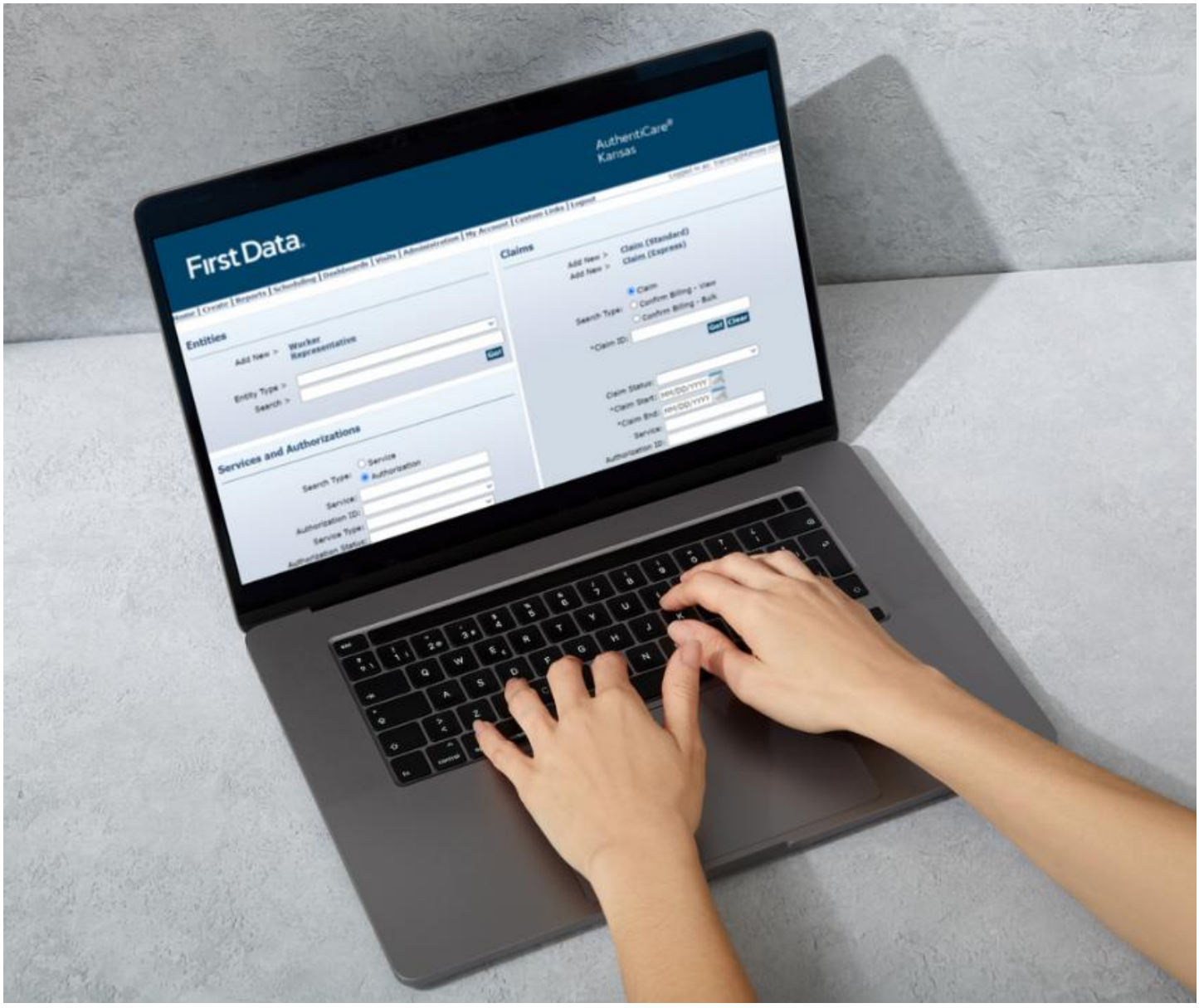

Functionality Differences

AuthentiCare® 2.0 and 3.0

Last Updated: 3/16/2026

Welcome to AuthentiCare 3.0!

1.0 Overview of Functional Differences

AuthentiCare 3.0 represents the next evolution of the AuthentiCare mobile application. While the overall caregiver experience remains familiar, the underlying technology and security model have been modernized to improve long-term stability and consistency across mobile platforms.

Platform Architecture and Technology
AuthentiCare 3.0 was rebuilt using .NET MAUI (Multi-platform App UI), a modern framework that allows a single, unified codebase to support both Android and iOS devices.

By moving to .NET MAUI, AuthentiCare 3.0 delivers several important advantages:

- **Improved Security Consistency**
  A single codebase ensures that security logic, authentication workflows, and protections are applied identically across Android and iOS, eliminating platform-specific discrepancies.

- **Greater Code Stability and Quality**
  Maintaining one shared codebase reduces complexity, lowers the risk of platform-specific defects, and improves overall application reliability.

- **Faster Enhancements and Fixes**
  Updates, bug fixes, and security improvements can be developed and deployed more efficiently, benefiting all users regardless of device type.

- **Consistent Cross-Platform Behavior**
  Caregivers receive the same experience and functionality whether they use Android or iOS, reducing variability and support challenges.

This architectural change is invisible to end users but provides meaningful long-term benefits for agencies and caregivers alike.

User Interface and Experience
From a user interface (UI) and user experience (UX) perspective, AuthentiCare 3.0 remains intentionally familiar. The login experience is nearly identical, check-in and check-out workflows are unchanged, and day-to-day usage mirrors AuthentiCare 2.0. Caregivers transitioning to 3.0 should experience minimal disruption and little to no retraining.

1.1 Key Change #1 - Device ID Registration

One of the most significant changes between AuthentiCare 2.0 and 3.0 relates to Device ID handling.

1.1.1 AuthentiCare 2.0 Device ID Process

Currently, when a caregiver begins using the AuthentiCare 2.0 mobile application:

- They must contact their employer (via phone or email) to provide their Device ID
- The Device ID is a unique identifier tied to each phone or tablet
- Device ID is a required component of multi-factor authentication

To successfully establish a session:

- Worker ID and password must be valid
- Device ID must match what is stored in the worker's profile

If the Worker ID and password are correct but the Device ID does not match, the login is denied.

1.1.2 Device ID Changes in AuthentiCare 3.0

AuthentiCare 3.0 calculates the Device ID string differently than AuthentiCare 2.0. As a result, all existing caregivers will need to register a new Device ID the first time they log into AuthentiCare 3.0.

This process is enabled at the SysAdmin level in AuthentiCare, and can be turned off any time per the State's request.

First-Time Login Experience in AuthentiCare 3.0

Once AuthentiCare 3.0 is available in the app stores, the first-time login flow is as follows:

- After downloading the app, caregivers are prompted to enter a Mobile Setup Code (this process is identical in AuthentiCare 2.0 and 3.0)
- For the State of New Mexico, the code is: NMCCPRD
- The caregiver enters their Worker ID and password, as they do today
- If the credentials are valid, the system detects that a new Device ID is being used

A popup message appears:

"New Device ID detected. Please click 'Continue' to receive a PIN via email to continue using AuthentiCare." The options are Cancel and Continue.

- After selecting Continue, AuthentiCare sends an email with the subject line: **"Your AuthentiCare Mobile App DeviceID reset request"**
- The email is sent from DoNotReply@firstdata.com

- The email contains a six-digit code, displayed in red font, and is valid for 30 minutes

- The caregiver enters the six-digit code into the app
- This action writes the new Device ID to the worker profile
- Future logins proceed normally without repeating this process

- A second email is sent confirming that the Device ID was successfully changed

Important Email Requirement

It is critical that caregivers have a unique, accessible email address on their worker profile.

If a caregiver does not have an email address, or if the email address is a shared or provider agency email, they will not be able to complete the Device ID registration process themselves.

In These Cases, the caregiver must follow the existing process used in AuthentiCare 2.0: they must contact their employer, share the new Device ID displayed in AuthentiCare 3.0, and an authorized user must manually enter the Device ID through the web portal.

Password Reset Reminder

As with AuthentiCare 2.0, a valid email address is required for caregivers to reset their own mobile passwords.

Access Between Versions

Once a caregiver successfully logs into AuthentiCare 3.0, their access to AuthentiCare 2.0 is revoked. Fiserv is developing internal guidance for edge scenarios where a caregiver may need to temporarily return to AuthentiCare 2.0 after logging into 3.0.

Summary

The move from AuthentiCare 2.0 to 3.0 introduces meaningful improvements in platform consistency and security, while preserving the caregiver experience users rely on today. The primary functional change is the Device ID registration process.

1.2 Key Change #2 - Client Lookup Enhancements

Another key difference between AuthentiCare 2.0 and AuthentiCare 3.0 is the way caregivers can search for clients within the mobile application.

1.2.1 Client Lookup in AuthentiCare 2.0

In AuthentiCare 2.0, when a caregiver uses the **Client Lookup** feature, they must enter either:

- The Client ID, or
- The client's full last name

For example, if a caregiver is searching for a client with the last name **"Gonzalez"**, the entire last name must be entered in order for the client record to appear. Partial last name searches are not supported.

1.2.2 Client Lookup in AuthentiCare 3.0

AuthentiCare 3.0 introduces a more flexible client search experience. Caregivers may continue to search by Client ID or full last name, exactly as they do today. In addition, partial last name searches are now supported.

For example, to locate a client with the last name **"Gonzalez"**, the caregiver may enter:

- "Gon"
- "Gonz"
- "Gonza"
- Or any other partial last name entry, provided it is the first letters of the last name.

1.2.3 Important Note

AuthentiCare 2.0 and 3.0 continue to enforce the same security and data-access rules. Caregivers can only search for and view clients associated with their specific provider agency. The expanded search capability does not expose additional clients or cross-agency data.