

### General

**Q: What is changing?**

A: The process of logging into AIG applications will now require multi-factor authentication (MFA). This means that when you log in with your user login and password, you will also be required to verify the login through a secondary means of verification of your choosing (mobile application or SMS). This change will be rolled out to applications in a phased approach, so you may notice login interface updates in waves depending on the number of AIG applications you access.

**Q: Why is the login experience changing?**

A: AIG is integrating an updated authentication system into the login experience to enhance security for your online accounts.

**Q: Which MFA methods are available to me?**

A: The MFA options that are supported include mobile authenticator application (currently, Okta Verify) and SMS Authentication.

**Q: Can I use a different application for MFA other than Okta Verify?**

A: At this time, Okta Verify is the only supported authentication application. Alternatively, you may select to verify the authentication through SMS message.

**Q: What if I don't have a smart phone (e.g., I have a flip phone)?**

A: There are other MFA options available such as SMS Authentication that can be used without a smart phone.

**Q: Where can I download the mobile authenticator applications (Okta Verify)?**

A: You may download the mobile authenticator application from the App Store (Apple) or Google Play Store (Android). If you choose to use the Okta mobile authenticator, make sure to download Okta Verify (not Okta Mobile).

**Q: Do I need to download and install an app for MFA?**

A: An additional software download is only necessary if you choose to verify through OKTA Verify. Alternatively, you may also choose to verify via SMS Authentication, which do not require an app installation.

**Q: Will I need to authenticate more than once if I use multiple AIG applications?**

A: There is no need to reauthenticate if you are accessing other applications that use the same MFA method. Once you have authenticated, you can access all of your applications.

**Q: Will the MFA process change when my password expires?**

A: No. The MFA method will not change if the password expires or is reset.

**Q: Will the application timeout process be different?**

A: The application timeout will stay the same; however, you will need to reauthenticate the login using the MFA when you log back in.

### Application Specific Information

**Q: What is Okta?**

A: **Okta CIAM** is a third-party solution used by AIG for user authentication to access various AIG systems and applications.

**Okta Verify** is an MFA application provided by Okta to provide a second factor to log in and establish stronger assurance for your account protection.

**Q: What personal information does Okta collect?**

A: In order to authenticate a user's identity, AIG utilizes the Okta CIAM solution collects and stores users' name, email address, phone number, unique phone identifiers, and IP addresses. This information is stored in an Okta CIAM cloud environment as long as a user will need access to an application and will need to be authenticated for access. This allows users who log into multiple AIG applications to only need to authenticate their login once for all applications during a session. For information about AIG's privacy practices, visit <https://www.aig.com/privacy-policy>.

Okta Verify is separate application managed by Okta that provides codes that can be used as a second authentication factor to log into other services.

**Q: What personal information is required for Okta Verify?**

A: Okta Verify may collect personal information as part of the verification process. AIG does not have access to personal information collected by Okta Verify. For more information about Okta's Privacy Policy, see <https://www.okta.com/privacy-policy/>.

**Q: Can I download and activate Okta Verify on more than one device?**

A: At present, Okta Verify can be activated only on one device.

**Q: Does Okta Verify use mobile data or require extra storage?**

A: Okta Verify uses minimal data – to the order of a few bytes. It does not require any extra storage.

**Q: What personal information is collected if I use SMS authentication?**

A: If you choose to use SMS, no personal information will be collected by an authentication application, but limited personal information will be collected through the Okta CIAM solution to authenticate your identity, including name, email address, phone number, unique phone identifiers, and IP address.