AppConnect Frequently Asked Questions

Contents

Why are we upgrading our access management?

We are upgrading our access management to improve security and make it easier to manage who can access our systems. The upgraded system will ensure that only the right people can access the right applications at the right time. It will also protect our information from unauthorised access and make it easier to set up secure logins for staff and external agencies.

What's changing - AppConnect:

AppConnect is a self-registration portal for external users of the Department's applications to request access to those applications. This new version offers a two-phase approval process to ensure the verification and confirmation of the user's identity by their respective organisation before granting access to the Department's applications. Both organisation authorities, as well as new users will be able to submit registration requests.

Users will experience an improved onboarding process with Single Sign-On (SSO). This means users can log in once and access multiple applications without needing to re-enter their credentials.

As part of the transition, users will be given guest Microsoft Azure accounts with Multi-Factor Authentication. Multi-Factor Authentication (MFA) is a secure authentication process that requires you to provide more than one verification method to confirm your identity when attempting to log in. This process is designed to enhance the security of your accounts by adding an extra layer of protection beyond just a password.

During the registration process, users will need to set up MFA to complete their Azure account setup. This ensures that all users have an added layer of security when accessing applications. MFA prompts and setup will occur once a user has been successfully granted access

Additionally, AppConnect enables external agencies and the application owners to conduct User Access Reviews (UAR) effortlessly by providing automated reminders and allowing current users to retrieve reports to review and confirm access.

Why do we need AppConnect?

Right now, the Department uses different methods to onboard users and manage access, which can cause inconsistencies and security risks. AppConnect solves these problems by offering a streamlined and standardised way to manage user access with enhanced security through Multi Factor Authentication. This system ensures that approval and user access details can be regularly audited and reported as needed. It also provides application owners and organisational authorities with standard and secure access control.

When will AppConnect be available?

The AppConnect project team is currently collaborating with applications containing critical and sensitive information to facilitate their transition to the new onboarding method using AppConnect. Application support and business teams will be contacted directly by the project team according to the project timeline. The team will work closely with the application teams to ensure a smooth transition.

How will people know how to use the new platform?

User guides are available for AppConnect, these guides can soon be accessed from the AppConnect website under the Help section.

What is MFA?

MFA stands for Multi-Factor Authentication. It's a security process that requires users to provide multiple forms of identification before accessing an account or system. At the Department MFA will seek to confirm your identity via Microsoft Authenticator

By requiring multiple forms of verification, MFA significantly enhances security, making it much harder for unauthorised individuals to gain access.

How do I know MFA is secure?

1. **Enhanced Security**: MFA significantly enhances security by requiring multiple forms of verification, making it much harder for unauthorised users to gain access.
2. **Reduced Risk of Breaches**: Even if one factor (like a password) is compromised, the additional layers of authentication provide a strong defense against breaches.
3. **Encryption**: MFA solutions often use encryption to protect the data being transmitted, ensuring that your information remains secure, even from the departments.
4. **User Control**: You have control over the authentication methods used, such as biometrics, or one-time codes.
5. **Regular Updates**: MFA systems are regularly updated to address new security threats and vulnerabilities.

What is a Microsoft Azure guest account?

A Microsoft Azure guest account allows external users to access resources within a Microsoft Azure environment such as the Department's. These accounts are typically used for collaboration with partners, vendors, or contractors who need access to specific resources and applications but are not part of the organisation.

This setup enhances security by ensuring that external collaborators have only the access they need without exposing the Department's entire infrastructure.

What happens if I don't action the Microsoft Azure guest account request?

Eventually your log in access to eBusiness will be removed. However, if you have not actioned the email request you can simply chose to log in to the relevant application by selecting 'log in with Microsoft' and you'll be guided by a workflow to implement your guest account and MFA.

What is single sign on?

Single Sign-On (SSO) is an authentication process that allows a user to access multiple applications or systems with one set of login credentials. Here are the key aspects of SSO:

- Unified Access: Users log in once and gain access to all the applications and systems they have permissions for, without needing to log in separately to each one.
- Improved User Experience: SSO simplifies the login process, reducing the need to remember multiple usernames and passwords.
- Enhanced Security: By centralising authentication, SSO can improve security through stronger, more consistent authentication policies and reduced password fatigue.

SSO is commonly used in enterprise environments to streamline access to various internal and external applications, improving both security and user convenience.

Application administrators and owners

What does this mean for Application/Business owners and support?

As an Application/Business Owner from the Department, it will be your responsibility to review access requests validated by organisations and approve access as needed or nominate an application access approver to do so on your behalf.

AppConnect also provides the flexibility for an application/Business owner to take up the responsibility of an organisation authority or organisation access approver as needed for scenarios when an organisation does not have an approver in place.

External Agencies

What does this mean for external agencies?

It is essential for external agencies to ensure that their employees follow the agreed process for requesting access to the Department's applications via AppConnect. Agencies may nominate an Organisation Authority or Organisation Identity Approver, who will be added to the AppConnect system. This will ensure that access requests and user details are validated and confirmed by the organisation before being sent to the Department's Application Owner/Application Access Approver. The Organisation Authority or Organisation Identity Approver will also be responsible for conducting User Access Reviews via AppConnect as required by the Department.

Organisation Authority or Organisation Identity Approvers already registered via eBusiness will be automatically transferred to AppConnect with no activity required from them other than the individual setting up their new account and MFA. Refer to ‘What does this mean for existing Application Users?’

Application users

What does this mean for existing Application Users?

For most existing external users* of department applications, the transition will the following steps:

1. The user will be imported to AppConnect for the relevant application
2. A Microsoft Azure guest account will be created for the user, and they will receive an email to set up their multi-factor authentication and complete the Microsoft Azure account
3. The user can now log directly into the application

Once their AppConnect account is active they can either login directly through the application URL or via AppConnect, both paths will require MFA.

* Where external users already have an Azure guest account, they will only be required to set up their MFA. This may occur where one application they access has been transitioned to AppConnect before any other application they access.

What does this mean for new Application Users?

When requesting access for the first time, users will have the ability to request access via a new self-registration portal. They will register on AppConnect and receive an email verification link to complete their user details and select the relevant application.

Once the user has been verified and accepted to access the application, they will receive another email to finalise their account.