Multi-factor Authentication

Frequently Asked Questions

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, SMS, or phone call). 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 Google Authenticator), Desktop Authentication, SMS Authentication, or Voice Call Authentication.

Q: Which MFA option does AIG recommend?

A: The MFA options that are supported via the Okta CIAM solution used by AIG include mobile authenticator application (currently, Okta Verify and Google Authenticator), desktop authentication, SMS Authentication, or Voice Call Authentication. AIG does not make recommendations regarding any authentication method, and users may select any of the supported methods that fit your needs. Please note that best practice for a secure connection is to use an authentication application rather than SMS or Voice Call Authentication. For more information regarding MFA best practices, click here.

Q: Can I use a different application for MFA other than Okta Verify or Google Authenticator?

A: At this time, Okta Verify and Google Authenticator are the two supported mobile authentication applications. Alternatively, you may select to verify the authentication through Desktop Authentication, SMS message or Voice Call authentication.

Q: Where can I download the mobile authenticator applications (Okta Verify, Google Authenticator)?

A: You may download either of the mobile authenticator applications 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: What if I don't have a smart phone (e.g., I have a flip phone)?

A: There are other MFA options available including SMS Authentication, Voice Call Authentication or Desktop Authentication that can be used without a smart phone.

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 either OKTA Verify or Google Authenticator. Alternatively, you may also choose to verify via SMS Authentication or Voice Call Authentication, which do not require an app installation.

Q: **Do I need to download and install software for Desktop MFA?**

A: An additional software is not necessary for Desktop Authentication. Google Authenticator for desktop is only available for the Chrome Browser as an extension button,

Q: How will I log in if my cell phone isn't working or is unavailable?

A: You will need to use an MFA to verify your login each time. Contact the appropriate Help Desk to reset the MFA method.

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. For more information about Okta Verify.

Multi-factor Authentication

Frequently Asked Questions

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: What is Google Authenticator?

A: Google Authenticator is an application managed by Google that provides codes that can be used as a second authentication factor to log into other services. If you set up 2-Step Verification, you can use the Google Authenticator app to receive codes. You can still receive codes without internet connection or mobile service.

Q: What personal information does Google Authenticator collect?

A: Google Authenticator may collect personal information as part of the verification process. AIG does not have access to personal information collected by Google Authenticator. For more information about Google's Privacy Policy, see https://policies.google.com/privacy.

Q: Can I download and activate Okta Verify or Google Authenticator on more than one device?

A: At present, Okta Verify can be activated only on one device. Google Authenticator may be used on multiple devices. The Google Authenticator app must be downloaded on all devices you want to use.

Q: Does Okta Verify or Google Authenticator 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. Google Authenticator does not require any internet or mobile connection and does not require extra storage.

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

A: If you choose to use SMS or voice authentication, 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.