CHANGE HEALTHCARE

Insight. Innovation. Transformation.

Assurance Reimbursement Management™

Customer Release Notes

Last updated: August 25, 2023

Summary of Features and Enhancements

Assurance 8.7.2 | October 2023

Contents

What's New in Assurance 8.7.2? 3
Migration to CIAM 4
Assurance User Master Changes 4
Enforcement Activation 4
Paper Commands 6
Additional Updates 7

© 2023 Change Healthcare Operations LLC. All rights reserved.

This material contains confidential, proprietary information. Unauthorized use or disclosure of the information is strictly prohibited.

What's New in Assurance 8.7.2?

The Assurance 8.7.2 release contains information to help customers complete their **migration to Customer Identity Access Management (CIAM)** and understand new access to **paper commands**, as well as some additional updates. Use these release notes to find out more about these updates.

Migration to CIAM

All Assurance users will be required to access Assurance using CIAM credentials by the end of 2023.

The Assurance 8.7.2 release includes updates to automate the linking of users when enforcement of CIAM credentials is activated for your facility.

Paper Commands

Paper commands functionality is now available in Google Chrome™ (Chrome) and Microsoft Edge™ (Edge). Accessing paper commands functionality has been streamlined.

The red box indicates required customer action.

The Change Healthcare delta sign indicates a related customer service order number (SO#: ZZZZZZZZZZ) or subtopic. It is available for easier reference to proactively notify customers.

© 2023 Change Healthcare Operations LLC. All rights reserved.

This material contains confidential, proprietary information. Unauthorized use or disclosure of the information is strictly prohibited.

Migration to CIAM

All Assurance users will be required to access Assurance using CIAM by the end of 2023.

The Assurance 8.7.2 release includes updates to automate the linking of users when the enforcement to use CIAM credentials is activated for the users at your facility.

Activation of CIAM enforcement will occur in **phases beginning in October 2023.**

- **Users will be notified** of their specific enforcement activation date **prior to activation.**

You do not need to wait for the activation of CIAM enforcement.

- **You can migrate users to CIAM before enforcement** by linking them to CIAM in the Assurance user master (Maintenance > Master Setup > User).

After being linked to CIAM, users will access Assurance with the **Customer Identity Access Management (CIAM)** hyperlink on the login page:



Assurance User Master Changes

After CIAM enforcement, administrators will no longer be able to unlink users from CIAM. However, administrators can disable users who are linked to CIAM.

Enforcement Activation

After enforcement is activated, any user that enters their legacy credentials on the login page will be prompted to either validate or confirm their email address.

- **Users with validated email addresses** who have set up their CIAM passwords will be logged in to Assurance.
  - Users who have access to and are linked to a single CID will be taken directly to their landing page.
  - Users who have access to and are linked to multiple CIDs will see a Client Selection popup, for selection of the desired CID for access.

© 2023 Change Healthcare Operations LLC. All rights reserved.

This material contains confidential, proprietary information. Unauthorized use or disclosure of the information is strictly prohibited.

- **Users without validated email addresses** or those who have not set up their CIAM passwords will see a page asking them to confirm or enter their email address.
  1. If there is no email address for a user in the Assurance user master, the user will be prompted to enter their email address for validation then enter the One Time Passcode received via email before proceeding.
  2. If there is an email address for a user in the Assurance user master, the user will be asked to confirm that the email is correct or modify the email address if needed.
     - If the user changes the email address, they will be required to validate the new email address before proceeding.
  3. Validated email addresses will automatically be added to the Assurance user master and the user will be automatically linked to CIAM.
  4. When linking to CIAM for the first time, a user will receive a CIAM Welcome email with a link to set up their CIAM password. The Welcome email is valid for 72 hours.
  5. The first time a user logs in with CIAM, they will be prompted to download and install PingID for multifactor authentication (MFA).
  6. When the process for installation and authentication is complete, users will access Assurance with the **Customer Identity Access Management (CIAM)** hyperlink on the login page.

Assurance users need to validate or enter their addresses and set up their passwords for using CIAM.

Notes

- **Legacy Log In:** If a user enters their legacy credentials to log in to Assurance after linking to CIAM, they will receive a message on the login page that they now need to use the **Customer Identity Access Management (CIAM)** hyperlink.
- **PingID:** If users are not prompted to install PingID when they initially log in, they should expect an email notification soon after that will specify a date for MFA activation using PingID. Users will be prompted to install PingID on the date indicated in the email notification.
- **Turnkeys:** Customers that have Assurance installed at their own facilities (i.e., Turnkey customers) are not required to migrate to CIAM for Assurance access.

© 2023 Change Healthcare Operations LLC. All rights reserved.

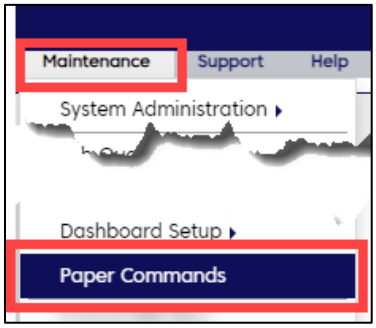
This material contains confidential, proprietary information. Unauthorized use or disclosure of the information is strictly prohibited.

Paper Commands

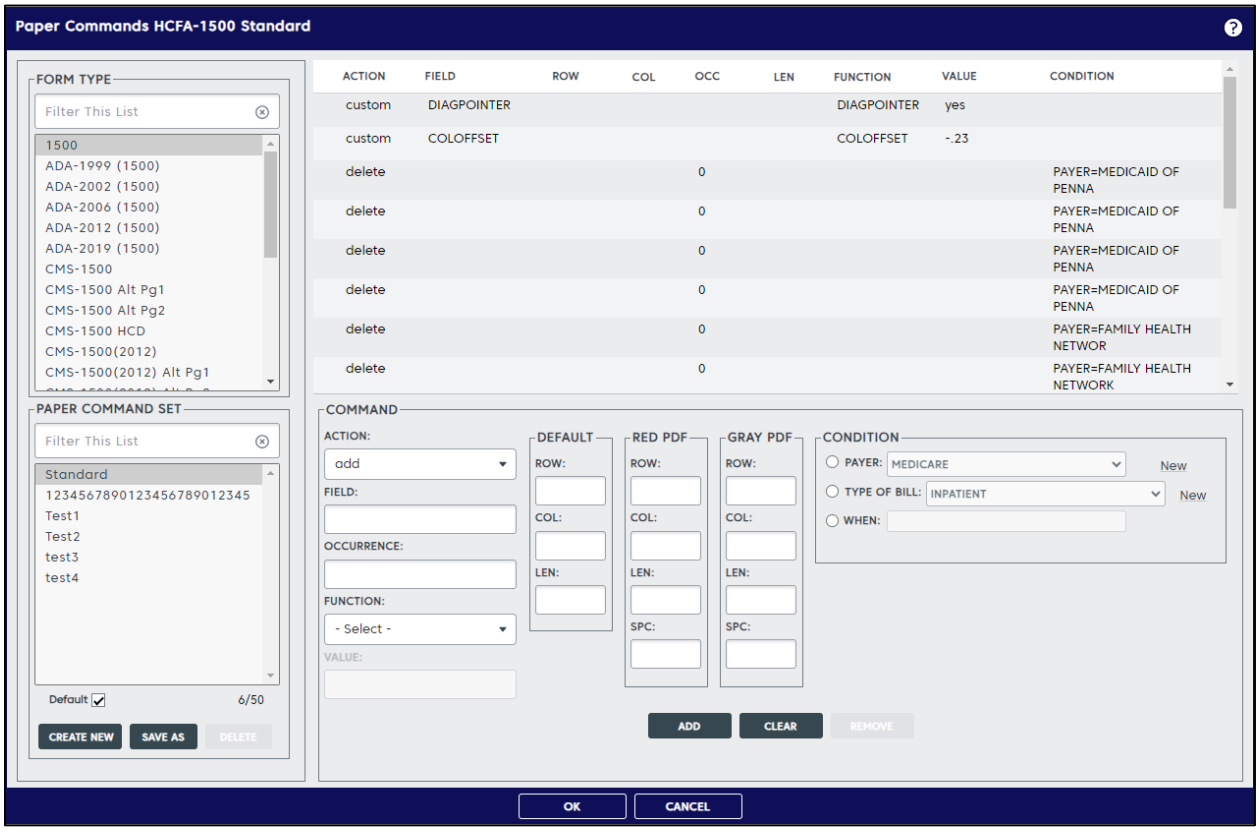
The Paper Commands page is now available in Chrome and no longer requires Edge sites.xml setup.

Paper commands access has been streamlined; however, **paper commands functionality remains the same**.

The Paper Commands menu option is now a single selection off the Maintenance menu:



Paper commands are now set up so that users can **select the form type** and **update/ create paper command sets** all from a single Paper Commands page!



© 2023 Change Healthcare Operations LLC. All rights reserved.

This material contains confidential, proprietary information. Unauthorized use or disclosure of the information is strictly prohibited.

Additional Updates

SO#	Resolution
n/a	Users can configure how and when to receive dashboard notifications when Assurance has encountered a failure to save: • To configure this notification in Dashboard Maintenance, select "Claim Discard - System SAV" in Event Thresholds. • The notification will contain the affected bridge filename.
8005312088	The Changes tab in CFI has been corrected so that clicking the DATE column header will return the FIELD NAMES to the default sort order of A-Z.
8005330692, 8005402956	Eligibility Payer Profile Maintenance has been updated so that payers can be added to the ENABLED PAYERS panel on the right for a client with no Payer Aliases.
8005405513	Assurance has been updated to improve the login experience when users log in to Assurance after a session timeout.
n/a	Remit removal SQL agent job has been updated to do the following: • reduce failures by checking the list contents before making additions. • queue the items with the oldest import date to be removed first.
8005404101	The release job and send/receive mail processes have been adjusted to allow time to receive large mail files.
n/a	Assurance has been updated so that the Set Up FTPS Agent page now loads correctly.
8005380675	Set Up Agent functionality has been updated so that newly added Auto Submit schedules save as expected.
8005320305, 8005414087	Medicare Direct Entry (MDE) has been updated so that all provider IDs associated with an account appear on the Direct Entry Accounts page when the Shared function is used across linked CIDs.

© 2023 Change Healthcare Operations LLC. All rights reserved.

This material contains confidential, proprietary information. Unauthorized use or disclosure of the information is strictly prohibited.