

Technical Instructions for Accessing the Health Plan Management System (HPMS)

Upon completion of the HPMS migration scheduled for April 2, 2004, Medicare managed care organizations (MCOs) will have three connectivity options available to them:

1. Dial-up access through the AT&T-managed Medicare Data Communications Network (MDCN);
2. T-1/Lease Line access through the AT&T-managed MDCN; or
3. Internet access through a Secure Socket Layer Virtual Private Network (SSL VPN) using your organization's Internet Service Provider (ISP).

This document discusses the requirements and procedures for using each of these three methods. Options 1 and 2 require that your organization have an MDCN account from AT&T, while option 3 requires that your organization have Internet access via an account with an ISP. In all three cases, each user must have a valid CMS user ID and password for access to the HPMS system.

1. Dial-up access through the AT&T-managed MDCN

A. General Requirements:

This access method requires a PC workstation, with modem capability, and a copy of the AT&T Global Network Client software installed on the workstation. **These instructions refer to version 5.0x, the most recent version of the AT&T dialer client software.**

This software is available for download from the AT&T website at:

www.attbusiness.net/regctr. **It is recommended that organizations using an earlier version of this software visit the AT&T website and obtain the most recent version.**

As stated above, your organization must obtain an MDCN access account from AT&T to use this connection method. Information regarding account purchase and setup is available from Mr. Dana Fleming at 803-763-1460.

B. Migration Requirements:

If your organization uses the dial-up method to access HPMS today, certain steps must be taken to configure your AT&T account and your Global Network Client software for the migrated HPMS. AT&T is modifying all current MCO dial-up accounts to allow access to the new HPMS address. In addition, each user must modify their client dialer software to allow this access. To make this modification, follow these steps.

1. Verify that you are using the most recent version of the dialer software by starting the client and clicking on **Help**. While earlier versions will continue to permit access to the HPMS migration site, these instructions are written for users with version 5.0x of this software.

2. If you do not have the current version, go to the AT&T website at www.attbusiness.net/regctr to download and install version 5.0x of the dialer client. During the software setup process, do not make an entry when prompted for a DNS Server name.

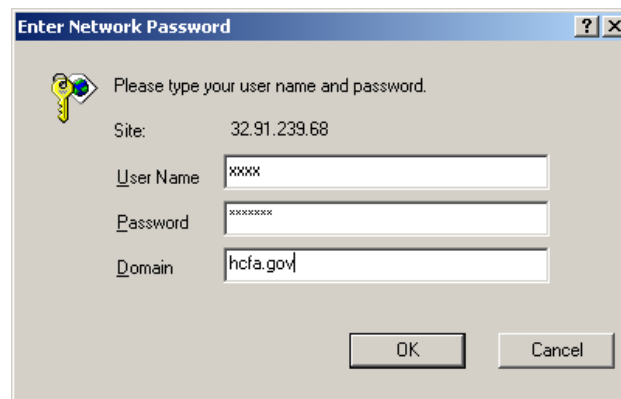
C. Dial Connection Process:

To connect to the HPMS Migration site, start the AT&T Global Network Client software and login to the MDCN network using your AT&T Global Network Client user ID and password.

NOTE: The procedure discussed here will work with either version 4.x or 5.x of the dialer software.

Upon connecting to the MDCN network, start the Microsoft Internet Explorer browser software and enter the HPMS migration site IP address (**32.91.239.68**) in the Address field at the top of the browser screen. At this point, you will be presented the following screen (Figure 1) for logging into the HPMS application using your CMS-issued user ID. After entering a valid CMS user ID, password, and domain (**hcfa.gov**) on this screen and clicking on the **OK** button, you will be taken to the HPMS homepage.

Figure 1



2. T-1/Lease Line access through the AT&T-managed MDCN

A. General Requirements:

Connecting to the HPMS application using this method also requires an MDCN account with AT&T. An account of this type establishes a permanent high-speed link between your organization's local area network and the MDCN network. While this type of account is more costly, it is recommended for organizations with higher usage/access rates. When this option is selected, AT&T technicians work closely with the organization's local network managers to ensure that both networks are optimally configured to permit access from the user site to the HPMS application.

B. Migration Requirements:

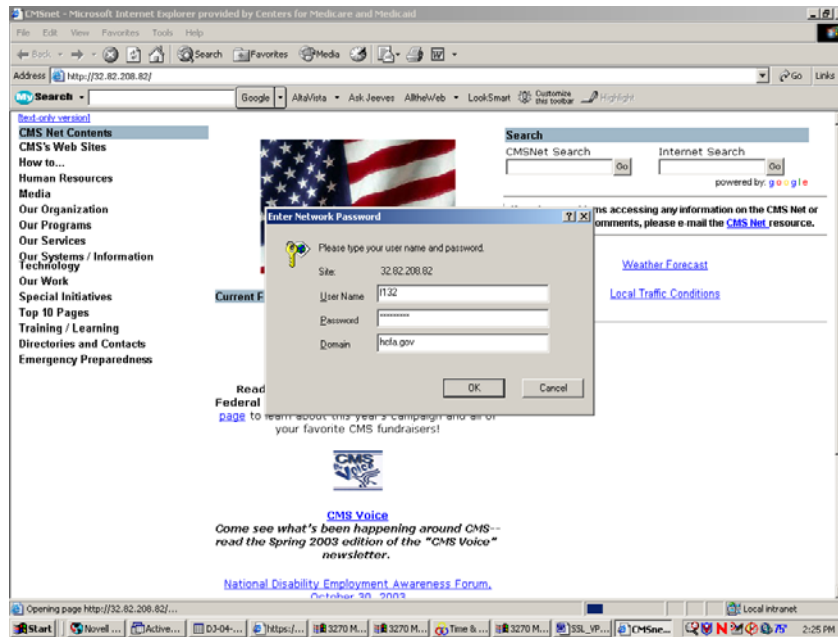
If your organization uses a T-1/lease line to access HPMS today, certain steps must be taken to configure your existing account for the migrated HPMS. In this instance, your local network managers must work closely with AT&T network engineers to ensure that connectivity exists from your local site through the MDCN network to the HPMS migration site. This will require changes to both your network and the MDCN network. To ensure connectivity, MCO local network managers must:

1. Modify your network to permit traffic from the HPMS Migration IP address into your network environment. The HPMS Migration IP address is: **32.91.239.68**.
2. Notify CMS and AT&T of your network source IP addresses, so that AT&T can modify the MDCN network to permit traffic from your network source address to the HPMS Migration IP address. To assist with this step, CMS distributed a questionnaire on September 11, 2003 to all MCOs, which requested that you identify your method of connectivity to the system and all network source IP information. This questionnaire and its cover memorandum are available on the HPMS homepage (see 9/11/2003 item). We urge any organizations that have not yet returned this questionnaire to do so as soon as possible to ensure proper connectivity to the HPMS migration site.

C. T-1/Lease Line Connection Process:

Because this option provides a permanent connection from the organization to the MDCN network, there is no need for the user to establish network connectivity for each HPMS session. Rather, this connectivity is established during the account setup. To connect using this option, the user starts their Microsoft Internet Explorer browser software and enters the HPMS migration site IP address (**32.91.239.68**) in the Address field at the top of the browser screen. The HPMS login prompt will then appear (Figure 2). At this prompt, the user must enter a valid CMS-issued user ID and password and **hcfa.gov** in the domain field. Clicking on the **OK** button will bring the user to the HPMS homepage and the start of their HPMS session.

Figure 2



3. Internet access through an SSL VPN using your organization's ISP

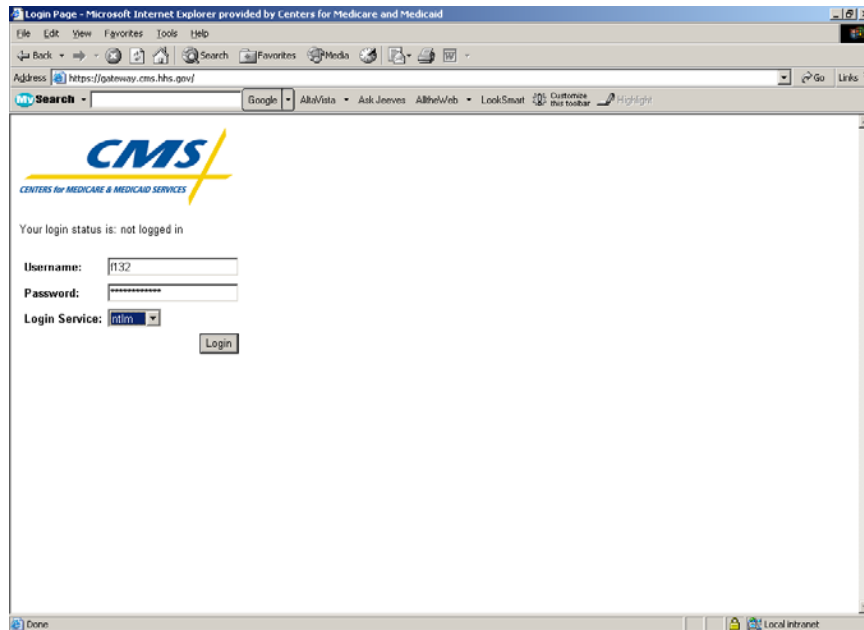
A. Requirements:

The only requirement for this option is that the user must have access to the Internet from their workstation. There are no other unique requirements for the user or their Internet Service Provider for accessing the HPMS application using this option.

B. SSL VPN Connection Process:

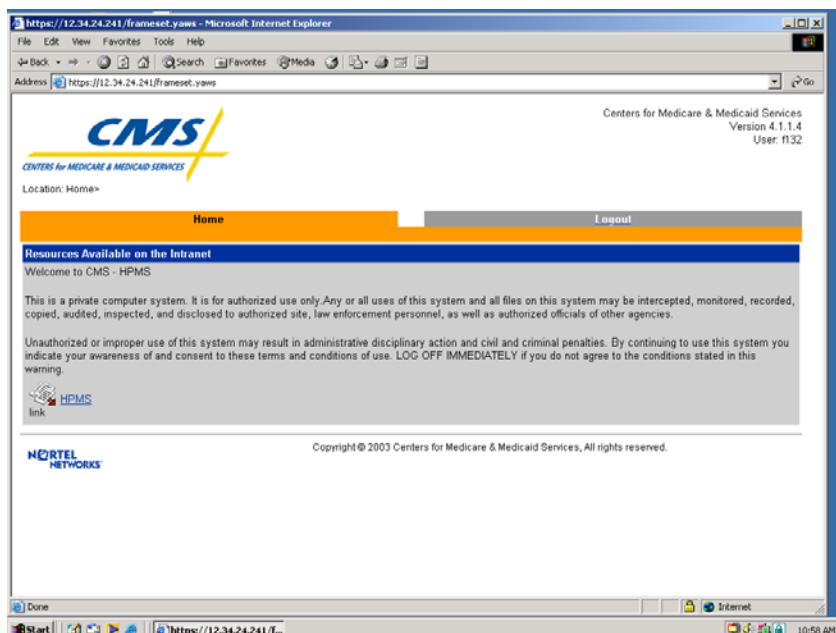
To connect to the HPMS application using this option, the user will first initiate an Internet session through their existing, local ISP using the Microsoft Internet Explorer browser software. Next, the user will enter <https://gateway.cms.hhs.gov> in the Address field at the top of the browser screen. The user will be taken to the CMS SSL VPN authentication screen as shown in Figure 3.

Figure 3



At this point, the user must enter a valid CMS-issued user ID and password in the appropriate fields. In addition, the user must select **hcfa.gov** as the Login Service. Once the user clicks on the **Login** button, they will be taken to the CMS SSL VPN Portal Page (Figure 4). This screen provides a link to the HPMS system. By selecting this link, the user will be taken to the HPMS homepage to begin their session.

Figure 4



Resetting an Expired Password

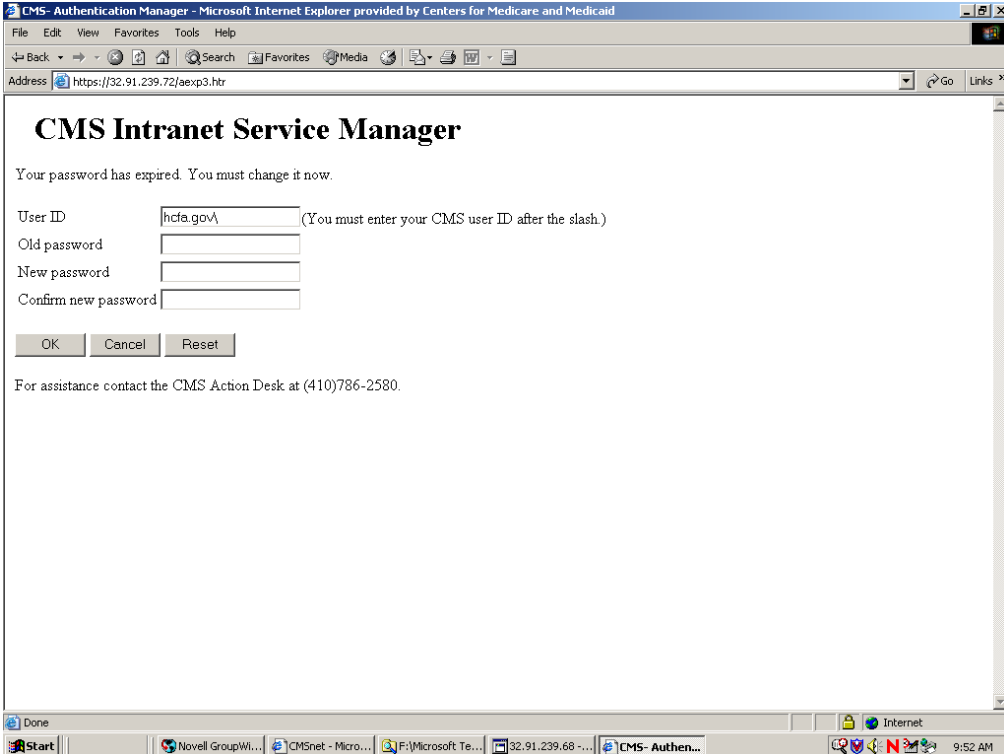
The screens presented to the HPMS user for the purposes of resetting expired passwords will look slightly different depending on your selected access method. This section describes the two primary methods for resetting passwords in HPMS.

A. Dial-Up and T-1/Lease Line Access through the MDCN Network:

You may receive a message during the login process from the “CMS Intranet Service Manager” prompting you to reset an expired password (Figure 5). To reset your password, you must complete the information required on this screen as follows:

1. In the Account field, enter your four-character CMS user ID after the hcfa.gov\.
2. In the Old Password field, enter the same password you provided on the previous screen just prior to reaching this point.
3. In the New Password field, enter a new password of your choice, ensuring that it is at least six to eight characters long and uniquely different from your current password.
4. In the Confirm New Password field, re-enter your new password.
5. Click on the **OK** button to complete the password change.

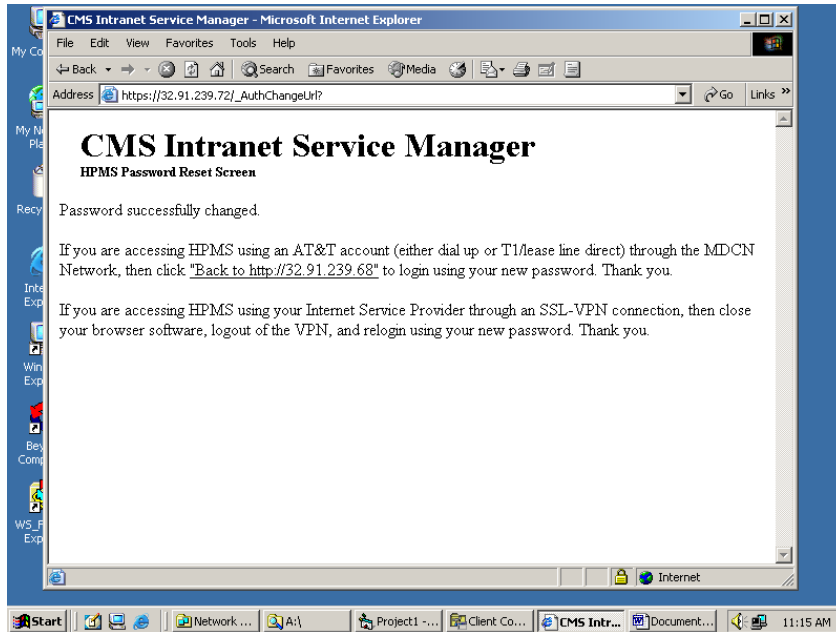
Figure 5



The screenshot shows a web browser window titled "CMS - Authentication Manager - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid". The address bar shows "https://32.91.239.72/jaexp3.htm". The main content area displays the "CMS Intranet Service Manager" header and a message: "Your password has expired. You must change it now." Below this message are four input fields: "User ID" (containing "hcfa.gov\"), "Old password", "New password", and "Confirm new password". There are three buttons: "OK", "Cancel", and "Reset". At the bottom, it says "For assistance contact the CMS Action Desk at (410)786-2580." The Windows taskbar at the bottom shows the Start button and several open applications, including "Novell GroupWi...", "CMSnet - Micro...", "F:\Microsoft Te...", "32.91.239.68 ~...", and "CMS- Authen...". The system clock shows "9:52 AM".

You will then see a “Security Alert” message that asks if you would like to proceed. Click on the **Yes** button to confirm that you do wish to proceed. You will then see another message stating that your password was successfully changed (Figure 6).

Figure 6

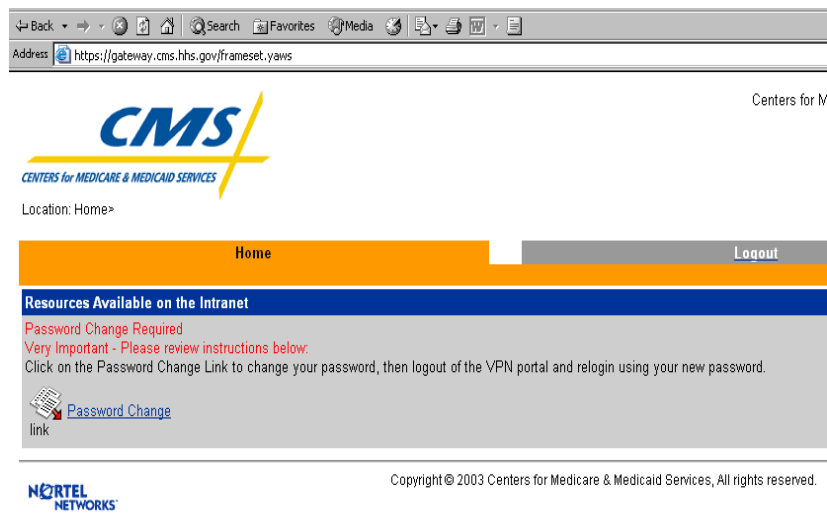


Because you are using the MDCN, click on the “**Back to <http://32.91.239.68>**” link to return to the HPMS login process. Proceed to login using your new reset password.

B. Internet Access through the CMS SSL VPN:

If your password expires when you are attempting to login using the SSL VPN, you will see the screen shown in Figure 7. This screen instructs the user to click on the “Password Change” link, which is highlighted in blue, to proceed to change their password.

Figure 7



After clicking on this link, you will be taken to the screen shown in Figure 8. To reset your password, complete the information required on this screen as follows:

1. In the Account field, enter your four-character CMS user ID after the hcfa.gov\.
2. In the Old Password field, enter the same password you provided on the previous screen just prior to reaching this point.
3. In the New Password field, enter a new password of your choice, ensuring that it is at least six to eight characters long and uniquely different from your current password.
4. In the Confirm New Password field, re-enter your new password.
5. Click on the **OK** button to complete the password change.

Figure 8

IIS - Authentication Manager - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Centers for Medicare and Medicaid Services

SSL VPN password reset screen

Your password has expired. You can change it now.

Account

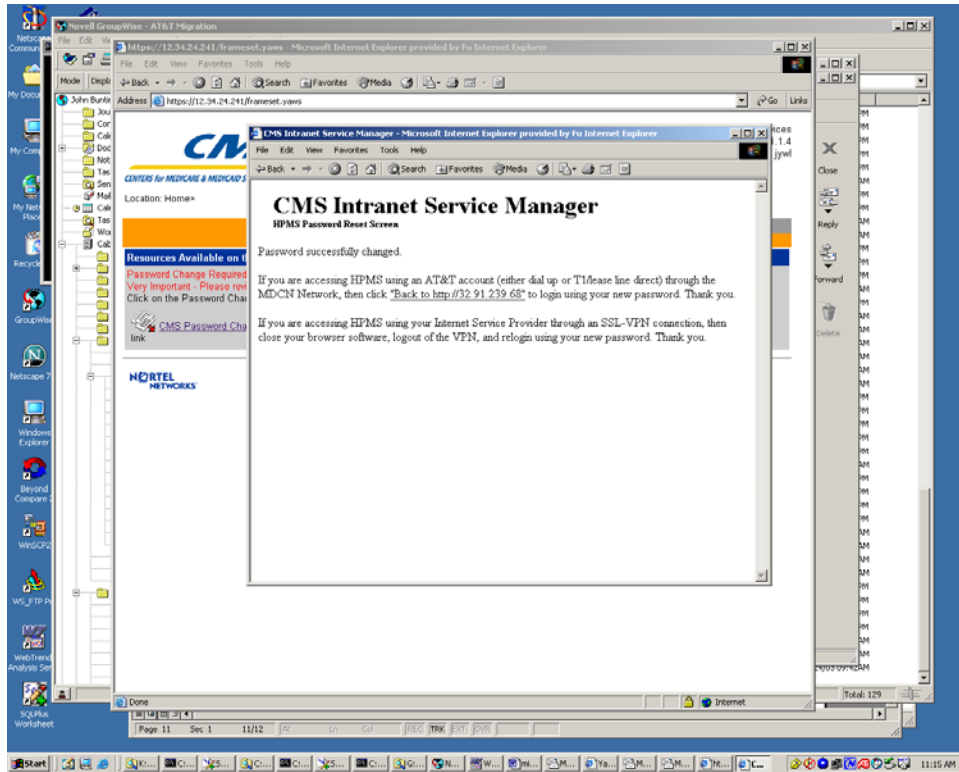
Old password

New password

Confirm new password

You will then see the following screen (Figure 9) confirming your password reset. Because you are using the SSL VPN, you must close the “CMS Intranet Service Manager” browser window, logout of the SSL VPN by clicking on the “Logout” link on the portal page, and login again to the SSL VPN portal using your new password.

Figure 9



NOTE: The password resetting screenshots for the SSL VPN solution are preliminary and are subject to change.

Technical Assistance

Please contact Don Freeburger at either 410-786-4586 or dfreeburger@cms.hhs.gov with questions about these instructions.