FORDWAY

fordway.com

Service Description
Azure AD Identity and Authentication services

Gold Microsoft Partner

Microsoft

Contents

01	Why do you need this?	**1-2**
02	What is Microsoft Entra?	**2**
03	Azure AD Versions	**2-3**
04	Implementing Conditonal Access	**3-6**
07	Implementing Privileged Identity Management	**7-8**
08	Service Outline	**8-9**
09	About Fordway	**10**
10	Service Terms	**10-12**
11	Ordering	**13**

Why do you need this?

Microsoft Azure AD, now part of Microsoft's Entra suite of Identity Management products, is the foundation of most organisations' Identity, Access and Authentication management.

Identity is the key to ensuring effective user and device security and ensuring seamless access to resources in our hybrid, multi-cloud world. It is also the foundational element for implementing effective Zero-Trust access and connectivity to organisational resources.

Fordway's Azure AD and Entra Identity Management services provide skills, capabilities and services developed from over 30 years' experience of configuring, managing and securing identity for our customers.

01 Why you need this?...continued

Our services help ensure that your organisation implements and maintains effective Identity management and security in the cloud, on premise or hybrid. The majority of organisations have granted excess permissions to users that they do not require, creating a larger attack surface. Because of its importance, the majority of bad actors start with attempting to breach and steal identity.

02 What is Microsoft Entra?

Microsoft Entra is Microsoft's newly released product family that encompasses all of their identity and access capabilities. The Entra family consists of Microsoft Azure AD and four new products:

- Cloud Infrastructure Entitlement Management (CIEM), which provides permissions analysis and management across multiple providers, allowing global policies to be set, managed and revoked from a central console
- Verified ID, which provides decentralised identity management to create, issue, and verify credentials with an identity verification solution to enable more secure interactions with anyone or anything.
- Workload Identities, which provides Conditional Access policies for workloads (rather than users and devices) and services to secure connections to them
- Identity Governance, which centrally controls access to SaaS applications and services that use Azure AD as an identity provider

03 Azure AD Versions

Azure Active Directory is available in three editions, with differing capabilities and costs, you need to ensure that you are licensed for the appropriate version to use the desired capabilities.

Azure Active Directory Free. This is provided with Office 365 E1, E3, E5, F1, A1, A3, A5; Microsoft 365 Business Basic, Apps for Business, Business Standard, Business Premium, A1; and included with Azure, Dynamics 365, Intune, and Power Platform. It provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.

Azure Active Directory Premium P1. Available as a separately licensed product or included with Enterprise Mobility + Security (EMS) E3 and Microsoft 365 E3, A3, F1, F3 subscriptions. In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager, and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

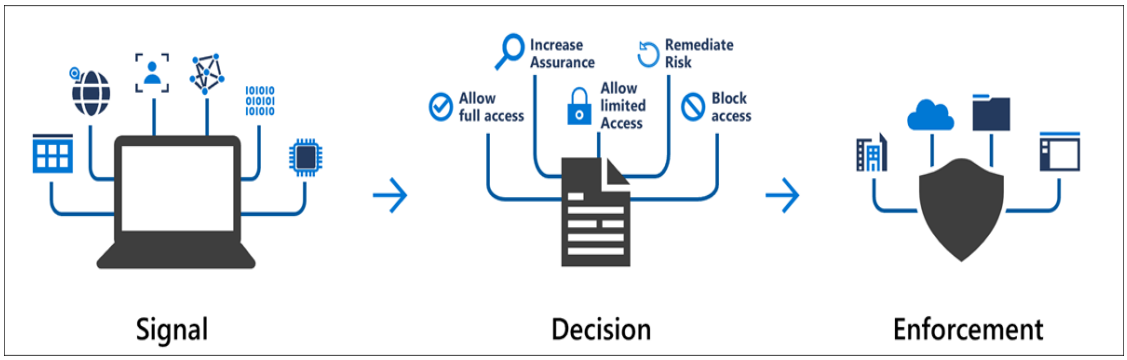
Azure Active Directory Premium P2. Available as a separately licensed product or included with Enterprise Mobility + Security (EMS) E5 and Microsoft 365 E5, A5 subscriptions. In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

Other Microsoft Entra products are separately licensed and not included in any of the above mentioned subscriptions.

04 Impementing Conditional Access

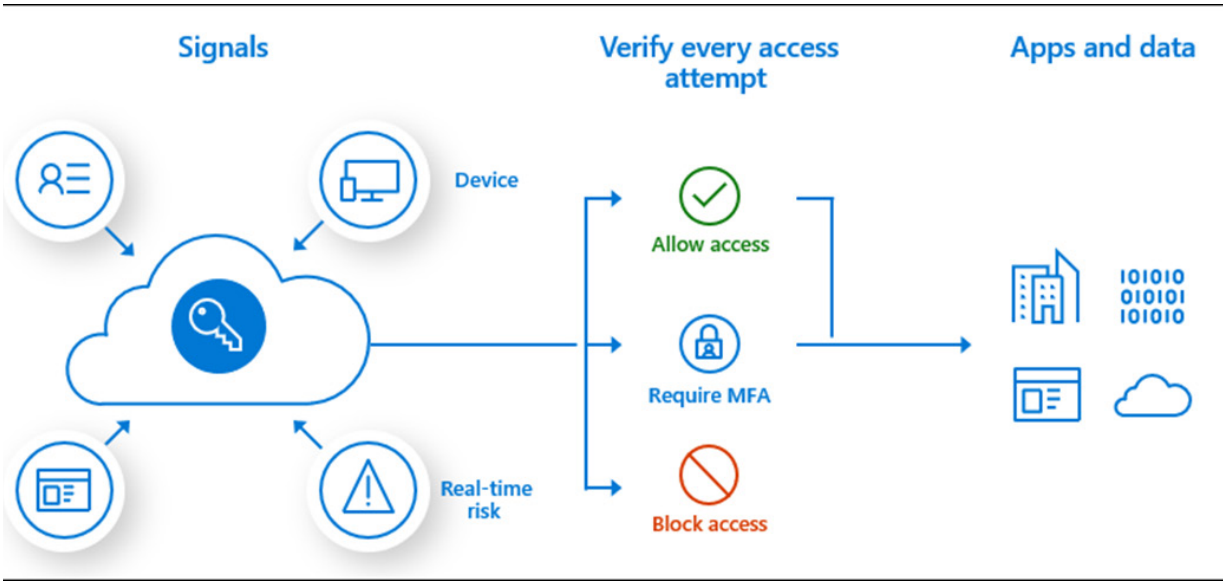
Conditional Access, available with Plan 1 and enhanced in Plan 2, is a core element of effective security and a key component for implementing Zero Trust Security, whose basic principle is that all users, devices and networks are untrusted until they are verified.

Conditional Access brings signals together to make authentication decisions, enforcing organisational access policies.



Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. For example: A payroll manager wants to access the payroll application and is required to use multifactor authentication after the password has been accepted to access it.

04



Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organisation's first line of defence for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Between the three Azure AD versions, the capabilities of each are:

Capability	Details	Azure AD Free / M365 Apps	Azure AD Premium P1	Azure AD Premium P2
Risk policies	Sign-in and user risk policies (via Identity Protection or Conditional Access)	No	No	Yes
Security reports	Overview	No	No	Yes
Security reports	Risky users	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Full access
Security reports	Risky sign-ins	Limited Information. No risk detail or risk level is shown.	Limited Information. No risk detail or risk level is shown.	Full access
Security reports	Risk detections	No	Limited Information. No details drawer.	Full access
Notifications	Users at risk detected alerts	No	No	Yes
Notifications	Weekly digest	No	No	Yes
MFA registration policy		No	No	Yes

04

Common signals

Common signals that Conditional Access can take into account when making a policy decision include the following signals:

User or group membership

- Policies can be targeted to specific users and groups giving administrators fine-grained control over access.

IP Location Information

- Organizations can create trusted IP address ranges that can be used when making policy decisions.
- Administrators can specify entire countries/regions IP ranges to block or allow traffic from.

Devices

- Users with specific devices or marked with a specific state can be used when enforcing Conditional Access policies.
- Use filters for devices to target policies to specific devices like privileged access workstations.

Application

- Users attempting to access specific applications can trigger different Conditional Access policies.

Real-time and calculated risk detection

- Signals integration with Azure AD Identity Protection (requires AAD Plan 2) allows Conditional Access policies to identify risky sign-in behaviour. Policies can then force users to change their password, do multifactor authentication to reduce their risk level, or block access until an administrator takes manual action.

Microsoft Defender for Cloud Apps (separately licensed)

- Enables user application access and sessions to be monitored and controlled in real time, increasing visibility and control over access to and activities done within your cloud environment

Common decisions

Block access

- Most restrictive decision

Grant access

- Least restrictive decision, can still require one or more of the following options:
  - Require multifactor authentication
  - Require device to be marked as compliant
  - Require Hybrid Azure AD joined device
  - Require approved client application
  - Require app protection policy (capability currently in preview)

04

Commonly applied policies

Examples of policies that can be enforced:

- Requiring multifactor authentication for users with administrative roles
- Requiring multifactor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for Azure AD Multifactor Authentication registration
- Blocking or granting access from specific locations or and requiring multifactor authentication for access from untrusted or unknown locations
- Blocking risky sign-in behaviours
- Requiring organisation-managed devices for specific applications
- Requiring up to date endpoint security is in place before granting access

05 Implementing Privileged Identity Management

If you are licensed for Azure AD Plan 2, Privileged Identity Management (PIM) enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other services such as Microsoft 365 or Microsoft Intune.

Reasons to use

Organisations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of:

- a malicious actor getting access
- an authorised user inadvertently impacting a sensitive resource

However, users still need to carry out privileged operations in Azure AD, Azure, Microsoft 365, or SaaS apps. Organisations can give users just-in-time privileged access to Azure and Azure AD resources and can oversee what those users are doing with their privileged access.

What does it do?

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Some of the key features of Privileged Identity Management are:

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit
- Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments

What can you manage in PIM

Today, you can use PIM with:

Azure AD roles – Sometimes referred to as directory roles, Azure AD roles include built-in and custom roles to manage Azure AD and other Microsoft 365 online services.

Azure roles – The role-based access control (RBAC) roles in Azure that grants access to management groups, subscriptions, resource groups, and resources.

PIM for Groups – To set up just-in-time access to member and owner role of an Azure AD security group. PIM for Groups not only gives you an alternative way to set up PIM for Azure AD roles and Azure roles, but also allows you to set up PIM for other permissions across Microsoft online services like Intune, Azure Key Vaults, and Azure Information Protection.

05

You can assign the following to these roles or groups:

Users - To get just-in-time access to Azure AD roles, Azure roles, and PIM for Groups.

Groups - Anyone in a group to get just-in-time access to Azure AD roles and Azure roles. For Azure AD roles, the group must be a newly created cloud group that's marked as assignable to a role while for Azure roles, the group can be any Azure AD security group. We do not recommend assigning/nesting a group to a PIM for Groups.

PIM is specifically targeted at the system administrators. The key issue with administrator access is that they can literally do anything and that is a massive risk to any organisation, whether it is accidental deletion of entire systems, deliberate misuse, or hacked by unknowns. It is vital to ensure this type of access is locked down, only granted when necessary and audited. It is also essential to minimise the number of administrators within any organisation. With PIM only the specific access to limited areas/servers, for time-bound periods can be granted. Fordway will assist any organisation in delivering secure role based, just-in-time policies and configuring the dashboard and reports to ensure all access is audited and understood.

06

Service Outline

Fordway's Azure AD and Entra Authentication Management Service offers 3 elements, each of which can be provided as separate engagements, or the three can be combined into a single comprehensive Identity Management improvement service.

Stage 1: Review and plan

This element of the service reviews the customer's current Active Directory, Azure AD and other Identity and Authentication service(s) against organisational requirements to help define if they are fit for purpose, correctly configured to meet the organisation's authentication controls and security needs or require change. Further to the standard identity 'health check' this phase provides, Fordway can deliver a comprehensive security audit and review of all identity and authorisation components as part of this phase, and identify potential vulnerabilities. If remediation or change is required, the review service will identify the changes needed plus the process, timescales, risk and indicative cost to implement these changes.

Stage 2: Implement and transform

Once the desired changes and the plan to implement them have been agreed, Fordway provide the technical expertise and experience to help implement the defined and agreed changes. Typically, these involve the implementation of Conditional Access as an initial stage to migrating the organisation to Zero Trust access, Privileged Identity Management for those organisations licensed for it, and implementing effective audit and security controls using Defender for Identity or third-party products.

06

We've been specialists helping organisations make best use of and optimising identity management since Novell Directory Services in the 1990's, and have worked with both Active Directory and Azure Active Directory since they were introduced in 1999 and 2010 respectively. We have completed over 1000 projects involving them, many involving integration with complimentary authentication providers.

Stage 3: Monitor, manage, update and secure

Once the new Identity and Authentication controls have been implemented and configured, the service needs looking after and securing, incidents need investigating and resolving, policies and access rules need regular reviews and updates, new SaaS applications and services requiring authentication are added and current services phased out.

There is also the continual churn of and management of joiners, movers and leavers to process, new devices and locations to be added, further requests to fulfil plus regular discussions as the Azure AD and Entra evolve whether it is worthwhile adding new capabilities.

Fordway provide a comprehensive service to manage all of these elements, through our 24 x 7 Service and Security Operations and our extended working hours Service Desk. Collectively these will ensure the ongoing management of the following:

a) Azure AD

  i. User, Computer and Group Management

b) Azure Active Directory Domain Services

  i. User, Computer and Group Management

c) Certificate management

d) ADFS synchronisation and/or AAD Connect

e) File Management/Azure Files/OneDrive

f) Active Directory

  i. User, Computer and Group Management

g) Conditional Access rules and policy management and updates (AAD Plan 1 and 2 only)

h) Privileged Identity Management (PIM, AAD Plan 2 only) for administrators and 3rd parties requiring access

i) Set up and administration of self-service password resets

j) Manage and allow just-in-time (JIT) access

k) Manage Multifactor Authentication tools and processes

07 About Fordway

Fordway offers over 30 years' experience advising and delivering strategic IT infrastructure and IT service delivery change to complex enterprises.

Fordway's consultancy helps inform your strategy and review the options relevant for your organisation. Our advice will be aligned to your business requirements. We can then assist with the ongoing migrations, operational management and optimisation of the resulting cloud service, based on best practice defined by the ITIL service management framework.

08 Service Terms

Service Initiation (on-boarding)

The service onboarding is a professional services engagement. The following procedure will be used to commence the service:

- Understand the work requirements
- Sign Non-Disclosure Agreements
- Provide a combination of Project Manager, consultants and engineers relevant for the work profile
- Review the customer requirements and determine the contractual requirements
- Agree the scope of the engagement with the customer and provide a Project Initiation Document which will define the engagement.
- Schedule work
- Commence engagement
- Provide deliverables
- Complete engagement

Suitable resources are likely to be required from the customer and potentially third-party organisations to initiate the service, working alongside Fordway staff. The actual roles and responsibilities will be finalised and agreed in the Project Initiation Document.

Termination Terms

Termination terms are per G-Cloud framework contract terms and conditions.

Service Levels

As the service is hosted and run from Microsoft Azure, the service levels will be defined by the underlying Microsoft SLAs for Azure, in line with the resilience configured in the environment.

08 Service Terms (...continued)

Service Management

Service Management is provided as part of the service. Customers will have an assigned Service Delivery Manager, access to Fordway's Customer Portal for service incidents and request management, plus monthly service reports and scheduled service reviews. All service is delivered to ISO20000 and aligned to the ITIL best practice framework.

Financial Recompense

Fordway offers service credits if the Fordway provided elements of the service do not consistently meet the SLA. Interruption or failure of underlying Azure infrastructure is covered by Microsoft's Service Credits.

Service Connectivity

The Service is Internet based, the customer will need suitable capacity and quality Internet connectivity to allow VPNs to be created to access the Azure resources. The customers Azure tenancy will be managed through Fordway's Azure Lighthouse/Azure Resource Manager tenancy management framework for the duration of the service.

Trial of Service

Not applicable to this service, although elements of the transition will be tested and can be implemented as a pilot. These requirements will be determined as part of the Project Initiation Document.

Data Security

Fordway is Cyber Essentials Plus accredited. Customer data is managed to ISO27001, 27017 and 27018 certified procedures. All data is stored, processed and managed in Azure. Where applicable Fordway will recommend, implement and operate suitable Azure Backup and Recovery procedures for the environment. Azure costs for these will be charged to the customer's Azure accounts.

Training

Fordway will provide skill transfer where applicable and documentation as part of the service onboarding. Formal training and courses can be provided if required.

Customer Responsibilities

Fordway will apply data access restrictions and other information security policies as mandated by the customer and required within Fordway's own organisational security controls. The customer is required to provide the necessary resources and information to allow Fordway to achieve the service deliverables as agreed within the Project Initiation Document.

08 Service Terms (...continued)

Change Management

All changes will be delivered through the Change Management process defined and configured in Fordway's Customer Portal. The process and toolset can interface with the customers Change Management processes.

Data Migration

Where data migration is required, this can either be done as a chargeable element of the service onboarding by Fordway or undertaken by the customer as part of their responsibilities.

Backup and Restore

Where Fordway have the responsibility for maintaining and managing the customer backups, this will be included in the service. Where the customer chooses to manage their own backups, they will be accountable for this function.

Ordering

Fordway's services can be ordered by contacting your Fordway account manager or other members of our team on **01483 528200**, emailing **sales@fordway.com** or using the contact form on our website **www.fordway.com**

Our Accreditations

ISO 9001
ISO 14001
ISO 27017
ISO 27018
ISO 20000
ISO 27001

HEALTH & SOCIAL CARE NETWORK COMPLIANT

CYBER ESSENTIALS PLUS

Microsoft Partner
Microsoft
Gold Cloud Productivity
Gold Cloud Platform
Gold Datacenter
Silver Security
Silver Small and Midmarket Cloud Solutions

PSN Public Services Network

FORDWAY

Fordway Solutions Ltd,
Ground Floor, Mill Pool House,
Charterhouse Suite, Mill Ln,
Godalming GU7 1EY
01483 528 200,
www.fordway.com