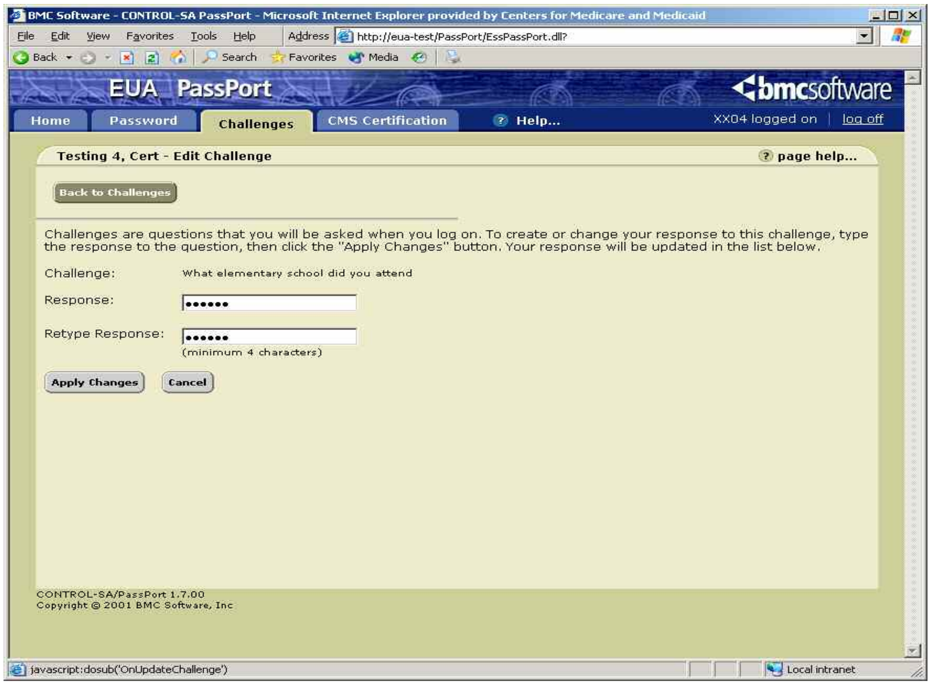
Challenge Name	Requires Response		
What year did you graduate	⊗	edit	clear
What is the make of your first car	⊗	edit	clear
What is your favorite beverage	⊗	edit	clear
What is your favorite sport	⊗	edit	clear
What is your favorite movie	⊗	edit	clear
Who is your favorite entertainer	⊗	edit	clear
What is the name of your first pet	⊗	edit	clear
What elementary school did you attend	⊗	edit	clear
What is your favorite vacation place	⊗	edit	clear
What is the name of a childhood friend	⊗	edit	clear
Who is your favorite teacher	⊗	edit	clear
What is your grandmother's first name	⊗	edit	clear

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

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 15.

Figure 15—"Edit Challenge" Screen



BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Home
Password
Challenges
CMS Certification
Help...
XX04 logged on
log off
page help...
Back to Challenges
Apply Changes
Cancel
javascript:dosub('OnUpdateChallenge')
Local intranet

Testing 4, Cert - Edit Challenge

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.

Challenge: What elementary school did you attend

Response: ••••••

Retype Response: ••••••
(minimum 4 characters)

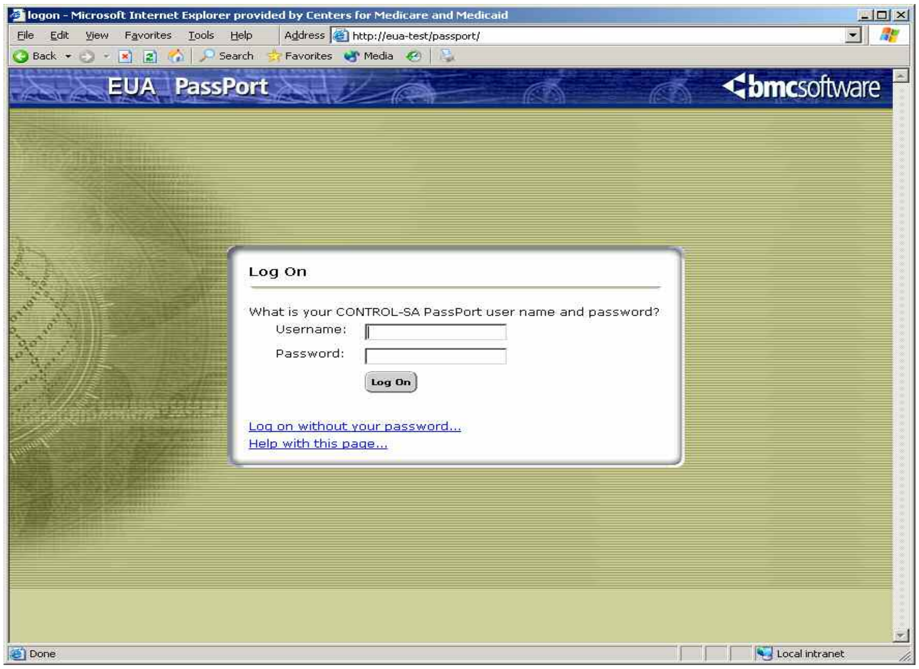
CONTROL-SA/PassPort 1.7.00
Copyright © 2001 BMC Software, Inc

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 16.

Figure 16—"Log On Without Your Password" Screen



logon - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/passport/
Back Search Favorites Media
EUA PassPort
bmcsoftware
Log On
Log On
Done
Local intranet

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

Username:

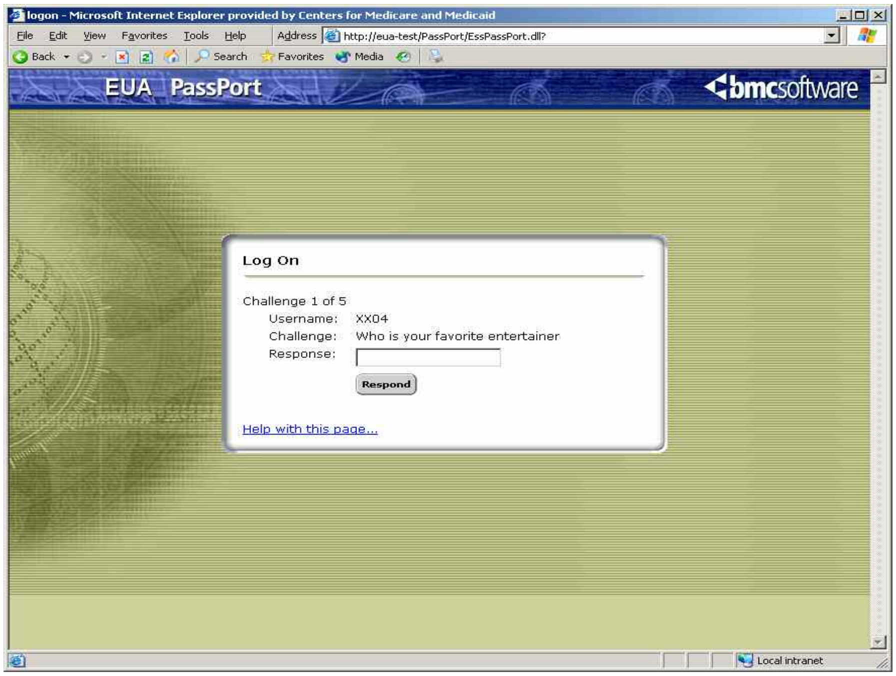
Password:

Log on without your password...

Help with this page...

The user will be asked to provide responses to five randomly selected challenges, as illustrated in Figure 17.

Figure 17—"Five Randomly Selected Challenges" Screen



logon - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid
File Edit View Favorites Tools Help
Address http://eua-test/PassPort/EssPassPort.dll?
Back Search Favorites Media
EUA PassPort
bmcsoftware
Log On
Respond
Local intranet

Challenge 1 of 5

Username: XX04

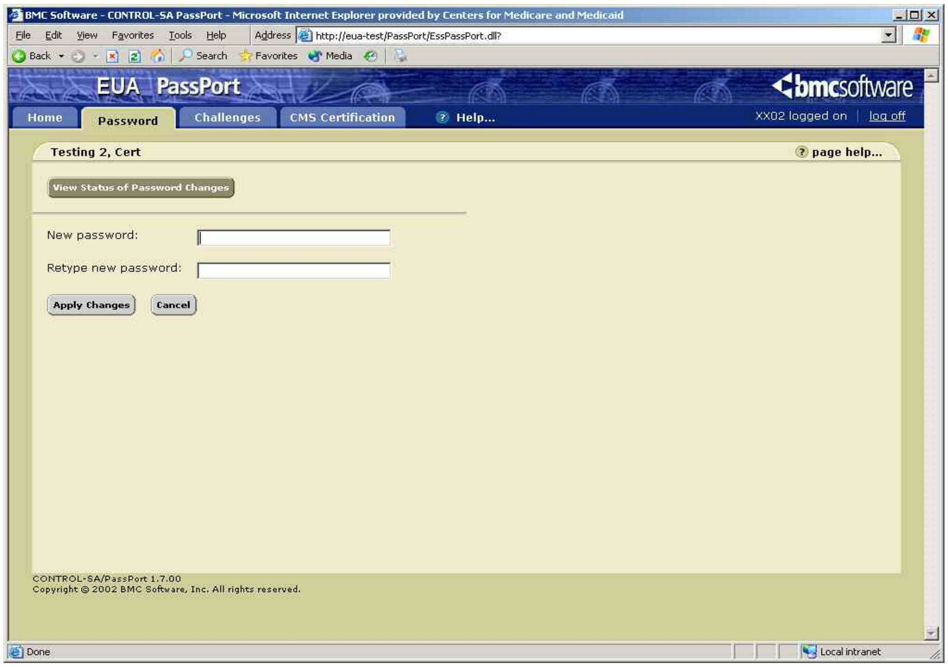
Challenge: Who is your favorite entertainer

Response:

Help with this page...

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 18.

Figure 18—"Passwords" Tab



BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid

Address http://eua-test/PassPort/EssPassPort.dll?

Testing 2, Cert

New password:

Retype new password:

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

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
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 19—WorkFlow Connect Job Code

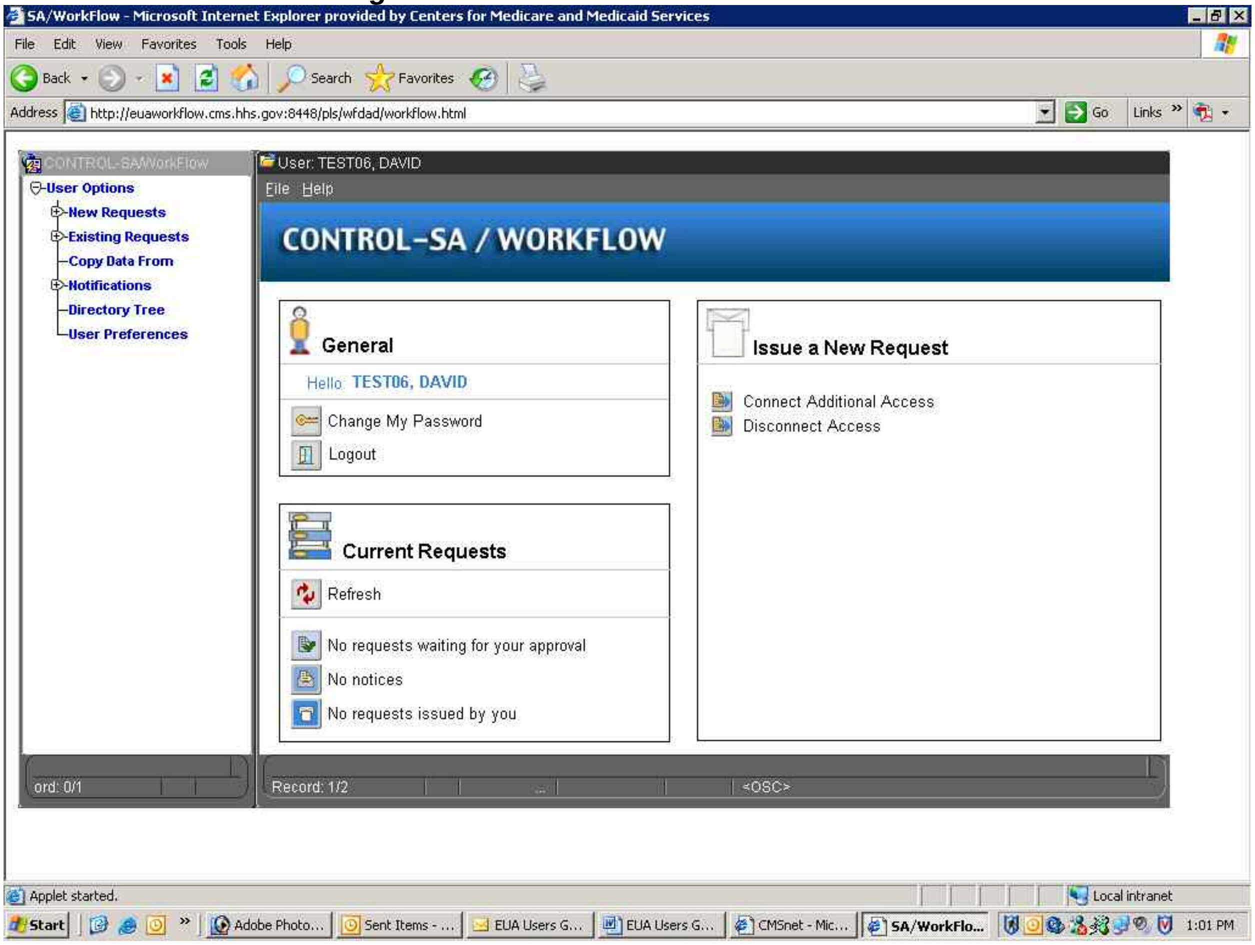
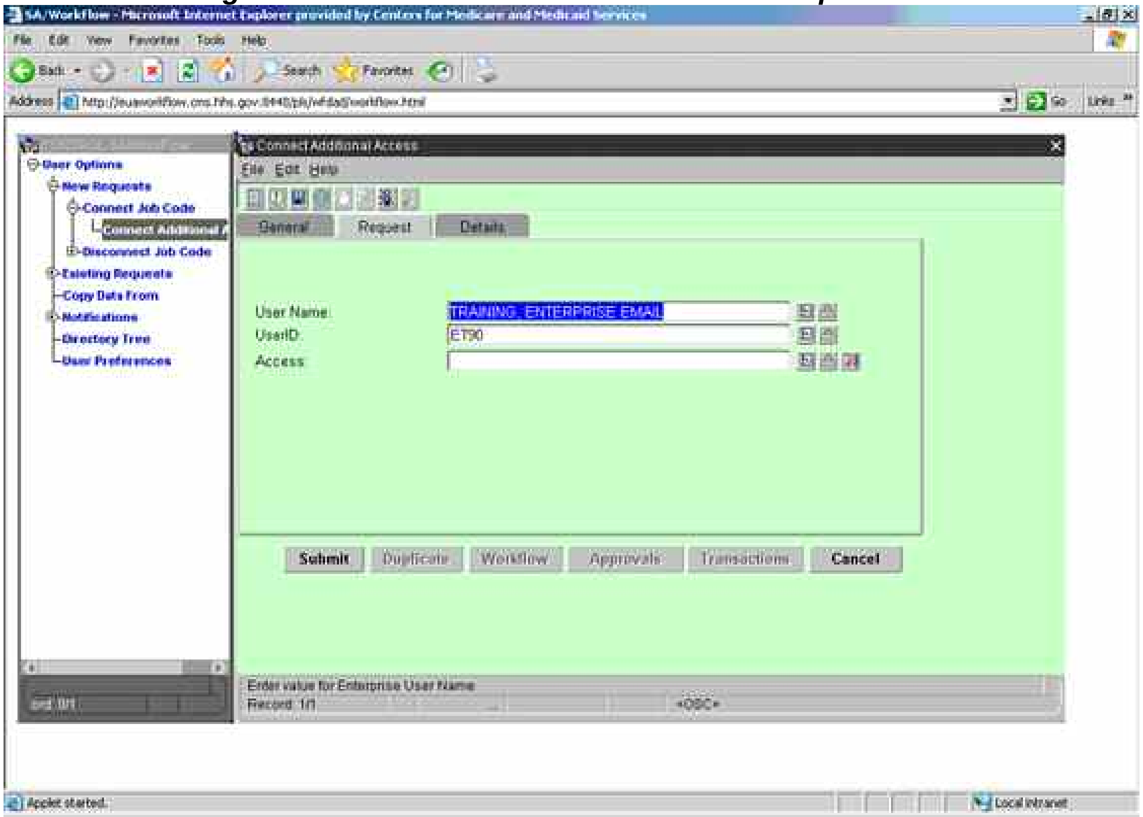


Figure 20 is displayed.

Figure 20—WorkFlow Connect Job Code Request Tab



Address: http://euaworkflow.cms.hhs.gov:8440/pls/wfdad/workflow.html

User Name: TRAINING, ENTERPRISE EMAIL

UserID: ET90

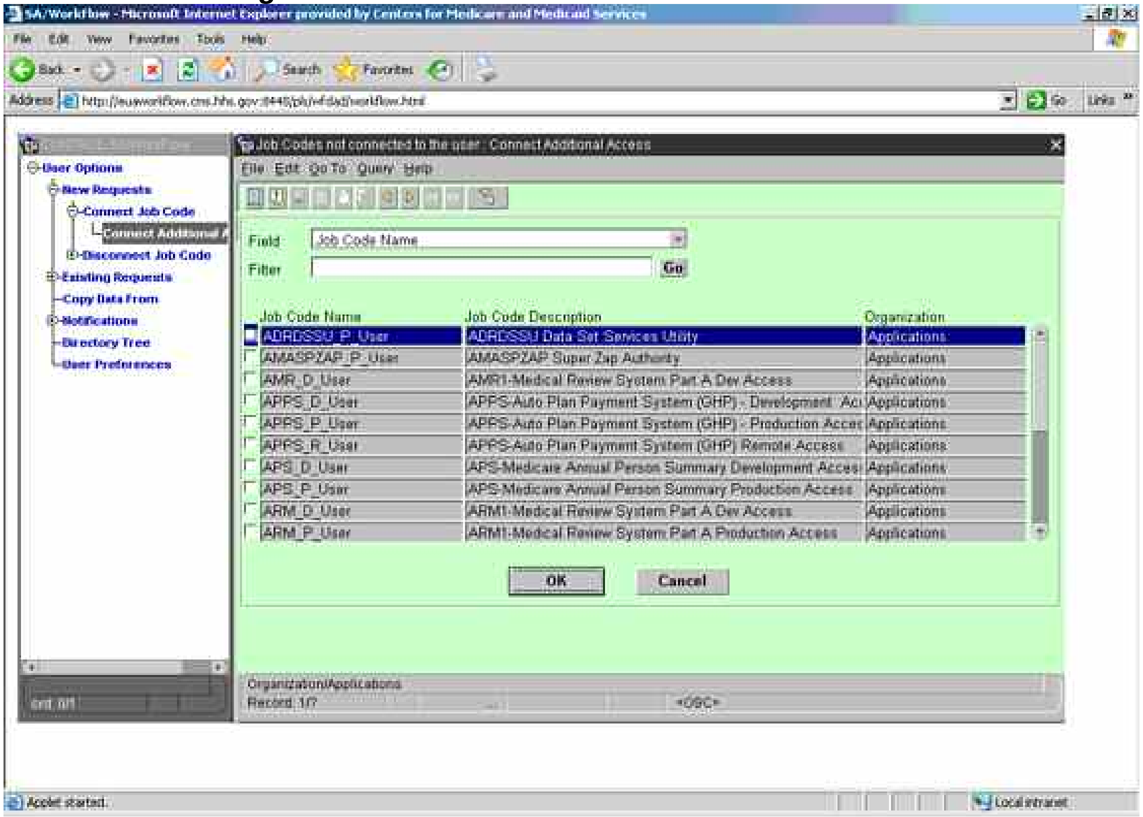
Access:

Enter value for Enterprise User Name

Record: 1/1 <OSC>

1. Key in the four-character CMS User ID in CAPS in the User ID field then type ENTER.
2. Verify the user’s name.
3. 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


SA/WorkFlow - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services
File Edit View Favorites Tools Help
Back Search Favorites
Address http://euaworkflow.cms.hhs.gov:8445/pls/wf-das/workflow.html
Go Links
User Options
New Requests
Connect Job Code
Connect Additional A
Disconnect Job Code
Existing Requests
Copy Data From
Notifications
Directory Tree
User Preferences
Job Codes not connected to the user : Connect Additional Access
File Edit Go To Query Help
OK
Cancel
Organization/Applications
Record: 1/7
<OSC>
Applet started.
Local intranet

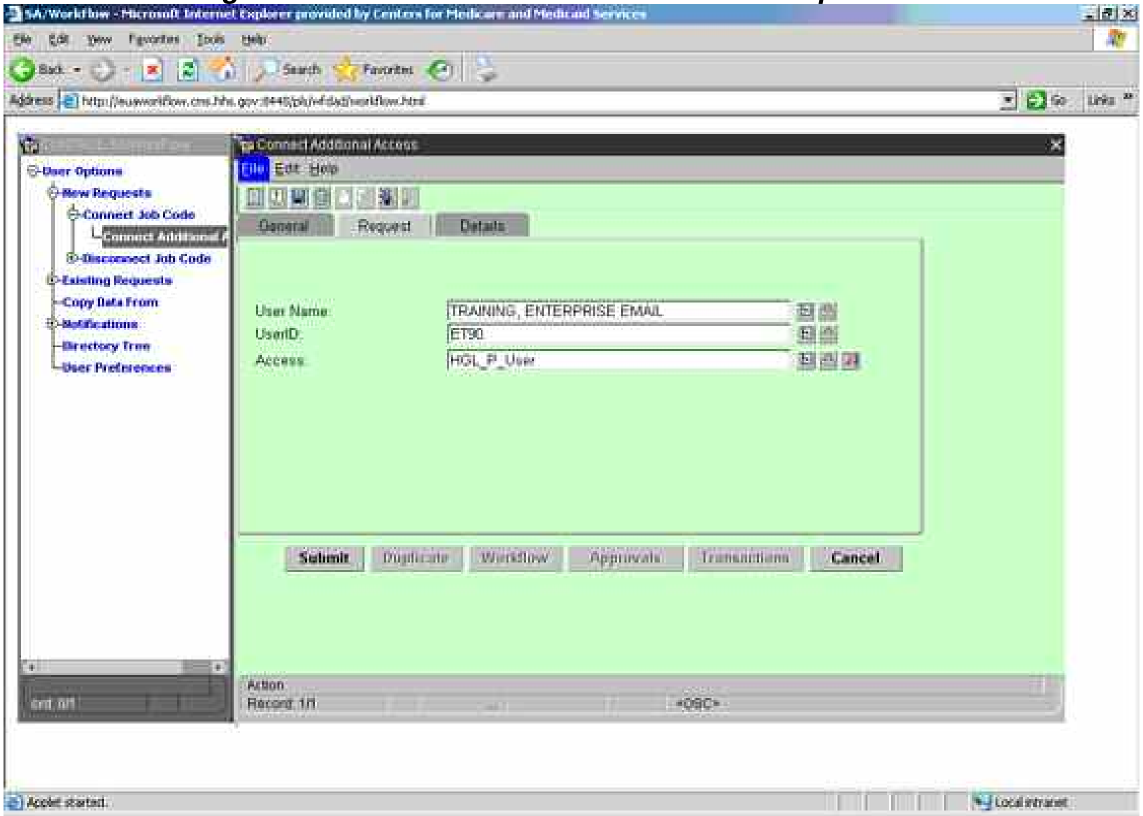
Field: Job Code Name

Filter: Go

	Job Code Name	Job Code Description	Organization
□	ADRDSSU_P_User	ADRDSSU Data Set Services Utility	Applications
□	AMASPZAP_P_User	AMASPZAP Super Zap Authority	Applications
□	AMR_D_User	AMR1-Medical Review System Part A Dev Access	Applications
□	APPS_D_User	APPS-Auto Plan Payment System (GHP) - Development Acı	Applications
□	APPS_P_User	APPS-Auto Plan Payment System (GHP) - Production Accec	Applications
□	APPS_R_User	APPS-Auto Plan Payment System (GHP) Remote Access	Applications
□	APS_D_User	APS-Medicare Annual Person Summary Development Acces	Applications
□	APS_P_User	APS-Medicare Annual Person Summary Production Access	Applications
□	ARM_D_User	ARM1-Medical Review System Part A Dev Access	Applications
□	ARM_P_User	ARM1-Medical Review System Part A Production Access	Applications

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

Figure 22—WorkFlow Connect Job Code Request Tab



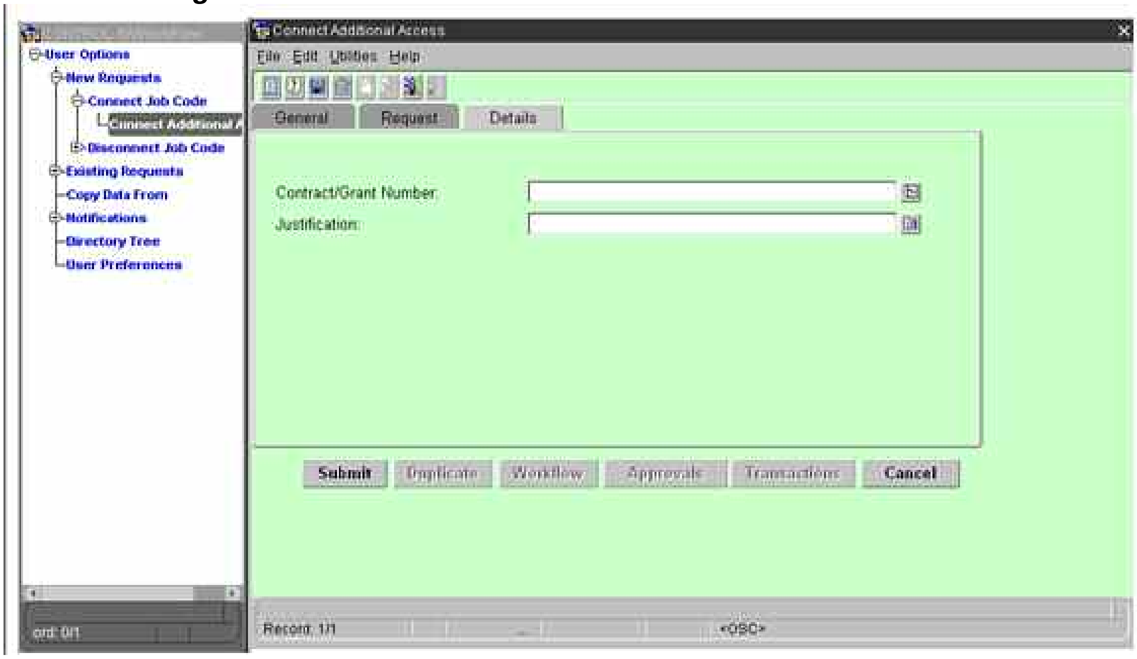
User Name: TRAINING, ENTERPRISE EMAIL

UserID: ET90

Access: HGL_P_User

7. Click on the detail tab and enter the justification and Contract Number.

Figure 23—WorkFlow Connect Job Code details Tab



Contract/Grant Number:

Justification:

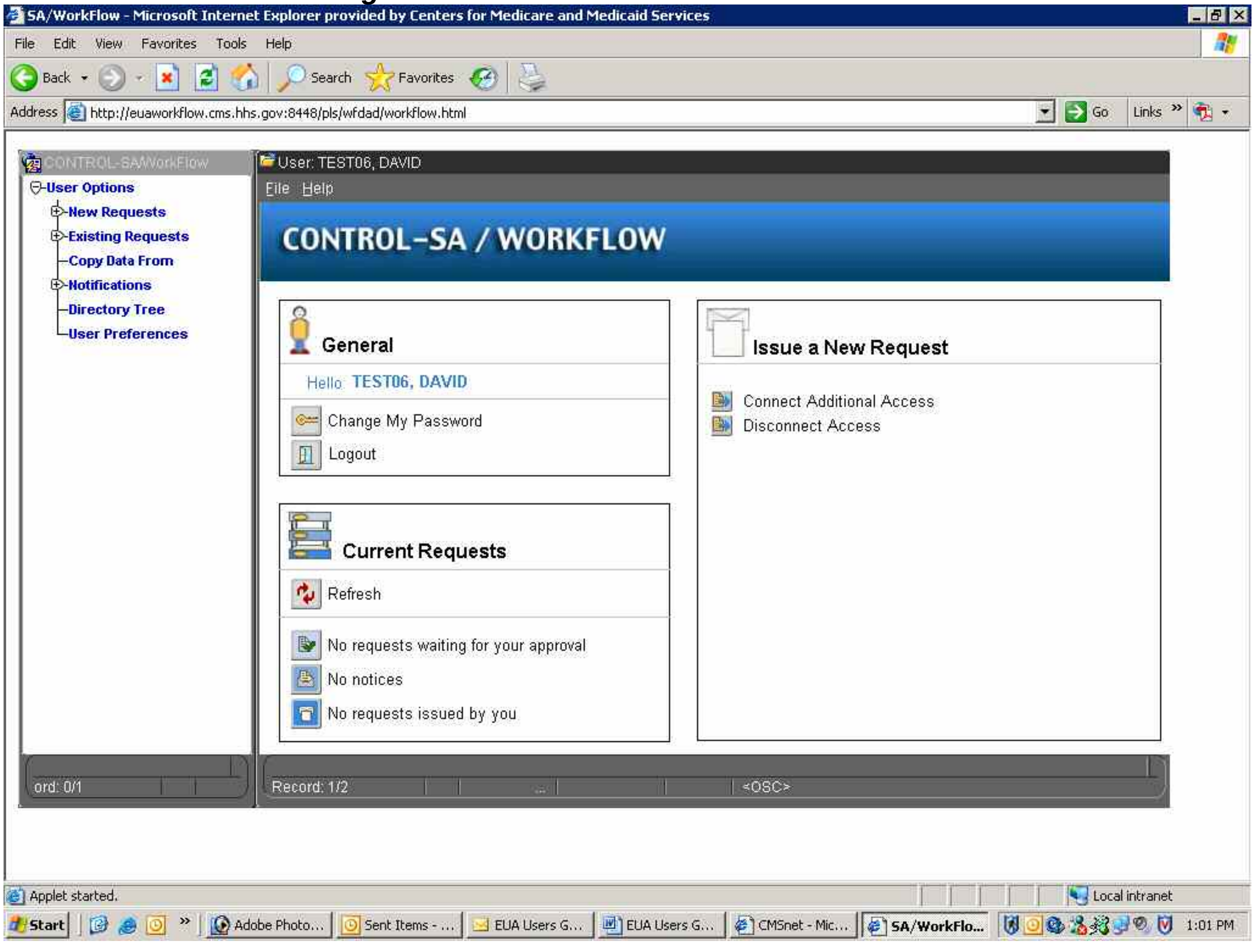
Submit request. A WorkFlow request number will be generated for your request. The request is routed to the designated approver. On approval, the access is granted.

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 24—WorkFlow Connect Job Codes



SA/WorkFlow - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services

Address http://euaworkflow.cms.hhs.gov:8448/pls/wfdad/workflow.html

User: TEST06, DAVID

Hello TEST06, DAVID

No requests waiting for your approval

No notices

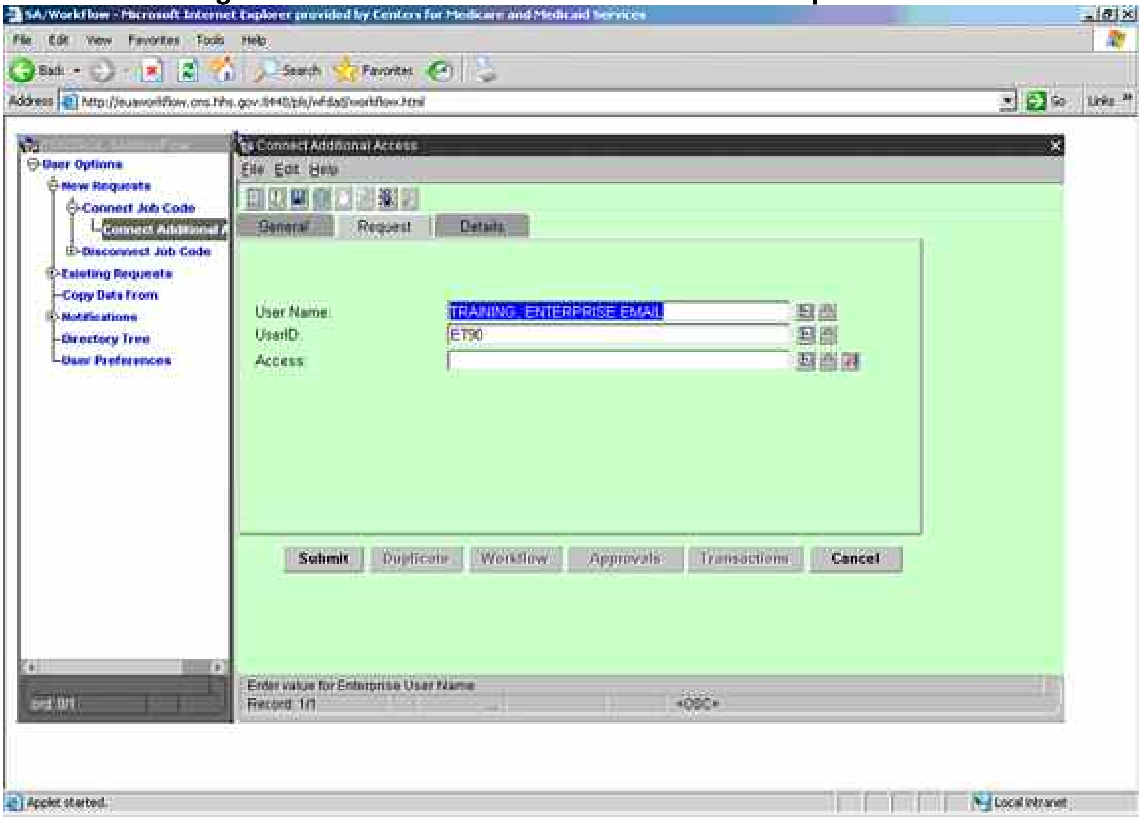
No requests issued by you

Record: 1/2

Applet started.

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

Figure 25—WorkFlow Connect Job Code Requests Tab



User Name: TRAINING, ENTERPRISE EMAIL

UserID: ET90

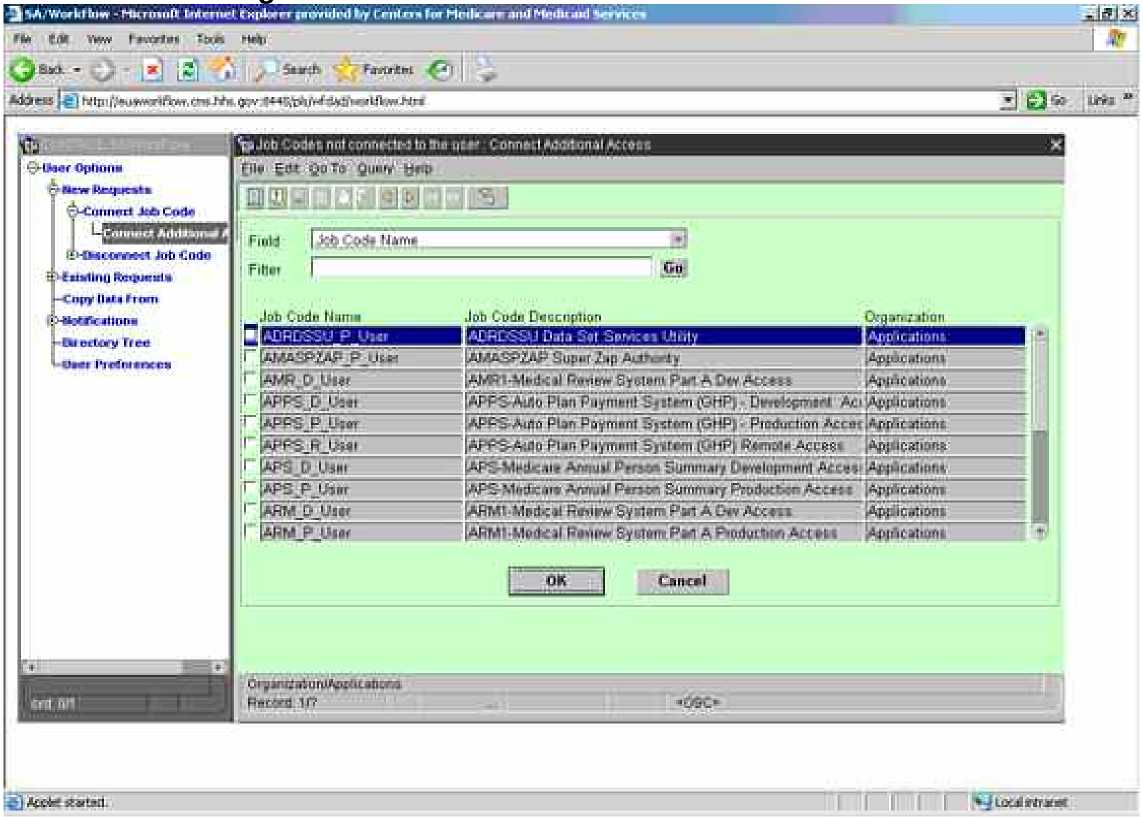
Access:

Enter value for Enterprise User Name

Record: 1/1 <OSC>

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



SA/Workflow - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services
File Edit View Favorites Tools Help
Back Search Favorites
Address http://euaworkflow.cms.hhs.gov:8445/pls/wf-dad/workflow.html
Go Links
User Options
New Requests
Connect Job Code
Connect Additional A
Disconnect Job Code
Existing Requests
Copy Data From
Notifications
Directory Tree
User Preferences
Job Codes not connected to the user : Connect Additional Access
File Edit Go To Query Help
OK
Cancel
Applet started.
Local intranet

Field: Job Code Name

Filter:

Go

	Job Code Name	Job Code Description	Organization
□	ADRDSSU_P_User	ADRDSSU Data Set Services Utility	Applications
□	AMASPZAP_P_User	AMASPZAP Super Zap Authority	Applications
□	AMR_D_User	AMR1-Medical Review System Part A Dev Access	Applications
□	APPS_D_User	APPS-Auto Plan Payment System (GHP) - Development Ac	Applications
□	APPS_P_User	APPS-Auto Plan Payment System (GHP) - Production Acces	Applications
□	APPS_R_User	APPS-Auto Plan Payment System (GHP) Remote Access	Applications
□	APS_D_User	APS-Medicare Annual Person Summary Development Acces	Applications
□	APS_P_User	APS-Medicare Annual Person Summary Production Access	Applications
□	ARM_D_User	ARM1-Medical Review System Part A Dev Access	Applications
□	ARM_P_User	ARM1-Medical Review System Part A Production Access	Applications

Organization/Applications
Record: 1/?
<OSC>

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.

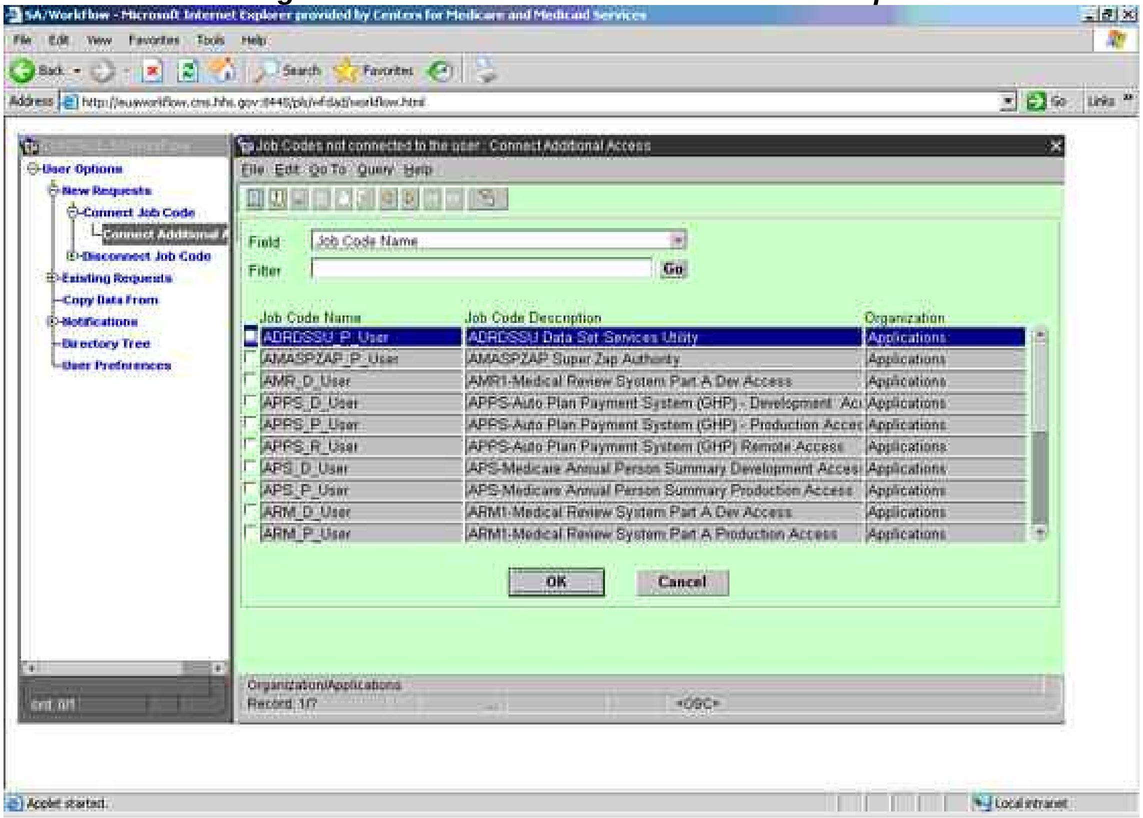
10. Click in the far left box of the required Job Code displayed; a check mark will appear.

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



SA/WorkFlow - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services
File Edit View Favorites Tools Help
Back Search Favorites
Address http://euaworkflow.cms.hhs.gov:8445/pls/wf/dad/workflow.html
Go Links
User Options
New Requests
Connect Job Code
Connect Additional A
Disconnect Job Code
Existing Requests
Copy Data From
Notifications
Directory Tree
User Preferences
Job Codes not connected to the user : Connect Additional Access
File Edit Go To Query Help

Field: Job Code Name

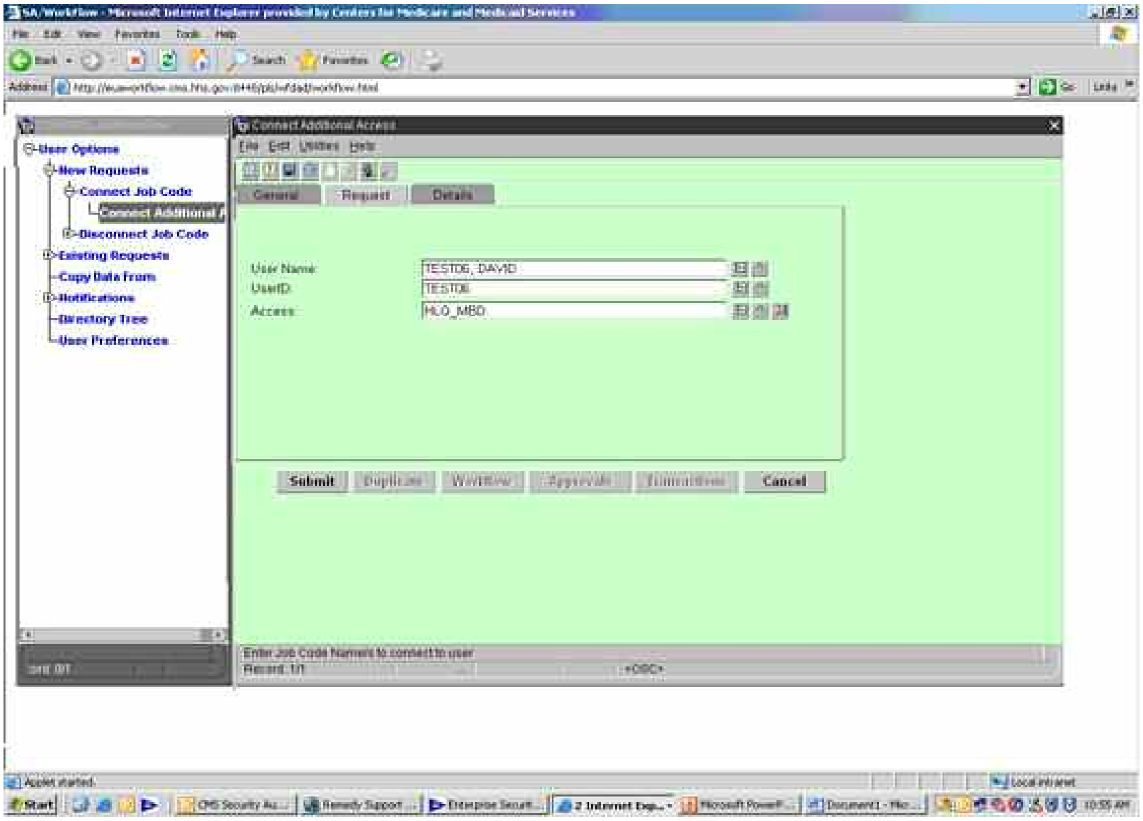
Filter:

	Job Code Name	Job Code Description	Organization
□	ADRDSSU_P_User	ADRDSSU Data Set Services Utility	Applications
□	AMASPZAP_P_User	AMASPZAP Super Zap Authority	Applications
□	AMR_D_User	AMR1-Medical Review System Part A Dev Access	Applications
□	APPS_D_User	APPS-Auto Plan Payment System (GHP) - Development Acc	Applications
□	APPS_P_User	APPS-Auto Plan Payment System (GHP) - Production Acces	Applications
□	APPS_R_User	APPS-Auto Plan Payment System (GHP) Remote Access	Applications
□	APS_D_User	APS-Medicare Annual Person Summary Development Acces	Applications
□	APS_P_User	APS-Medicare Annual Person Summary Production Access	Applications
□	ARM_D_User	ARM1-Medical Review System Part A Dev Access	Applications
□	ARM_P_User	ARM1-Medical Review System Part A Production Access	Applications

Organization/Applications
Record: 1/?
<OSC>

Applet started.

Figure 28—WorkFlow Connect Job Request Tab

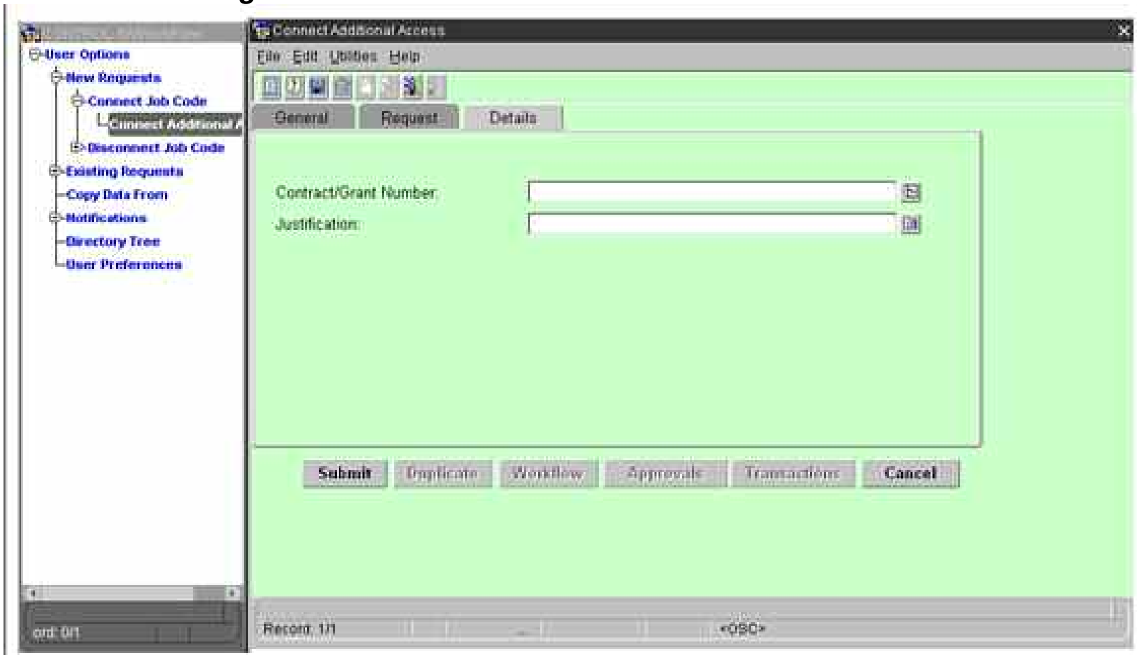


User Name: TESTO6, DAVID
UserID: TESTO6
Access: HLQ_MBD

Enter Job Code Name(s) to connect to user
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



Contract/Grant Number:

Justification:

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

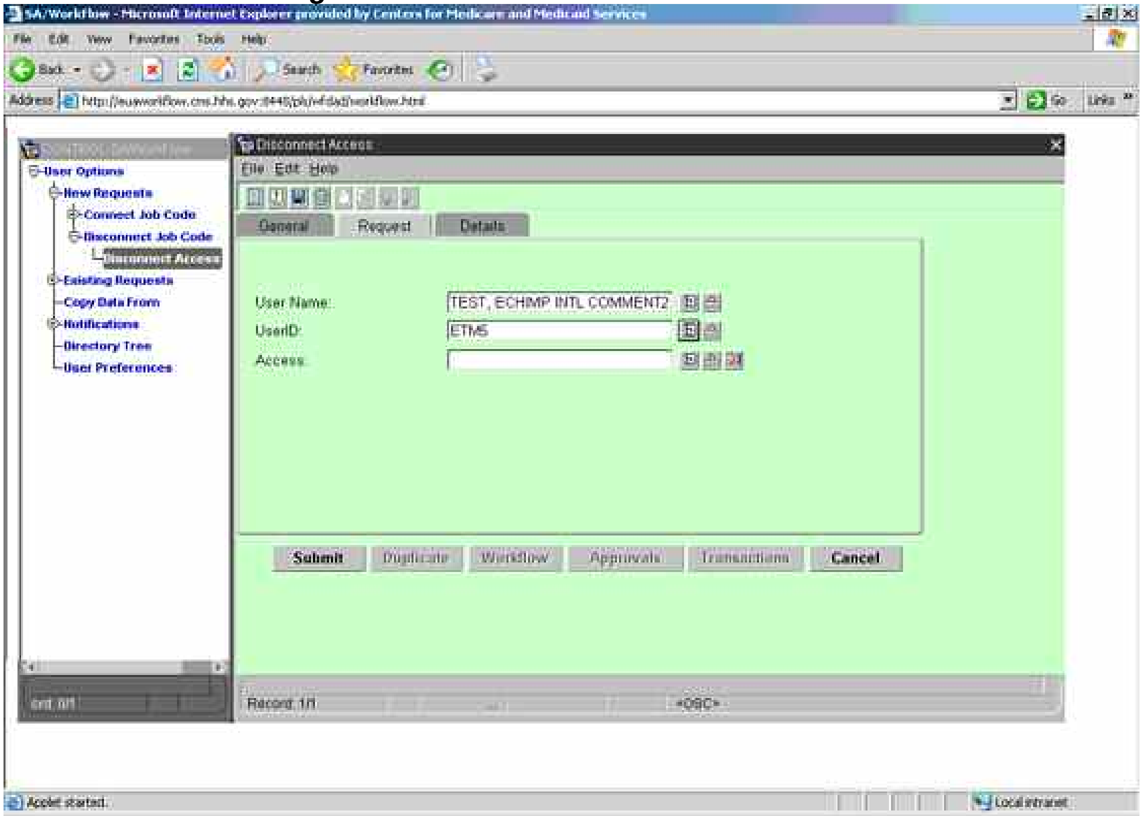
7.2 Disconnect Job Code

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.

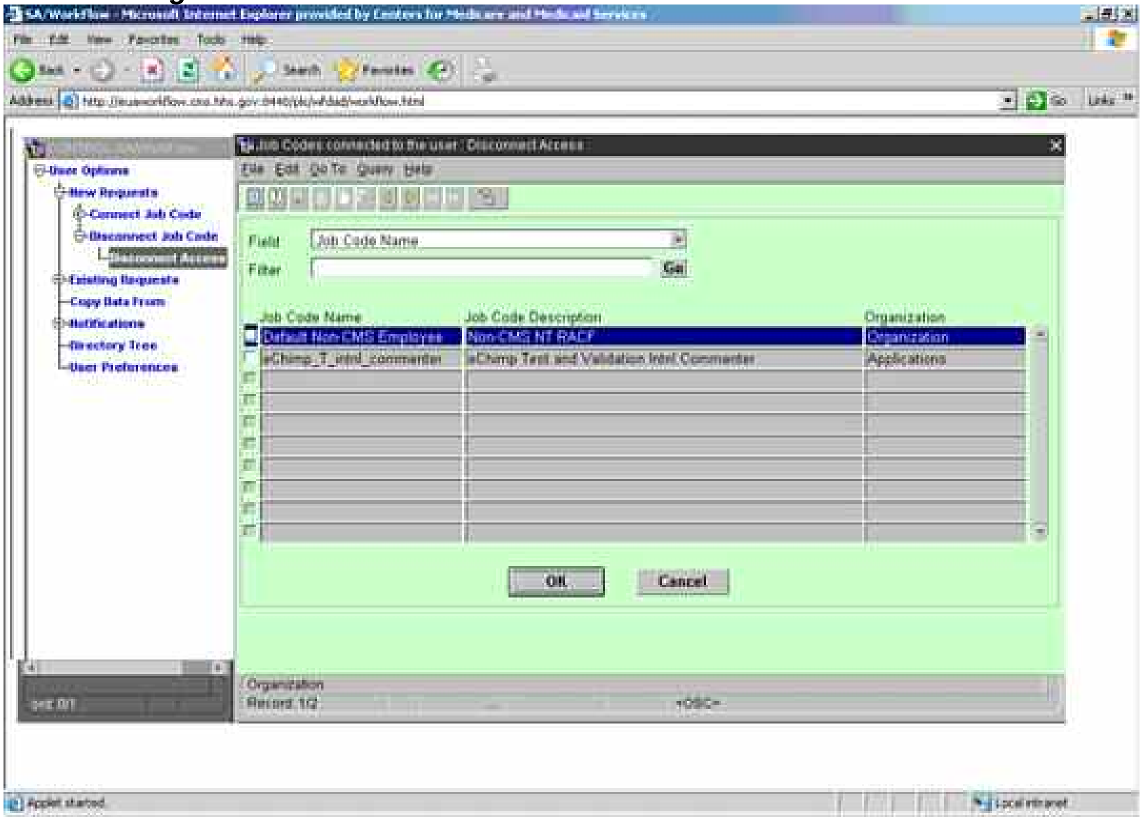
Figure 30—WorkFlow Disconnect Access



User Name: TEST, ECHIMP INTL COMMENT2
UserID: ETMS
Access:

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

Figure 31—WorkFlow Disconnect Access Job Code Selection


SA/WorkFlow - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services
File Edit View Favorites Tools Help
Back Search Favorites
Address http://euaworkflow.cms.hhs.gov:8440/pls/wfdad/workflow.html
Go Links
User Options
New Requests
Connect Job Code
Disconnect Job Code
Disconnect Access
Existing Requests
Copy Data From
Notifications
Directory Tree
User Preferences
Job Codes connected to the user : Disconnect Access
File Edit Go To Query Help
Go
OK
Cancel
Applet started
Local intranet

Field: Job Code Name

Filter:

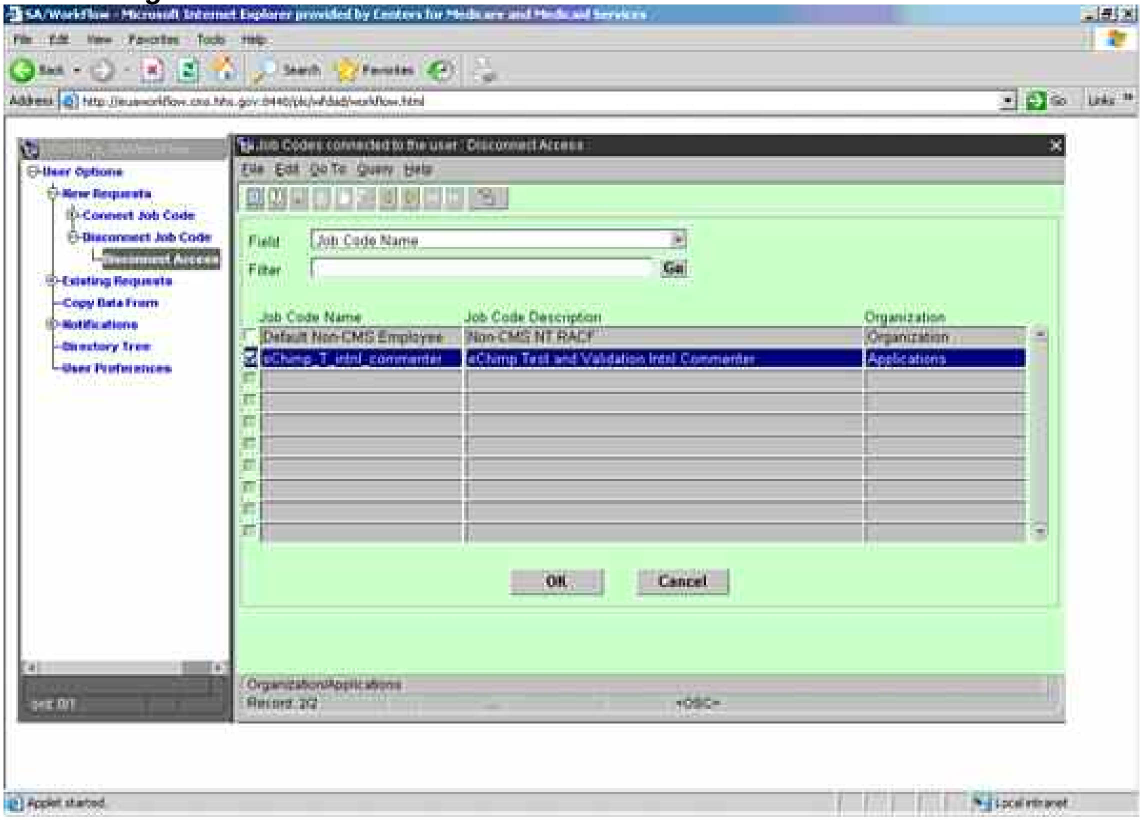
	Job Code Name	Job Code Description	Organization
□	Default Non-CMS Employee	Non-CMS NT RACF	Organization
□	eChimp_T_intnl_commenter	eChimp Test and Validation Intnl Commenter	Applications

Organization

Record: 1/2 <OSC>

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



Address: http://euaworkflow.cms.hhs.gov:8440/pls/wfdad/workflow.html

Field: Job Code Name

Filter:

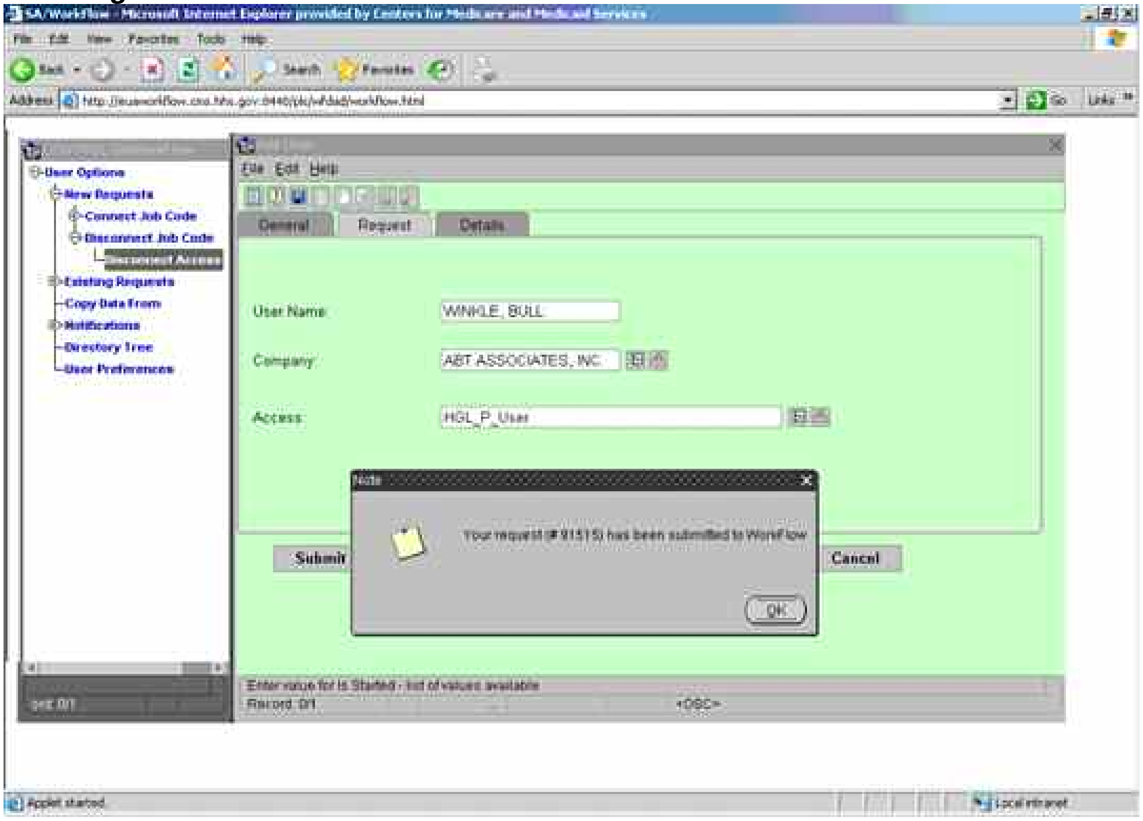
	Job Code Name	Job Code Description	Organization
□	Default Non-CMS Employee	Non-CMS NT RACF	Organization
☑	eChimp_T_intnl_commenter	eChimp Test and Validation Intnl Commenter	Applications
□			
□			
□			
□			
□			
□			
□			
□			

Organization/Applications

Record: 2/2 <OSC>

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



User Name: WINKLE, BULL

Company: ABT ASSOCIATES, INC

Access: HGL_P_User

Your request (# 91515) has been submitted to WorkFlow

Enter value for Is Started - list of values available

Record: 0/1 <OSC>

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.

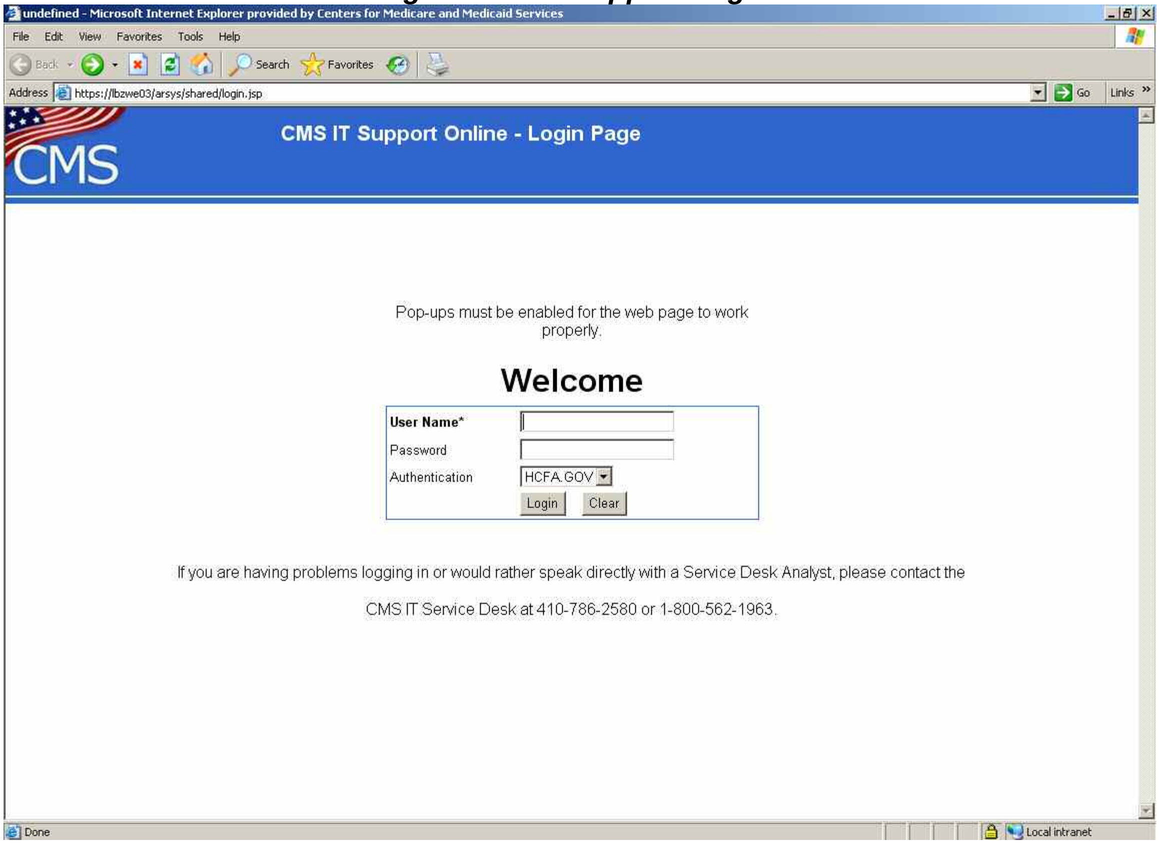
To open a trouble ticket, follow the few steps below.

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

IT SUPPORT.url

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

Figure 34—IT Support Logon



undefined - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services
File Edit View Favorites Tools Help
Back Search Favorites
Address https://lbzwe03/arsys/shared/login.jsp
Go Links
CMS
Done
Local intranet

CMS IT Support Online - Login Page

Pop-ups must be enabled for the web page to work properly.

Welcome

User Name*

Password

Authentication HCFA.GOV

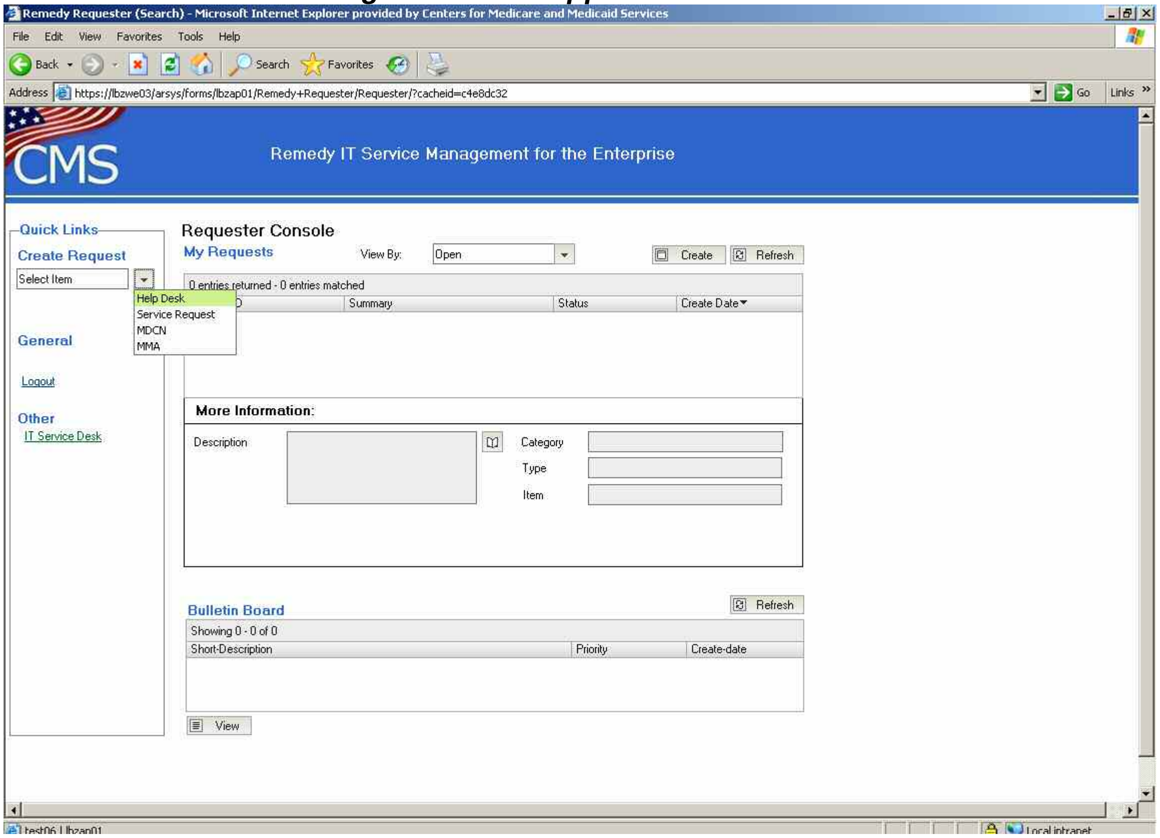
Login Clear

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



Remedy Requester (Search) - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services

Address https://lbzwe03/arsys/forms/lbzap01/Remedy+Requester/Requester/?cacheid=c4e8dc32

View By: Open

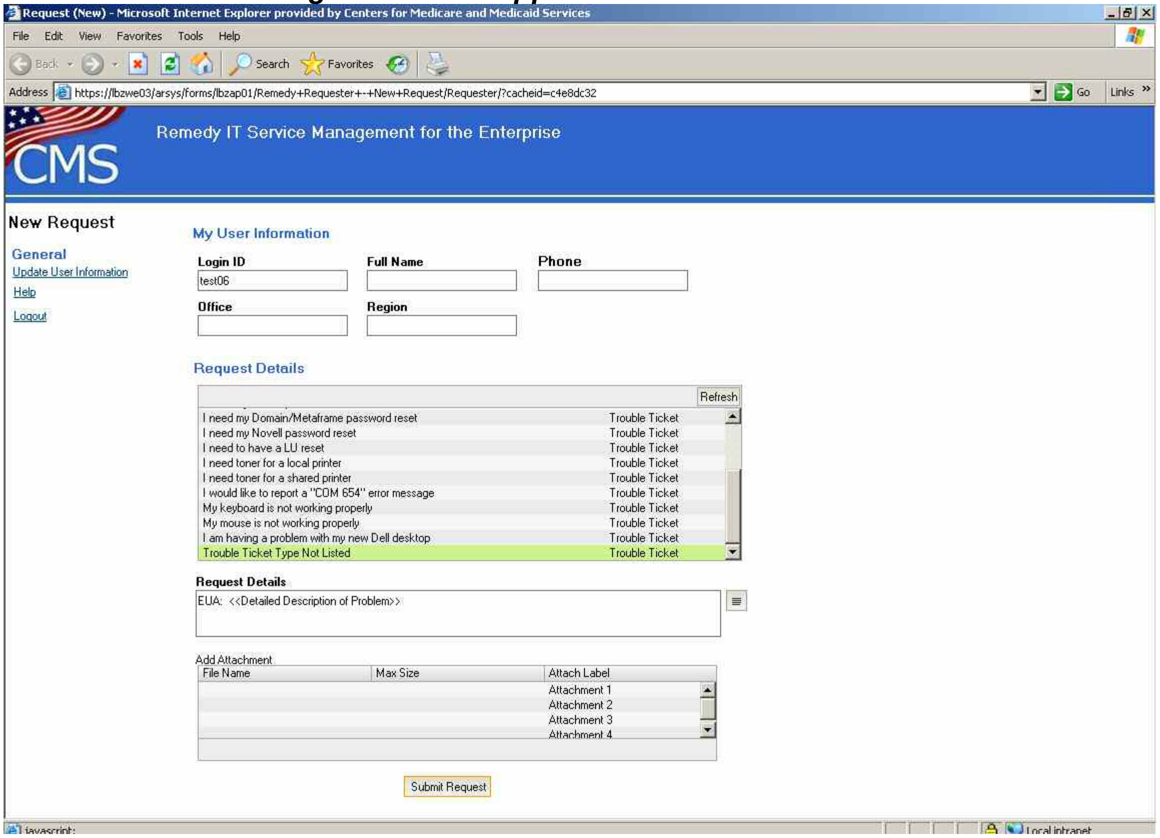
0 entries returned - 0 entries matched

Showing 0 - 0 of 0

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



Request (New) - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid Services
File Edit View Favorites Tools Help
Back Search Favorites
Address https://lbzwe03/arsys/forms/lbzap01/Remedy+Requester+-+New+Request/Requester/?cacheid=c4e8dc32
Go Links
CMS
Remedy IT Service Management for the Enterprise
New Request
General
Update User Information
Help
Logout

My User Information

Login ID: test06

Full Name:

Phone:

Office:

Region:

Request Details

I need my Domain/Metaframe password reset	Trouble Ticket
I need my Novell password reset	Trouble Ticket
I need to have a LU reset	Trouble Ticket
I need toner for a local printer	Trouble Ticket
I need toner for a shared printer	Trouble Ticket
I would like to report a "COM 654" error message	Trouble Ticket
My keyboard is not working properly	Trouble Ticket
My mouse is not working properly	Trouble Ticket
I am having a problem with my new Dell desktop	Trouble Ticket
Trouble Ticket Type Not Listed	Trouble Ticket

Request Details

EUA: <<Detailed Description of Problem>>

Add Attachment

File Name	Max Size	Attach Label
		Attachment 1
		Attachment 2
		Attachment 3
		Attachment 4

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.