PPL Next Gen Single Sign-On (SSO)

PPL Next Gen Single Sign-On (SSO)

Introduction

The purpose of this document is to provide information to market firms, and those responsible for IT change on the following topics.

- **PPL Next Gen Single Sign-On (SSO)**
- **Azure AD as an Identity Provider (IdP)**
- **Other Identity Providers (non-Azure)**
- **Multi-Factor Authentication (MFA)**
- **Getting ready for Next Gen SSO**
- **Questions & feedback**

The information contained in this document will support the use of PPL Next Gen and does not relate to the current platform (known as PPL v3).

PPL Next Gen Single Sign-On (SSO)

In line with other modern offerings, the authentication process for PPL Next Gen will use Single Sign-On (SSO). SSO will allow users to securely access the PPL Next Gen platform using their corporate credentials, rather than having to set-up and maintain yet another set of usernames and passwords. SSO functions are based on a trust relationship established between the party that holds the identity information (in this case the market firm's user directory) and the service/application which the user wants to access (PPL Next Gen).

Azure AD (AAD) is widely used in the insurance market; Next Gen's authentication functionality has been designed with this in mind. As part of the user onboarding process in Next Gen, end-users will be added as Guests in the PPL Next Gen Azure AD. Read more about Azure AD Guesting here:

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

This process also allows non-Azure AD users to be guested to the PPL Next Gen AD and access the platform securely.

Azure AD as an Identity Provider (IdP)

Market firms which are already using Azure AD as their IdP will be able to easily manage their users' access to PPL Next Gen. Moreover, the same login credentials and multi-factor methods which the firm's users are accustomed to will apply.

By default, Azure AD blocks end-users from accessing applications residing outside of their home tenants. Azure AD admins will need to configure the admin consent workflow within their AAD, prior to PPL Next Gen usage within your company to make this work. The following resources provide guidance on how to make the necessary changes:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/review-admin-consent-requests

A corporate/Office 365 email address can also exist as a personal Microsoft account. At the point of accepting the Microsoft invitation, it is important that end users choose the 'Work or school account' as opposed to the 'Personal Account' so this can be managed by their market firm and take full advantage of their existing SSO configuration.

PPL will actively monitor sign-up and inform firms if we believe a user has registered incorrectly.

Other Identity Providers (non-Azure)

Not having an existing Azure AD profile should not be a barrier to any users wanting to use PPL Next Gen. Therefore, the guesting process caters for this and creates an Azure persona for the end-user. The following sequence of events occurs during the guesting process:

1. Companies may wish to communicate with their staff to follow the steps below.
2. PPL admin user invites User A (non-Azure user) to Next Gen using User A's corporate email address, prior to go live.
3. User A receives an email containing a link to accept the invitation.
4. When User A clicks on the invitation link, the Microsoft authentication system recognizes that this email is not currently associated with an Azure AD user.
5. User A is requested to provide some additional details such as their first and last names as well as choose a password for their new Microsoft account.
   NB: the email address for this new Microsoft account will be the corporate email address of User A. As for the password, this will be a new password which can be different from the user's existing corporate email password. The default Microsoft password complexity requirements apply:
   "Passwords must have at least 8 characters and contain at least two of the following: uppercase letters, lowercase letters, numbers, and symbols."
6. Once the necessary details are provided, User A is then deemed to have accepted the invitation and the guesting process is complete.
7. User A can now access Next Gen via their browser Using the email address and password chosen in step 5.

For non-Azure IdPs, it is worth noting that end-user's access to the PPL Next Gen platform cannot be managed centrally via the firm's active directory. As such, the joiners, movers, and leavers (JML) process is slightly more complicated and it is therefore suggested internal processes are updated to reflect this. It is important that in the scenario when a user leaves the organisation or their access to the PPL Next Gen platform is no longer required, PPL should be promptly notified to turn off this user's account in Next Gen.

Multi-Factor Authentication (MFA)

Multifactor authentication adds another layer of protection to the sign-in process of an application. A username/email and password combination is no longer deemed sufficient, from a security perspective, to validate and authenticate a user.

Azure AD supports the following MFA methods:

- Microsoft Authenticator app
- Windows Hello for Business
- FIDO2 security key
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call

PPL Next Gen mandates the use of MFA – therefore every user attempting to log in will need to satisfy this criterion.

Users from firms with existing Azure AD configurations will be using the MFA methods set by their own firms; they won't need to perform another MFA verification on top of what they are used to. However, any users who are currently not presented with any MFA challenges will be prompted to set up one of the above MFA methods so they can proceed to access PPL Next Gen.

Getting ready for Next Gen SSO

Technical pre-requisites

To ensure that end-users can successfully accept the email invitations and access the PPL Next Gen platform, it is recommended that domain administrators perform the following checks:

- Ensure that users can receive invitation emails from 'invites@microsoft.com'.
- Verify that end-users who wish to access PPL Next Gen have at least one MFA method set up.
- The admin consent flow to allow access to PPL Next Gen is correctly configured (if applicable).

Once these pre-requisites have been verified and accepted, market firms should inform PPL to confirm their SSO readiness. This should ideally be completed by end of November 2022.

Testing prior to cutover

In preparation of accessing the PPL Next Gen Production environment, PPL have made available a JIT (Joint Integrated Testing) environment where market firms can take a first look at PPL Next Gen and ensure that they are ready from an SSO perspective.

Here are a few scenarios that market firms might want to validate in the JIT environment prior to cutover:

- End users can receive invitation emails from Next Gen, originating from 'invites@microsoft.com'.
- The Azure AD admin consent is configured correctly to allow end users to successfully login to Next Gen.
- MFA validation methods are present and configured correctly.
- End-users can log in to the PPL Next Gen platform successfully.
- The ability to restrict a specific user's access to Next Gen in case the user leaves the organisation, or their credentials compromised.

Market firms will need to go through the guesting and configuration process for each Azure AD tenant they access e.g., once for JIT and again for Production. This is because PPL have segregated test and real users/apps.

Governance

The approach to PPL Next Gen platform authentication and security has been ratified by the PPL IT&T technical governance committee.

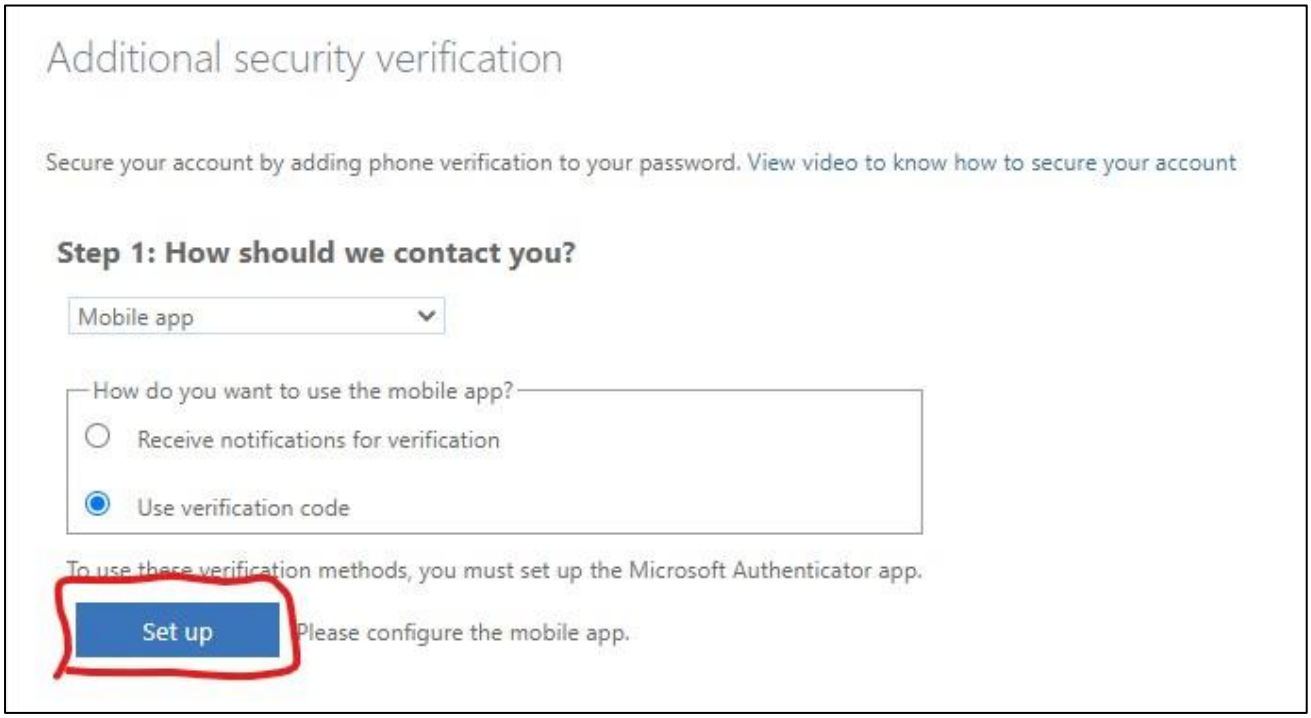
Frequently Asked Questions

Q: Can other MFA OTP providers be used?

A: Yes! By default, Azure lets users configure the Microsoft Authenticator as their One Time Password token provider. However, any other OATH compliant token generators can be used if required. Examples of these are: Google Authenticator, DUO MFA, Facebook Authenticator, Authy, FreeOTP, etc.

During MFA enrolment as part of accepting the Next Gen email invitation, a user will be prompted to provide 'Additional security information'.

Choose 'Mobile app' from the dropdown at the top of this screen and proceed to 'Set up'



On the next screen, choose 'Configure app without notifications. From here, users can use their preferred OATH compliant app to set it up either by scanning the QR code displayed on screen or by following the activation URL provided as an alternative.

Q: What happens if a user registers their corporate email as a personal account?

A: PPL will monitor account types and notify firms if they believe a user has registered incorrectly.

Q. If a user incorrectly registers with a personal account, will MFA still be enforced?

A. Yes. Although it will be an Azure AD supported MFA method, rather than the MFA preference of their corporate account.

Q. What happens if a firm fails to complete the pre-requisites checks?

A: There is a risk that end users won't receive their invitations and/or be able to access the PPL Next Gen platform.

Support & Feedback

If you have any questions or queries relating to this document, or any other enquiry relating to PPL, please contact your PPL Relationship Manager directly or email pplenquiries@placingplatformlimited.com.