Setting Up

Multi-factor Authentication

Quick Reference Guide

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, SMS, or phone call).

NOTE: The screens featured throughout this guide reflect the standard design, but the look and feel may vary slightly depending on the application.

NOTE: For questions relating to the multifactor authentication roll-out, including privacy related questions, review the FAQ.

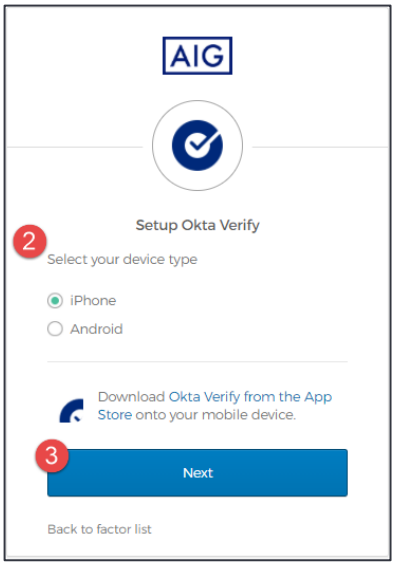
Setup Okta Verify

Users may at their discretion, choose from four currently supported methods to provide multifactor authentication. While only one method is necessary to authenticate the login, users may choose multiple MFA methods if desired, and may also change their MFA method at any time by contacting the Contact Center.

Okta Verify pushes an automatic verification to the user's mobile device (corporate or personal), allowing the user to the simply tap a notification to verify the login. Okta Verify must be installed on the user's mobile device to use this verification method.

To set up Okta Verify:

1. Click the **Setup** button in the Okta Verify option.
2. Click the **iPhone** or **Android** radio button to set up the appropriate device type.
3. Click the **Next** button.



To setup **Okta Verify** on mobile device:

1. Install Okta Verify by clicking on the links below.
   - iOS
   - Android
2. Launch **Okta Verify** on the mobile device.
3. Select **Organization** on the **Choose account type** screen.
4. Tap **Scan a QR code**. The QR code scanner opens.

NOTE: The app may need to be granted access to the device camera to continue.

5. Use the mobile device to scan the **QR code** on the computer screen. The account will be added to Okta Verify.
6. Click the **Next** button on the **Setup Okta Verify** screen.

If the QR Code does not work, click **Can't scan?** under the QR code to be given the option to activate Okta Verify via Email, SMS, or manually without Push Authentication. Follow the below instructions for the chosen activation method:

Email

1. Select **Send activation link via Email** and tap **Next**.
2. Open the email from Okta on your mobile device.
3. Tap **Activate Okta Verify Push** in the email. The Okta Verify app will open, and the **Enrolled in Push Authentication** will display.
4. Return to the setup page and ensure Okta Verify is displayed under Enrolled Factors.
5. Tap **Finish** on the mobile device to complete the process.

SMS

1. Select **Send activation link via SMS**.
2. Enter your mobile phone number in the **Phone number** field.
3. Tap **Next**.
4. You will receive a text message from Okta. Open this message and tap the link in it.
5. The Okta Verify app will open, and you should see a message that reads **Enrolled in Push Authentication**.
6. Return to the setup page and ensure Okta Verify is displayed under **Enrolled Factors**.
7. Tap **Finish** to complete the process.

Manual Setup without Push Authentication (not recommended)

1. Select **Setup manually without Push Authentication**. This will display a secret key you will use to configure the app.
2. Open the Okta Verify app.
3. Tap the **+** button.
4. Tap **No Barcode?**.
5. Enter your Okta account username and the secret key displayed on the Setup Screen.
6. Tap **Add Account**.
7. On the setup page, tap **Next**.
8. Tap the code displayed in the Okta Verify app to copy it, then paste it in the **Enter code** field.
9. Tap **Verify**.
10. Ensure Okta Verify is now displayed under **Enrolled Factors**.
11. Tap **Finish** to complete the process.

Additional Information

Click here for additional information about the Okta Verify application, including regarding personal information collected by Okta Verify. Okta Verify is a third-party application, and AIG does not manage or have access to any personal information that may be collected by the Okta Verify application.