

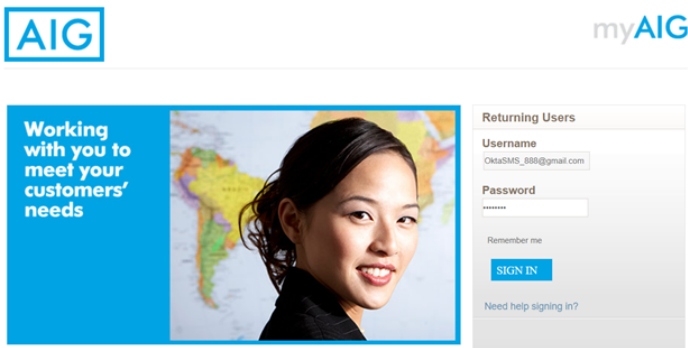
Overview

The process of logging into some AIG applications will now require a Multi-factor Authentication (MFA). This means that each time a user logs in, the login is required to be verified through a secondary means of verification (mobile application or SMS). **Note:** The screens featured throughout this guide reflect the standard design, but the look and feel may vary slightly depending on the application.

For Okta Verify:

To log into AIG applications using MFA:

1. Access the application's sign-on page.
2. Enter the **Username**
3. Enter the **Password**
4. Click the **Sign In** button. The **MFA** screen appears.



5. Click the **Send Push** button. A verification notification will pop up on the mobile device previously set up.

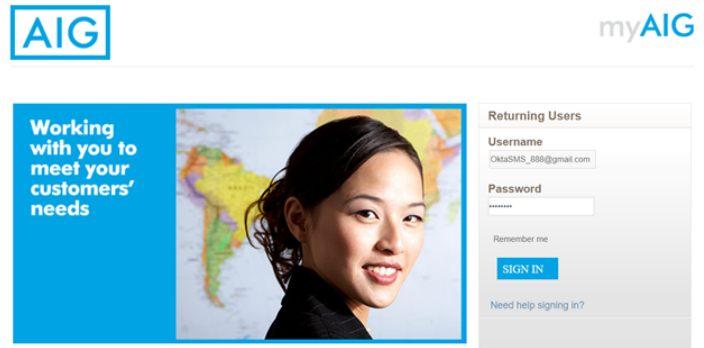


6. Click the **Yes, it's me** button on the mobile device notification. You are redirected to the application landing page.

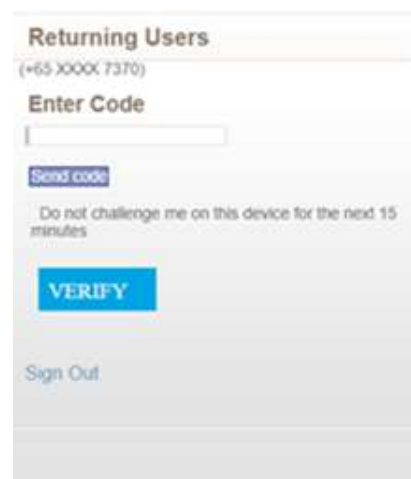
For SMS Authentication

To log into AIG applications using MFA:

1. Access the application's sign-on page.
2. Enter the **Username**
3. Enter the **Password**
4. Click the **Sign In** button. The **MFA** screen appears.



5. Click the **Send Code** button for SMS Authentication. A numeric code will be sent to your mobile device.



2. Enter the code into the **Enter Code** field. Click the Verify button. You are redirected to the application landing page.