MyGinnieMae
Okta Implementation FAQs

June 2026

Ginnie Mae
Our Guaranty Matters

@GinnieMaeGov /GinnieMaeGov Ginnie Mae

Basics and Policy

1. **What is changing with login?**
   Starting in late-September, all MyGinnieMae users will see a new Okta-hosted login page and will be required to setup an Okta-based phishing resistant multi-factor authentication (MFA) method. Passkeys will become the primary MFA login method for MyGinnieMae users. Okta Verify will serve as a secondary method for users who cannot use a passkey.

2. **What is a passkey?**
   A passkey is a modern sign-in credential based on the FastIdentity Online 2 (FIDO2)/WebAuthentication standard. It allows users to login with a method built into a device, such as Face ID, a fingerprint, Windows Hello, a device PIN, or a physical security key, instead of entering a password.

3. **What is Okta Verify?**
   Okta Verify is an authentication app that helps confirm a user's identity when signing in, through time-based push notifications, one-time verification code, or biometric verification.

4. **Why the shift to passkeys and Okta Verify?**
   Passkeys and Okta Verify reduce the risk of phishing, stolen credentials, and unauthorized access. They are designed to be phishing-resistant, and they also create a faster, simpler login experience by reducing password resets and login frictions. This transition also supports federal Zero Trust requirements.

Basics and Policy, continued

5. **Are passkeys now the default login method?**
   Yes, passkeys will be the default and preferred login method. At first attempt using passkeys with Okta, users will be guided through the steps to support this new method.

6. **When would users use Okta Verify instead of a passkey?**
   Users would use Okta Verify when a passkey is unavailable or cannot be used. For example, users may need Okta Verify if they are on a new device where the passkey is not available, using a device that does not support passkeys, or needing a fallback authentication method. In some cases, users may only have the option to use Okta Verify based on organizational policy.

7. **Do users need both a passkey and Okta Verify set up?**
   For users who can use passkeys, the recommended approach is to set up both. The passkey should serve as the primary login method, and Okta Verify should be set up as a secondary or backup method. However, depending on organizational policy, some users may only be able to use Okta Verify.

8. **Will the Okta MFA changes affect my RSA SecurID Soft Token?**
   No. The Okta MFA changes will not affect your RSA SecurID Soft Token. These changes apply only to the login process for accessing MyGinnieMae and do not change how your RSA SecurID Soft Token functions.

Enrollment and Setup

1. **How do users set up a passkey?**
   Users will follow the on-screen prompts to enroll a passkey using a supported login method on their device, such as fingerprint, face scan, PIN, or physical security key. Ginnie Mae will provide setup instructions to guide users through the enrollment process.
2. **How do users enroll in Okta Verify?**
   Users must first install Okta Verify on their device and then complete the enrollment process within the application. Ginnie Mae will provide setup instructions to guide users through installation and enrollment.
3. **Can users set up more than one passkey?**
   Yes. Users can enroll more than one passkey. Some passkeys are tied to a specific device, such as Windows Hello, while others may sync across eligible devices through a passkey manager, such as Google Password Manager. Only one passkey is required.
4. **Can users register passkeys or Okta Verify on multiple Desktop PC/laptop devices or mobile devices?**
   Yes, both can be enabled on the same device concurrently and on multiple devices. The MFA method must be available and set up on the same device being used to log in (a mobile device cannot be used to complete authentication for MyGinnieMae on a desktop device).
5. **Where will training materials (Quick Reference Cards) be available?**
   Quick Reference Cards will be published on the Ginnie Mae website.

Enrollment and Setup, continued

6. **What devices or browsers support passkeys and Okta Verify?**
   Passkeys are supported on most modern devices, operating systems, and browsers that support FIDO2/WebAuthn. Okta Verify is supported on recent versions of Android, iOS, iPadOS, macOS, and Windows 10 and 11, and it works best with the latest versions of Chrome, Firefox, Safari, and Edge 1 2 3 4. Users should keep their app, browser, and device software up to date to ensure proper setup and login.

7. **When must users set up passkeys or Okta Verify?**
   All MyGinnieMae users must begin using passkeys or Okta Verify starting in late-September.

8. **What is the "test link," and when should users use it?**
   The test link is a designated Okta-hosted login link that users will use during the early adoption period to access MyGinnieMae and complete early setup of Okta MFA. Users who begin using the test link must continue using it to log in with their Okta MFA setup until go-live and the required transition date. At go-live in September 2026, the MyGinnieMae login page will support the full Okta integration, and the test link will redirect to or become the main login page.

9. **How does the test link differ from production?**
   The test link allows users to set up their Okta MFA method for MyGinnieMae access. During the early adoption period, the production environment will still support OMA and OTP for MFA, while the test link will continue to support Okta MFA only. After decommissioning, the production link will also require Okta MFA only.

Enrollment and Setup, continued

10. **Do users need to register for Okta in advance of go-live?**
    Users are strongly encouraged to complete their set up of Okta MFA for MyGinnieMae access during the early adoption period. Otherwise, users will be required to complete their set up at first login after the go-live and required transition date.

11. **What happens if users do not enroll before go-live?**
    Users will not be locked out or disabled if they do not enroll before go-live. Instead, they will be prompted to set up their Okta MFA method the next time they log in.

12. **Will there be a grace period?**
    The early adoption period can be considered the grace period. After that period ends and the legacy method is decommissioned, users will be required to set up Okta MFA to continue using MyGinnieMae.

Daily Login Experience

1. **Will existing MyGinnieMae usernames change?**
   No. Existing MyGinnieMae usernames remain the same. The change affects how users authenticate, not their accounts or roles
2. **How do users log in with a passkey?**
   Users log in with the passkey saved on their device and complete the prompt using a fingerprint, face scan, PIN, or security key.
3. **How do users log in with Okta Verify?**
   Users log in with Okta Verify by approving a time-based push notification or entering a time-based one-time verification code in the app to confirm their identify.
4. **What happens if the passkey does not work?**
   If a passkey does not work, users can follow the on-screen prompts to log in with an available backup authentication method, such as Okta Verify.
5. **Can users choose Okta Verify instead of a passkey during login?**
   Users may be able to choose Okta Verify instead of a passkey during login, depending on their organization's authentication policies, the authentication methods they have enrolled, and the login options available for their device or browser.

Daily Login Experience, continued

6. **Will the login experience look different on mobile versus desktop?**
   The login experience is similar on mobile and desktop, but the prompts and available options may look slightly different depending on the device, browser, and authentication method. Users can log in with a passkey or Okta Verify on either platform, although desktop is the recommended experience when available.
7. **Are users required to authenticate each time they log in, or only after a period of inactivity?**
   Users will need to authenticate every login and after 20 minutes of inactivity.

Device Changes and Recovery

1. **What if users get a new phone or laptop?**
   Users will need to set up their passkey and Okta Verify again on the new device being used to log in to MyGinnieMae.
2. **What if users lose the device that stores the passkey?**
   If users lose the device that stores their passkey, they should use a backup login method, such as Okta Verify, if available. Users should remove the old device by managing their authentication methods in their profile settings or by contacting their organization administrator. Users will need to set up their passkey on a new device.
3. **What happens if users no longer have access to Okta Verify?**
   If users no longer have access to Okta Verify, they should use a backup login method, such as a passkey, if available. Users can reset Okta Verify by re-enrolling the app on their device through their organization's approved setup process.
4. **How do users recover access if both methods are unavailable?**
   If both login methods are unavailable, users will need to contact their organization administrator to recover access.
5. **Whom should users contact if they are locked out?**
   Users who are locked out should contact their organization administrator to unlock their account.

Security and Privacy

1. **Are passkeys more secure than passwords?**
   Yes. Passkeys are generally more secure than passwords because they are phishing-resistant, tied to the website or app they were created for, and use public-key cryptography so the private key stays on the user's device and is not shared with the server.
2. **Is biometric data shared with Okta or with users' organizations?**
   No, users' biometric data stays on their device and is not shared with Okta, their organization, or MyGinnieMae.
3. **Are there any browser settings, security configurations, or network controls (e.g., firewalls) that may block Okta MFA use?**
   Yes. Some browser settings, security configurations, or network controls may prevent passkeys from working properly. Users may see prompts related to MFA enrollment or verification, and if those prompts are blocked or dismissed, login may not continue. Restrictive browser or security settings, privacy-focused browser extensions, unsupported embedded browsers, network restrictions, and certain enterprise security policies can interfere with MFA authentication. Please review your browser, device, and network security settings if you experience any issues.
4. **What should users do if their organization restricts Okta Verify or passkeys?**
   If your organization restricts Okta Verify or passkeys, contact your organization administrator or the Ginnie Mae Help Desk for assistance. They can help you understand available access options and the next steps for login. If Okta Verify or passkeys are restricted by organizational policy, the user's internal support team will need to advise on approved access options.

Special Situations

1. **What if users work on a shared device?**
   Users who work on a shared device may need to follow their organization's specific login process because passkey use can vary in shared-device environments.
2. **What if users' browser or operating system does not support passkeys?**
   If users' browsers or operating system does not support passkeys, users may need to log in with Okta Verify as their primary authentication method.
3. **I already use Okta for other applications. Do I still need to set up Okta MFA for MyGinnieMae?**
   Yes. Even if you already use Okta for other applications, you must still set up your Okta MFA method for MyGinnieMae access. MyGinnieMae uses a separate Okta tenant, so this requires a separate account and MFA enrollment specific to MyGinnieMae. In other words, your existing Okta account for another application will not be the same account used for MyGinnieMae.

Support and Administration

1. **How do users reset a passkey?**
   Users can reset a passkey by following their organization's passkey reset process and setting up a new passkey on their device.
2. **How do users reset Okta Verify?**
   Users can reset Okta Verify by re-enrolling the app on their device through their organization's approved setup process.
3. **How do users update or remove MFA methods for MyGinnieMae?**
   Users can update or remove old devices by managing their authentication methods in their profile settings or by contacting their organization administrator.
4. **Where can users get help with setup or login issues?**
   Users can contact their organization's IT help desk or Ginnie Mae Customer Support Help Desk for help with setup or login issues.
5. **What information should users provide to the help desk?**
   Users should provide their name, device type, the issue they are experiencing, and any relevant error message or screenshot.