



The Enterprise System Process Guide

Introduction

Contents

System Introduction	1
Overview	1
HHAX System Key Terms and Definitions	1
System Login and User Interface	2
Privacy and Confidentiality Acknowledgement Requirements	4
Multi-Factor Authentication (MFA)	5
User Setup of MFA	5
Changing User MFA Settings	8
Adding a Mobile Phone Number	9
Change a Mobile Phone Number	10
Remove a Mobile Phone Number or Email Address	11
Change Default MFA Method	12
System Status Link	13
The Navigation Panel	15
15-Minute System Session Timeout	16

System Introduction

Overview

The HHAExchange (HHAX) **Enterprise** system is the all-encompassing platform offering a complete suite of functions and features facilitating the Homecare exchange process that connects Providers, Payers, Patients, and Caregivers under one umbrella.

With HHAExchange, Agencies can manage their business in a fully integrated solution, including the ability to:

- manage Agency demographics and system settings;
- perform Patient intake functionality;
- enter Caregiver data and track compliance;
- schedule Patients and Caregivers visits;
- confirm visits via EVV through a variety of methods (including IVR and a GPS-enabled Caregiver Mobile Application);
- invoice, bill, and track the utilization of authorizations; and
- perform payroll activities.

This category provides a high-level overview of the basic components and user interface of the *Enterprise* system, to include:

- how to Log In to the system,
- navigation of the system Modules;
- HHAX nomenclature and keyword configuration, and
- access to documentation in resources via the Support Center.

Please direct any questions, thoughts, or concerns regarding the content herein to [HHAExchange Customer Support](#).

HHAX System Key Terms and Definitions

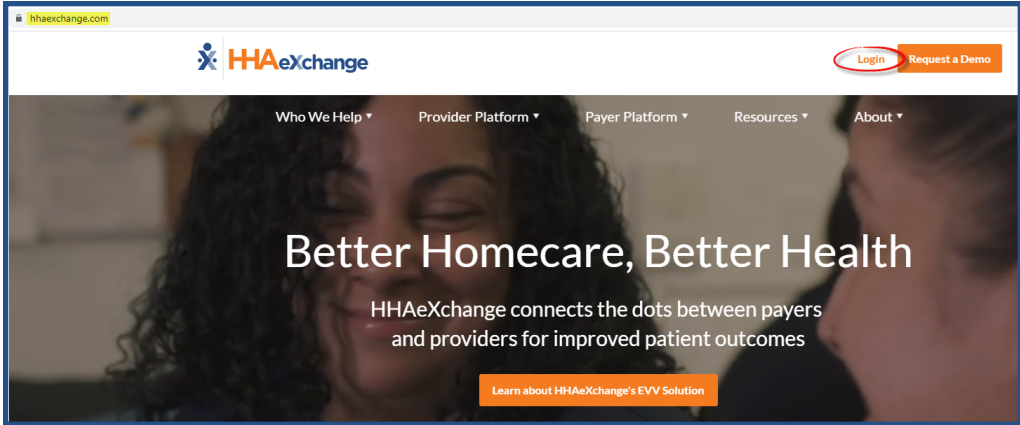
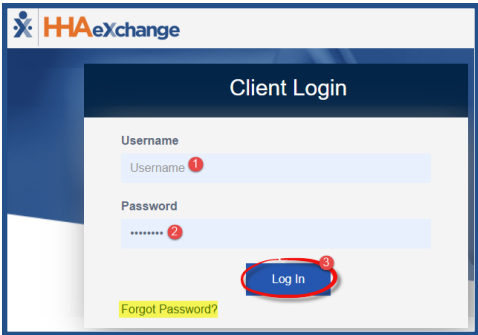
The following provides basic definition of HHAX System key terms applicable throughout the document.

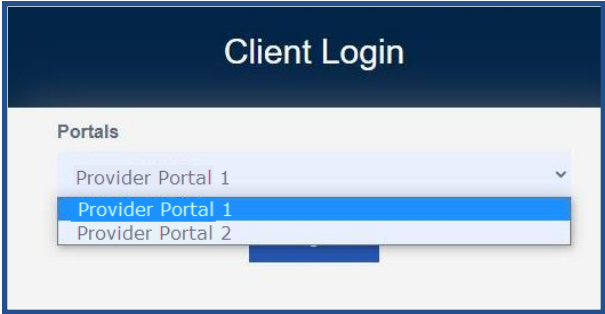
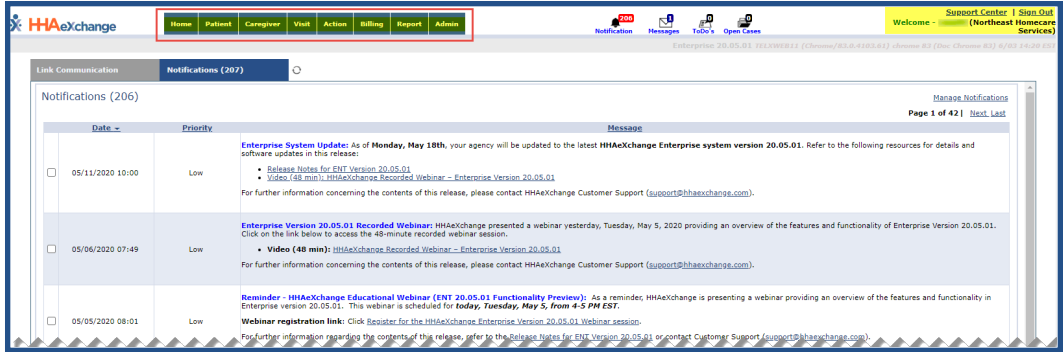
Term	Definition
Patient	Refers to the Member, Consumer, or Recipient. The Patient is the person receiving services.
Caregiver	Refers to the Aide, Homecare Aide, Homecare Worker, or Worker. The Caregiver is the person providing services.
Provider	Refers to the Agency or organization coordinating services.
Payer	Refers to the Managed Care Organization (MCO), Contract, or HHS. The Payer is the organization placing Patients with Providers.
HHAX	Acronym for HHAExchange

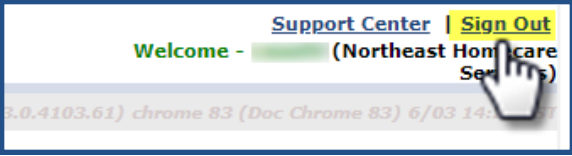
System Login and User Interface

All HHAX platforms are web-based applications requiring an internet connection to access the system. Any disruptions to internet service ends a user’s session, as the HHAX *Enterprise* platform does not support an “offline” mode. Additionally, if the system does not detect any activity for 15 minutes, the user is logged off for security purposes. Refer to the [15-Minute System Session Timeout](#) section for details.

The following table provides instructions on how to access HHAX systems.

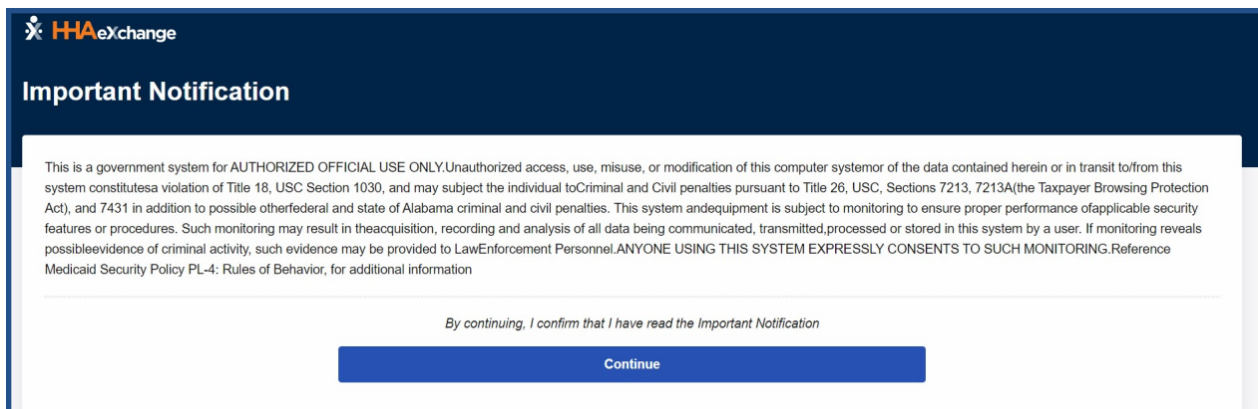
Step	Action
1	Open Internet Explorer and navigate to https://hhaexchange.com
2	<p>On the HHAX homepage, click the Login link.</p>  <p style="text-align: center;">HHAExchange.com</p>
3	<p>At the login window, enter user credentials as shown in the image below and click the Log In button.</p>  <p style="text-align: center;">Client Login Window</p> <p>Note: Click on the <i>Forgot Password?</i> link and follow system prompts to reset your password. Refer to the Self-Service Password Reset Job Aid for further details.</p>

Step	Action
4	<p><i>This step applies only to users with access to multiple portals.</i></p> <p>For users who have access to multiple portals, the system now prompts for an application selection once the Username and Password has been entered, as illustrated in the image to the right.</p> <div data-bbox="548 457 1149 768" data-label="Image">  </div> <p style="text-align: center;">Selecting a Portal</p>
5	<p>The system opens to the Home module, displaying recent System Notifications (via the Notifications tab). The Link Communication tab serves as a communication dashboard for correspondence between Payers and Providers who service Linked Contract Patients. Refer to the Communications (Linked Contracts) topic for full details and instructions. The <i>Notifications</i> tab displays the recent System Notifications issued by HHAX.</p> <p>The top panel is static* containing the Navigation Panel in the center and links to the Support Center and Logout to the right. User details are also indicated underneath the links along with the system environment in which the user is currently logged into.</p> <div data-bbox="321 1171 1377 1520" data-label="Image">  </div> <p style="text-align: center;">Navigation Panel and User Info, Highlighted in Yellow</p> <p>*These items remain permanent at the top of the screen regardless of where the user navigates in the system; allowing for easy navigation between modules and access to HHAX Support.</p>

Step	Action
6	<p>To log out of the system, click the Sign Out link.</p>  <p style="text-align: center;">Sign Out Link</p>

Privacy and Confidentiality Acknowledgement Requirements

Some users may be required to acknowledge a Privacy and Confidentiality statement before accessing the system. When presented, click on the **Continue** button to acknowledge and route to the *Home* screen.



Privacy and Confidentiality Acknowledgment

This setting can be adjusted by HHAX System Administration at an Office level for Providers who have multiple offices. Contact the [HHAX Support Team](#) for assistance.

Multi-Factor Authentication (MFA)

DISCLAIMER

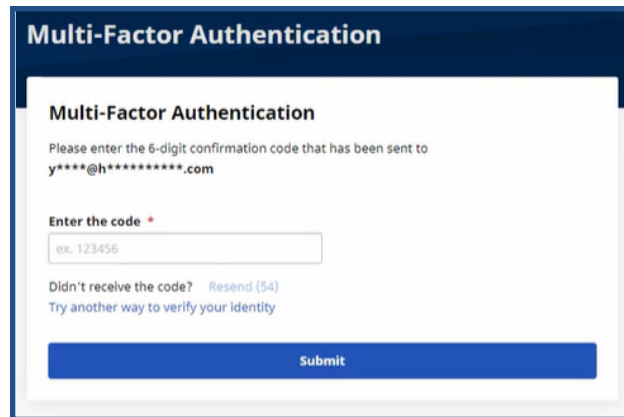
This feature is enabled by HHAX System Administration. Contact the [HHAX Support Team](#) for assistance.

Tip: You can press **Ctrl-F** on your keyboard to search this topic.

Multi-Factor Authentication (MFA) is an additional user security method that can be required at the Payer level and at the Provider Office level. When MFA is required, users must enter their Username and Password in addition to a unique and random system-generated code, obtained at a secure location (such as the verified mobile phone or email address on file).

After MFA is set up, upon logging into the system with their Username and Password, a six-digit system-generated code is sent to the user's designated secure location (email address or mobile phone).

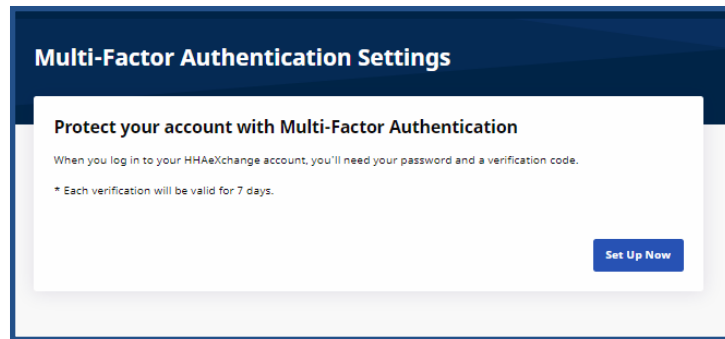
All users subject to MFA are asked to verify their identity using a unique MFA code every 30 days. Once the code is sent, the user has 30 minutes to enter and submit the code on the Authentication page to be allowed access to the system.



MFA Request Page

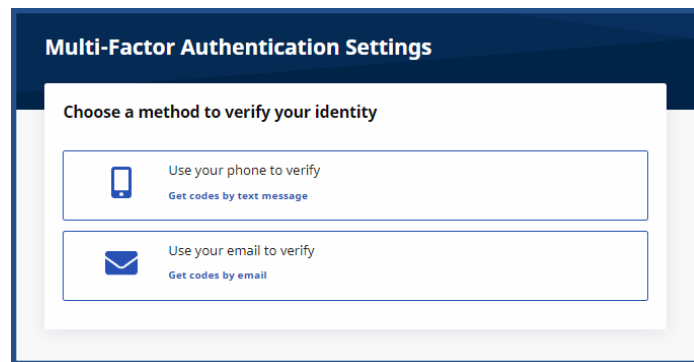
User Setup of MFA

Once the MFA setup is complete, a first-time Setup Request page opens when the Username and Password are entered. Click the **Set Up Now** button to continue.



MFA Setup Request page

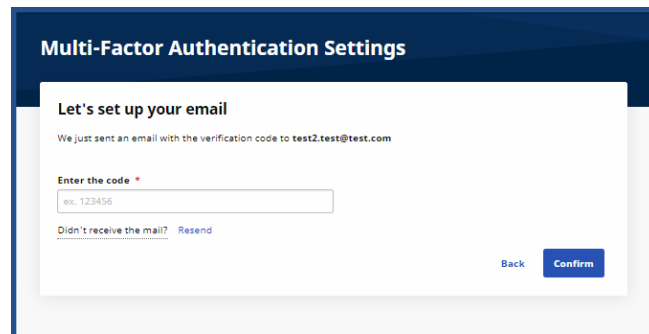
Select the method to verify your identity: via Text or Email, as seen in the following image.



Choose a Verification Method

If the **Use your email to verify** is selected, then the system sends a unique six-digit code by email to the email address on the HHAX User Profile. This code is valid for 30 minutes from the time of issue. If a new code is needed, click the **Resend** link to receive a new code after 60 seconds.

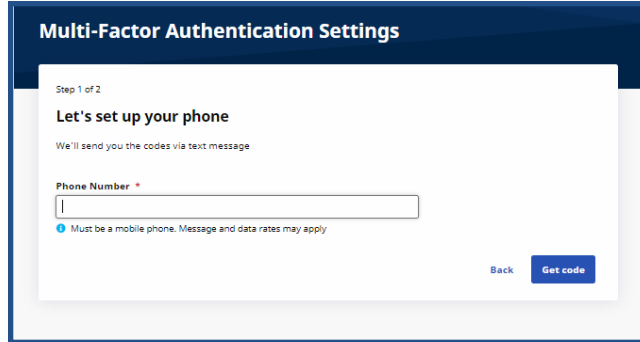
On the *Let's set up your email* page enter the 6-digit code and click **Confirm** to log in and access the system home page.



Email Setup

Note: Reauthentication is required every 30 days as well as when the browser is changed or the cache is cleared. A random and unique MFA code is sent to log into the system accordingly.

If the **Use your phone to verify** is selected, then the *Let's set up your phone* page opens. Enter the mobile phone number with area code in the **Phone Number** field and click **Get code**.

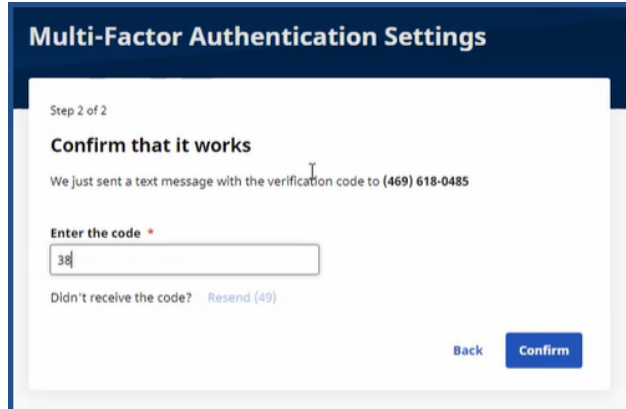


The screenshot shows a web interface titled "Multi-Factor Authentication Settings". It is "Step 1 of 2" and the heading is "Let's set up your phone". Below the heading, it says "We'll send you the codes via text message". There is a "Phone Number" input field with a red asterisk. Below the field is a blue note: "Must be a mobile phone. Message and data rates may apply". At the bottom right, there are "Back" and "Get code" buttons.

Phone Number Setup – Step 1

The system sends a unique six-digit code to the mobile phone number entered. This code is valid for 30 minutes from the time of issue. On the *Confirm that it works* page, enter the 6-digit code and click **Confirm** to log in and access the system home page.

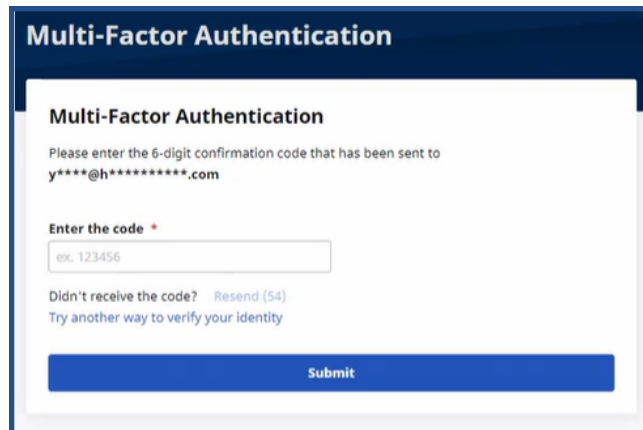
If a new code is needed, click the **Resend** link to receive a new code after 60 seconds.



The screenshot shows a web interface titled "Multi-Factor Authentication Settings". It is "Step 2 of 2" and the heading is "Confirm that it works". Below the heading, it says "We just sent a text message with the verification code to (469) 618-0485". There is an "Enter the code" input field with a red asterisk, containing the number "38". Below the field is a link: "Didn't receive the code? Resend (49)". At the bottom right, there are "Back" and "Confirm" buttons.

Phone Number Setup – Step 2

Note: Reauthentication is required every 30 days. A random and unique MFA code is sent to log into the system accordingly.



MFA Request Page

Changing User MFA Settings

Users subject to MFA can view and change their own MFA settings from within the Enterprise Portal.

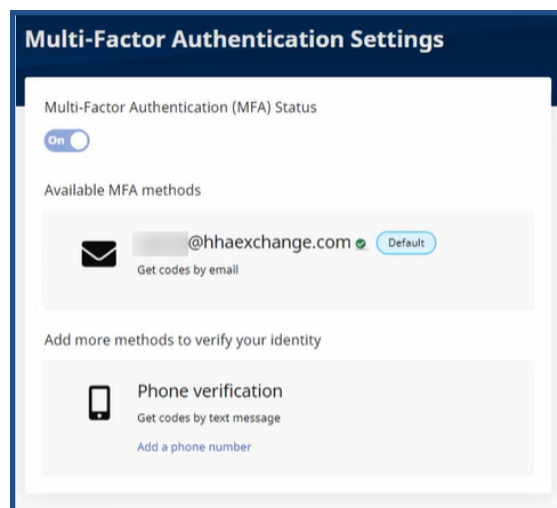
To change the MFA settings, click on the [MFA Settings](#) link (next to the [Support Center](#) link at top right) as seen in the following image. This link is only available to users who are subject to MFA.



MFA Settings Link Next to Support Center

Note: Users cannot disable Multi-Factor Authentication or change the email address from the MFA Settings page. When the email address is changed in the HHAX User Profile, the system prompts the user to set up MFA again on their next login.

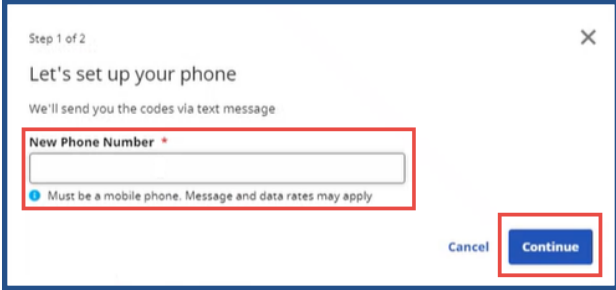
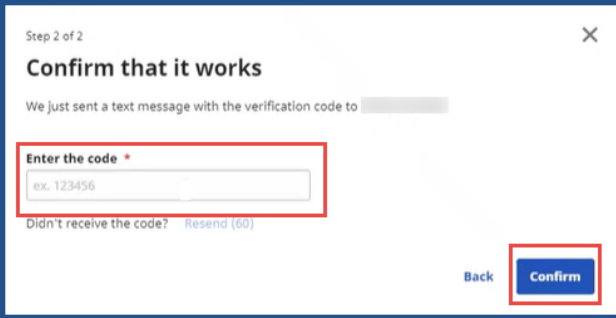
The Multi-Factor Authentication Setting page opens, as seen in the following image. Changes can be made to the MFA Settings as explained in the instructions under the image.



MFA Settings Page

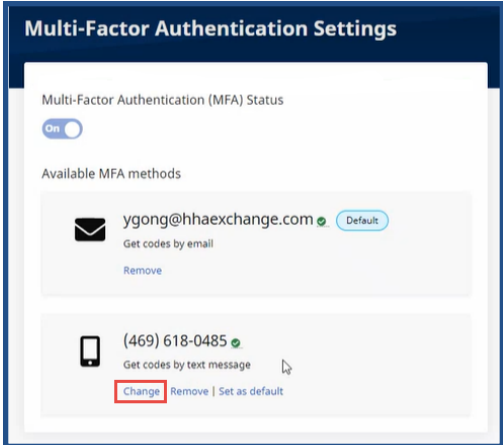

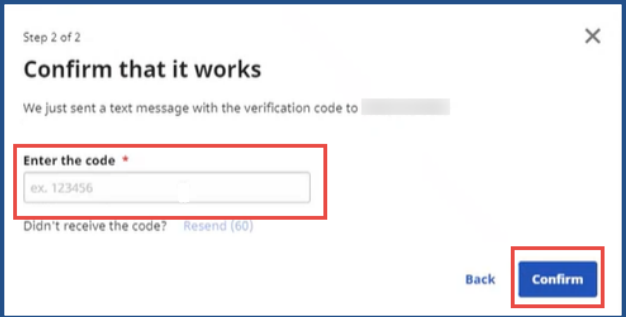
Adding a Mobile Phone Number

Complete the following steps to add a mobile phone number, when one has not been established.

Step	Action
1	Click on the Add a phone number link in the mobile phone section of <i>Available MFA methods</i> .
2	<p>Enter the phone number including area code in the New Phone Number field. Click Continue.</p>  <p style="text-align: center;">Phone Number Setup – Step 1</p>
3	<p>In the Enter the code field, type in the code sent to the mobile phone. Click Confirm to finalize.</p>  <p style="text-align: center;">Phone Number Setup – Step 2</p>



Change a Mobile Phone Number

Complete the following steps to change a mobile phone number.

Step	Action
1	<p>Click on the Change link in the mobile phone section of <i>Available MFA methods</i>.</p>  <p style="text-align: center;">MFA Settings Page</p>
2	<p>Enter the New Phone Number, and then click Continue.</p>  <p style="text-align: center;">Phone Number Change – Step 1</p>
3	<p>In the Enter the code field, type in the code sent to the mobile phone. Click Confirm to finalize.</p>  <p style="text-align: center;">Phone Number Change – Step 2</p>



Remove a Mobile Phone Number or Email Address

Complete the following steps to remove a mobile phone number or email address from available MFA methods.

Step	Action
1	<p>Click on the Remove link from either the email address or mobile phone section of <i>Available MFA methods</i>.</p> <div data-bbox="592 552 1105 1003" style="border: 1px solid #0056b3; padding: 10px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; margin: 0;">Multi-Factor Authentication Settings</p> <p>Multi-Factor Authentication (MFA) Status <input checked="" type="checkbox"/> On</p> <p>Available MFA methods</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p> ygong@hhaexchange.com Default</p> <p>Get codes by email</p> <p style="text-align: right;">Remove</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p> (469) 618-0485 Set as default</p> <p>Get codes by text message</p> <p style="text-align: right;">Change Remove</p> </div> </div> <p style="text-align: center; margin: 10px 0;">MFA Settings Page</p> <p><i>Note: Only one method can be removed; either the email or mobile phone, not both.</i></p>
2	<p>Click on the Remove button when prompted to confirm the removal.</p> <div data-bbox="586 1167 1114 1444" style="border: 1px solid #0056b3; padding: 10px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; margin: 0;">Confirm Removal ✕</p> <p>Please confirm you want to remove the MFA method: (123) 456-7890 - Text Message</p> <p style="text-align: right; margin-top: 10px;"> Cancel Remove </p> </div> <p style="text-align: center; margin: 10px 0;">Removal Confirmation</p>

Change Default MFA Method

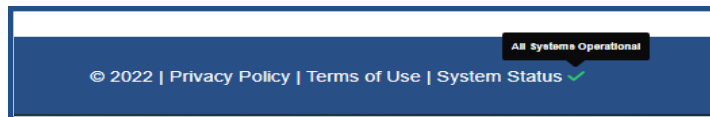
Complete the following steps to change the default MFA method.

Step	Action
1	<p>Click on the Set as default link in the email address or mobile phone section of <i>Available MFA methods</i>.</p> <div data-bbox="586 531 1105 991" style="border: 1px solid #004a87; padding: 10px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; margin: 0;">Multi-Factor Authentication Settings</p> <p>Multi-Factor Authentication (MFA) Status <input checked="" type="checkbox"/> On</p> <p>Available MFA methods</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p> ygong@hhaexchange.com Default</p> <p>Get codes by email</p> <p style="text-align: center;">Remove</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p> (469) 618-0485 🔒</p> <p>Get codes by text message</p> <p style="text-align: center;">Change Remove Set as default</p> </div> </div> <p style="text-align: center; margin-top: 5px;">MFA Settings Page</p>
2	<p>A banner at the top of the MFA Settings page indicates that the default setting has been changed.</p>

System Status Link




At the bottom of the Login page, a **System Status** page link readily indicates the status (health) of the various HHAX system functionalities. This is particularly helpful for users to gauge when systems slowness is reported/detected or when system access is down.

An icon displayed next to the System Status link indicates the system status, as seen in the following image. Hover over the icon for a brief definition of the status or click **System Status** for complete details.

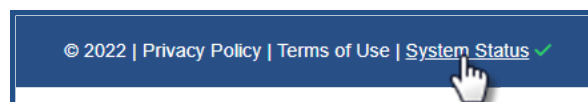


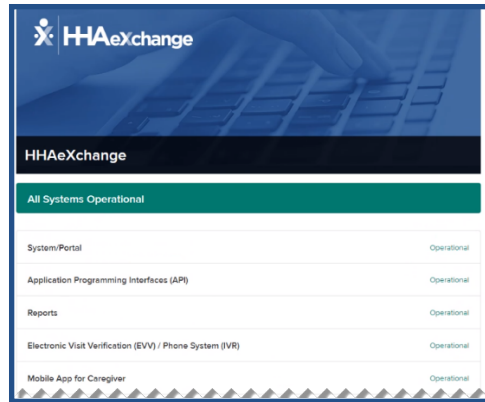
System Status Icon

The following table provides definitions for the various System Status icons.

Status	Icon
Operational	
Minor	
Major	
Critical	
Maintenance	

Click on the **System Status** link (as seen in the following image) to open the *System Status* page (as illustrated in the second image below).





System Status Page

The Navigation Panel

The **Navigation Panel** allows users to navigate between the different sections, or **Modules**, within the system (as illustrated below).



The Navigation Panel

The full navigation panel contains eight modules which are all permission based according to assigned User role; meaning, Providers can assign access to users in specific modules. For example, a Collections employee handling invoicing Visits may not need access to the **Admin** modules; therefore, the permission to access Admin functions may be deactivated.

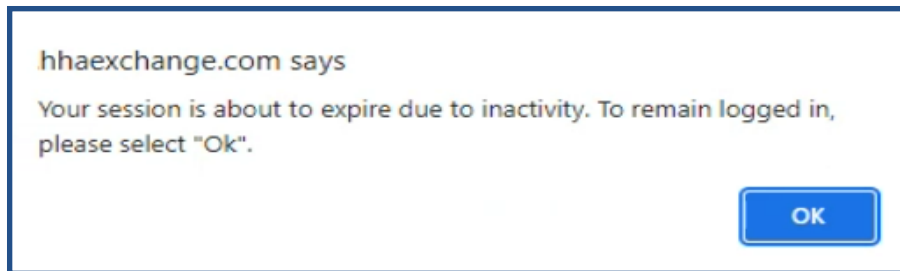
The following table offers a high-level summary of the actions available through each module.

Module	Description
Home	Home page where users can access internal communication tools. <ul style="list-style-type: none"> The Link Communications tab is used primarily by Providers who service Linked Contract Patients. Refer to the Communications category for details. The Notifications tab is a communications hub used to handle communications from HHAeXchange, between internal employees, and all active Caregivers. Refer to the Notifications Tab Job Aid for details.
Patient	Allows users to manage Patients and schedule visits.
Caregiver	Allows users to create and manage Caregivers, as well as assign them to visits.
Visit	Users can search for scheduled visits and manage visits.
Action	Contains an assortment of functions such as searching for Availability, Pending Placements, Payroll, Payer Communications, and many other features.
Billing	Allows users to handle all aspects of the billing process.
Report	Allows Providers to run reports based on specified filters and compile specific information into documents that may be saved outside of the software.
Admin	Allows users to manage key components of the system such as Role Permissions, among many others.

15-Minute System Session Timeout

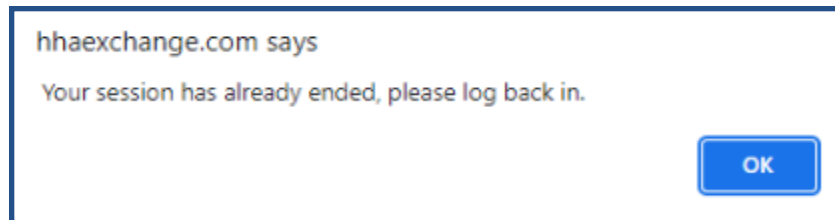
The session timeout functionality logs off users who are idle after 15 minutes of inactivity. At the 14-minute mark, the system issues a warning popup alerting the user that the session is about to expire, as seen in the following image.

Click on the **OK** button to continue in the session.



Session Expiration Alert

If left idle past the 15-minute threshold, then the following popup appears, prompting the user to click **OK** and route back to the *Login* page.



Session Expired

Note: System batch functionality (such as generating Invoice or Payroll Batches or Reports, which generate jobs that run in a background processor) continue to process and is not affected if a user's session times out after 15 minutes.