GinnieMae
Our Guaranty Matters

Modernization Bulletin

8/13/2026
No. 85

This publication will be used periodically to provide notifications and information about Ginnie Mae Modernization efforts. This is not a device to implement official policy changes to Ginnie Mae's Mortgage-Backed Securities (MBS) programs. If you have any comments or suggestions on how to make this publication more informative and helpful, please contact askGinnieMae@hud.gov.

Upcoming Changes to Authentication Experience for All MyGinnieMae Portal Users

Ginnie Mae is enhancing the security of the MyGinnieMae portal by introducing a new **Okta-hosted sign-in experience with phishing-resistant multi-factor authentication (MFA).** This enhancement will strengthen protection against credential-based cyber threats, support federal Zero Trust security requirements, and provide a more secure, modern sign-in experience for **all MyGinnieMae users.**

The transition will occur in two phases to allow users time to adopt the new experience before it becomes required.

What to Expect

Early Adoption Phase	During the Okta Early Adoption phase, **August 31 to September 25, 2026**, users may voluntarily begin using the new Okta sign-in experience by completing their MFA setup through a designated early adoption link for MyGinnieMae. This phase will provide an opportunity for users to become familiar with the new process and prepare for the transition before it is required. Users will continue to use their existing MyGinnieMae username and password and follow the on-screen instructions to set up Okta MFA; after successful authentication, they will be directed to their MyGinnieMae dashboard. Listening Sessions will occur weekly during this phase for users to share feedback about their experience or ask questions. Users may continue accessing MyGinnieMae as they do today through the existing portal link.
Go-Live and Required Transition Phase	Beginning **September 28, 2026**, all users will be required to sign in with an Okta MFA method to access MyGinnieMae. Upon go-live, the legacy authentication methods (email One-Time PIN (OTP) and Oracle Mobile Authenticator (OMA) application) will be decommissioned and replaced by Okta authentication.
First-Time Sign-In Setup	At first sign-in (either during the Okta Early Adoption phase using the designated early adoption link or upon go-live using the existing portal link), users will be guided through on-screen instructions to set up a required phishing-resistant MFA method supported through Okta. After completing the required first-time setup, users will be able to manage their own authentication methods through their

	MyGinnieMae security settings. Organization Administrators will also be able to reset authenticators on behalf of their users.
Passkeys (Primary MFA Method)	Passkeys will be the recommended primary authentication method. Users will set up a passkey on their device using existing built-in device security capabilities, such as biometrics, Windows Hello, Touch ID, or a device PIN, providing a more secure sign-in experience.
Okta Verify (Secondary MFA Method)	Okta Verify will be the secondary or backup authentication method when passkeys cannot be used. Users will install and enroll in the Okta Verify application on their device to authenticate using push notification, one-time verification code, or biometrics.

As Ginnie Mae prepares users for the upcoming changes, updates will be posted on the Modernization Initiatives page on GinnieMae.Gov under the section **"New Okta Multi-Factor Authentication (MFA) for MyGinnieMae Portal".** A timeline and slide deck of Frequently Asked Questions (FAQs) has been posted. Additional information including new Quick Reference Cards (QRCs) and the early adoption link for MyGinnieMae will be made available to support users in the Okta Early Adoption phase. If you have any questions, please email askGinnieMae@hud.gov.