
Provider OnLine

Log-In Instructions

Table of Contents

1 LOG-IN ACCESS	3
1.1 ENTERING THE USER ID AND PASSWORD	3
1.2 OVERVIEW AND PURPOSE OF ENTRUST.....	4
1.2.1 <i>Log-in for Users Who Are Active, But Not Currently Enrolled in Entrust</i>	4
1.2.2 <i>If the User Account Is Locked</i>	8
1.2.3 <i>Logging In for the First Time</i>	10
APPENDIX A: FREQUENTLY ASKED QUESTIONS	10
WHAT IF A USER WANTS TO ESTABLISH AN ACCOUNT FOR PROVIDER ONLINE, WHAT STEPS ARE REQUIRED?	10
WHAT IF A USER SUSPECTS SOMEONE KNOWS HIS OR HER PASSWORD?	10
WHAT HAPPENS IF THE USER’S ACCOUNT IS INACTIVE?	10
WHAT HAPPENS IF THE USER FORGETS OR WANTS TO CHANGE HIS OR HER PASSWORD?.....	10
WHAT HAPPENS IF THE USER FORGETS HIS OR HER USER ID?	10
WHAT IF THE USER CANNOT ACCESS PROVIDER ONLINE EVEN AFTER ENTERING THE USER ID AND PASSWORD?	10

1 Log-in Access

A link to Provider Online (POL) is located on the MedStar Select and MedStar Medicare Choice website. <http://www.MedStarProvidernetwork.com>

The provider homepage — which is public information contains information specifically designed for practitioners and providers affiliated with MedStar Select or MedStar Medicare Choice.

On the navigation menu, there is a box for authorized users to enter their established user ID and password to gain access to the secure POL.

1.1 Entering the User ID and Password

A user ID and password are required to gain access to the secure information on POL. These credentials are entered in the box displayed below, available on the left-hand navigation bar of the Provider homepage.

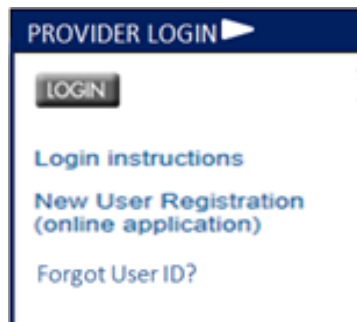


Figure 1: Log-in Box

The user ID is a unique identifier assigned to the user when he or she registers for access to POL. The password must be a minimum of eight characters. The password is case sensitive. Once the credential information is entered, click on the **Login** button.

This will grant the user access to the secure POL — if the credentials entered are accurate.

1.2 Overview and Purpose of Entrust

To establish more security around MedStar Health’s secure portals for members, providers, and employers, Entrust, a multifactor anti-phishing authentication device has been added. Many health care and financial organizations use Entrust, or a similar solution, to add more security around highly sensitive information like private health information.

Entrust provides the ability to not only verify the user, but the terminal (PC, laptop, etc.) from which the user is accessing the portal(s). This makes it necessary for users to validate themselves on each terminal on which they access the portal by answering the secret question challenge response.

During the registration process, users choose three questions to answer and they also choose a security image or “token” in which they assign a phrase, which become part of the normal sign-in process.

Authentication is restricted to three attempts to sign on to the portal. Following the third failed attempt to sign on, the account is locked and the user is required to contact the Health Plan Help Desk and speak to a representative to resolve the situation.

1.2.1 Log-in for Users Who Are Active, But Not Currently Enrolled in Entrust

Users that have active accounts, but are not currently enrolled for in Entrust, will have to register for the Entrust authentication.

1. The user logs in using his or her current user ID for POL.

User Login

Please enter your user id to login to HealthPlan Online.
If you forgot your user id, use the I forgot my user id link below.

HealthPlan Online Login:

UserID

[I forgot my user id](#)

Figure 2: Entrust: Login with POL User ID

2. After the user enters his or her user ID, the user is prompted to enter the current password.

HealthPlan Online Login

Enter your password to login to HealthPlan Online.
If you can't remember your password, use the "I forgot my password" link below.

HealthPlan Online Login:

Password [I forgot my Password](#)

Figure 3: Entrust: Enter Current POL Password

3. The user is then prompted to select and answer three security questions. (There are ten challenge questions. The three shown in this illustration are just an example.) It is important that the user remember his or her challenge questions and answers.

Set Challenge Questions/Responses

Please choose three distinct questions and Answers.
Please keep note of your Questions and Answers, as you will be required to answer them if there are ever problems with your account.

Challenge Questions

Challenge Question #1 :	What town were you born in?	<input type="text" value="Baltimore"/>
Challenge Answer #1 :		
Challenge Question #2 :	What is your favorite Sports team ?	<input type="text" value="Ravens"/>
Challenge Answer #2 :		
Challenge Question #3 :	What is your favorite color?	<input type="text" value="Blue"/>
Challenge Answer #3 :		

Figure 4: Entrust: Answer Three Security Questions

- After the user establishes his or her challenge questions and submits them, the user will need to choose a security image. (Each time the user logs in, he or she should look for this image and the corresponding phrase to be assured the website is a legitimate POL website.) The left-hand navigation bar can be used to display more images for the user to choose from.

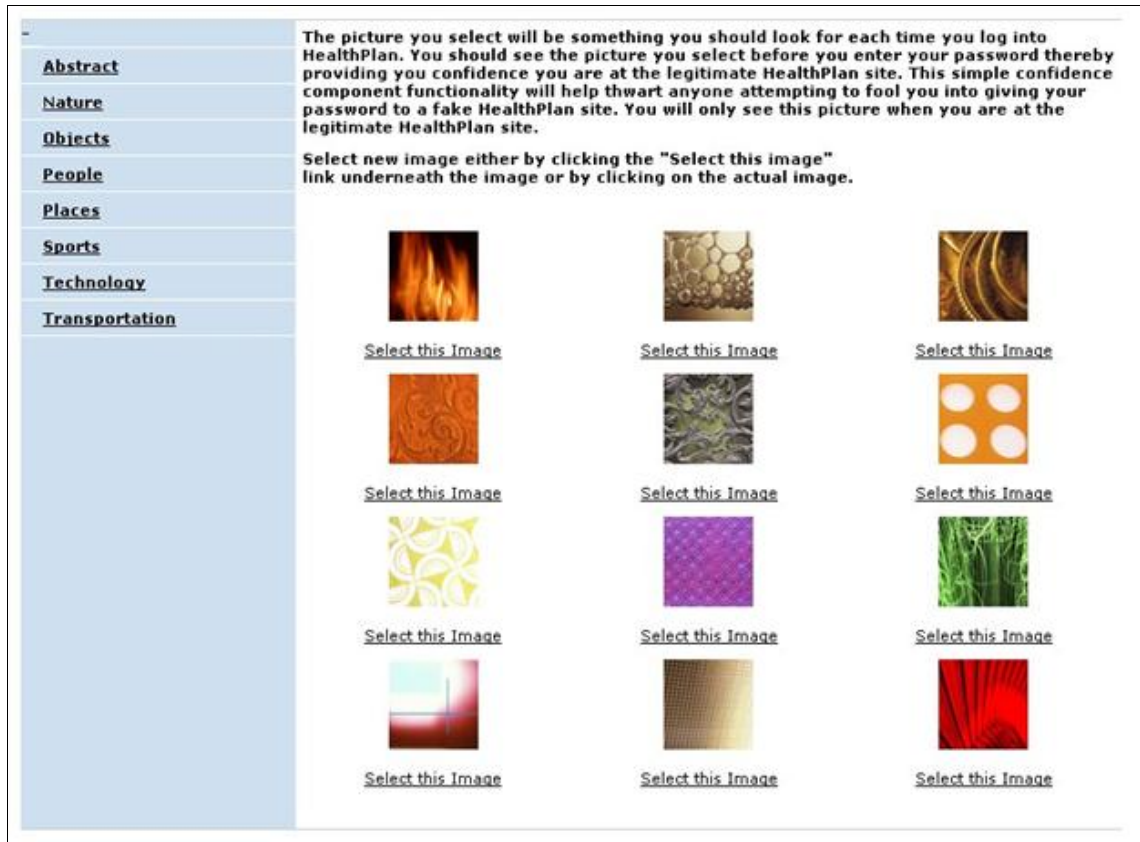



Figure 5: Entrust: Selecting a Security Image

- After the user chooses the security image, he or she will need to provide a message to associate with the image. The message can be as simple or as complex as the user would like. This message will always be displayed with the selected image from the previous step. If upon subsequent log-ins, the image and/or the message are not what the user established at initial setup, the user should not continue with the log-in process.

Enter Welcome Message

The welcome message you select will be something you should look for each time you log into HealthPlan. You should see the welcome message before you enter your password thereby providing you confidence you are at the legitimate HealthPlan site. This simple confidence component functionality will help thwart anyone attempting to fool you into giving your password to a fake HealthPlan site. You will only see this picture and welcome message when you are at the legitimate HealthPlan site.



Enter Welcome Message

Figure 6: Entrust: Establishing a Welcome Message

6. The user will be prompted to enter a new password that must be between 8 and 14 characters and contain at least three upper case characters and numbers. (There is a link on the password change screen to assist the user in creating a strong password.)

Filling out the Fields on this page, will allow you to change your password.
Please enter the Password you would like to change it to in the fields below. This will be an immediate change.

Change Password	
User Name:	<input type="text"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Password must be between 6 and 14 characters long and contain at least three of the following: <ul style="list-style-type: none"> • UpperCase Character • Number 	
Strong Password Guidelines	
<input type="button" value="Submit"/>	

Figure 7: Entrust: Password Change Screen

7. After the password is submitted, the user will then go to the POL homepage.

1.2.2 If the User Account Is Locked

1. If the user's account is locked due to unsuccessful password attempts, the following message will appear

Please Answer the following Questions so that we can Verify your Identity. Answering these questions helps us protect your account from intruders.

What is your favorite pets name?


 There is currently an issue with your account and it has been temporarily locked. Please [click here](#) to contact the Help Desk.

Figure 8: Entrust: Locked Account

-
2. Next, the user should select [click here](#) from the highlighted area above. A screen with the Health Plan Help Desk contact information will appear. Both the phone number and e-mail address are provided.

1.2.3 Logging In for the First Time

When the user tries to log in to the website after initial registration — and also after the initial session with POL — the log-in screens will appear slightly different to the user.

The user will first be asked to enter his or her user ID. The user will then be asked to answer one of his or her challenge questions. After answering the challenge question correctly, the user will be presented with the security image and corresponding phase.

Appendix A: Frequently Asked Questions

What If a user wants to establish an account for Provider OnLine, what steps are required?

All new users to Provider OnLine must first complete the Provider OnLine Registration Form, which can be downloaded from our public website at the following link <http://MedStarProviderNetwork.com>

What if a user suspects someone knows his or her password?

The user has the option to continue to use the current password until it expires or to change it immediately. The user can initiate a password change by selecting the “**Forgot My Password**” option during the log-in process. The user will have to answer challenge questions, which will also allow the user to change the current password.

What happens if the user’s account is inactive?

If the user logs in with his or her user ID and the account is inactive, he or she will receive a message to contact Provider Services at 1-855-242-1042.

What happens if the user forgets or wants to change his or her password?

After the user enters his or her user ID, a prompt for the password appears. Instead of entering the password, the user should click on **I forgot my password link**. The user will then need to answer some of the security questions established during the initial registration process. The user will then be prompted to reset his or her password.

What happens if the user forgets his or her user ID?

The user should call Provider Services at 1-855-242-1042.

What if the user cannot access Provider OnLine even after entering the user ID and password?

The user can also call Provider Services at 1-855-242-1042.