Best Practices Guide for Implementing Microsoft Entra

Your comprehensive roadmap to secure identity and access management

AzureCloud.pro

ⓘ INTRODUCTION

Why Microsoft Entra?

Formerly Azure Active Directory, Microsoft Entra has evolved into a comprehensive identity and access management platform that secures the modern enterprise.

Universal Connection

Connects employees, customers, and partners securely to applications, devices, and data

Zero Trust Foundation

Provides the foundation for Zero Trust security architecture and modern authentication

SECURITY PRINCIPLE

Principle of Least Privilege: The Cornerstone of Security

Minimal Permissions

Assign roles with only the minimum permissions necessary to complete specific tasks

Limited Scope

Restrict scope and duration of access to reduce overall risk exposure and attack surface

Tailored Roles

Leverage built-in roles or create custom roles specifically tailored to your organisation's unique needs

Critical Example: Avoid assigning broad administrator roles. Instead, assign narrowly scoped roles for specific resources and time-limited access.

AzureCloud.pro

AUTHENTICATION

Secure Authentication Practices

Modern Authentication Protocols

Implement robust, claims-based authentication that protects your organisation:

- Enforce OAuth2 for secure authorization
- Deploy OpenID Connect for modern identity
- Maintain SAML compatibility for legacy systems

Passwordless Future

Eliminate password vulnerabilities entirely by adopting passwordless authentication methods like Windows Hello for Business and FIDO2 security keys.

Infrastructure Security

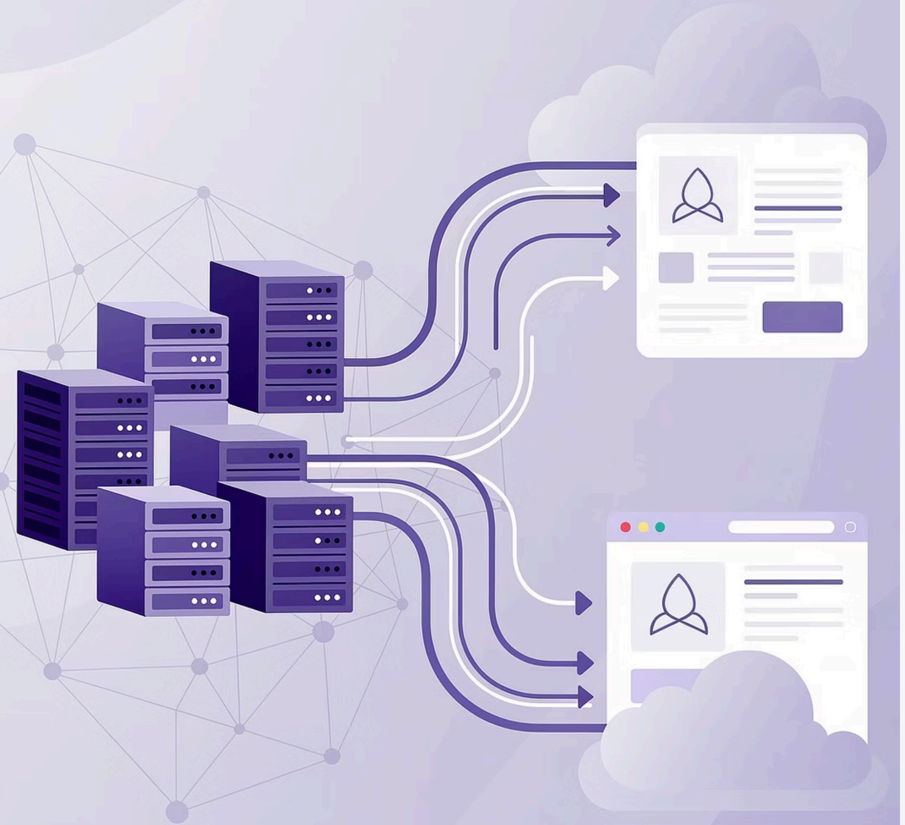
Secure workstations and infrastructure comprehensively to prevent credential theft and lateral movement across your network. A strong authentication system is only as secure as the endpoints it protects.

GOVERNANCE

Governance and Access Management

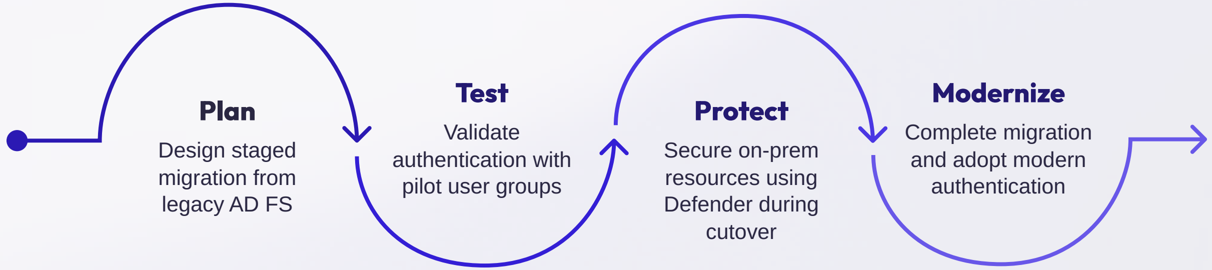
Robust governance ensures that user access remains controlled, auditable, and aligned with security policies. Microsoft Entra ID Governance provides the tools to implement dynamic access control.

Implement a "Deny by Default" security posture to restrict access unless explicitly granted, minimising the risk of unauthorised access.



MIGRATION

Application Migration Best Practices



Plan
Design staged migration from legacy AD FS

Test
Validate authentication with pilot user groups

Protect
Secure on-prem resources using Defender during cutover

Modernize
Complete migration and adopt modern authentication

Successful migration requires careful planning and phased execution. Test thoroughly with pilot users before full rollout to identify potential issues early and ensure seamless transition to modern authentication benefits.

AUTOMATION

PowerShell Automation and Security

01

Custom App Registration

Register custom applications for automation instead of using enterprise apps to precisely limit permissions

02

Apply Least Privilege

Grant only essential permissions in application configurations to minimise attack surface

03

Consistent Scripting

Utilise PowerShell for consistent configuration, monitoring, and maintenance across environments

04

Secure Credentials

Keep credentials and secrets secure; avoid client secrets wherever possible

PLANNING

Deployment Planning: Stakeholders & Roles

Key Stakeholder Identification

Successful deployment requires engagement from multiple stakeholders across the organisation:

- Executive Sponsor for strategic alignment
- IT Support for operational readiness
- Identity Architect for technical design
- Security Owner for risk management
- Compliance Manager for regulatory adherence

Define Responsibilities

Establish clear responsibilities using the RACI model to ensure accountability

Align Policies

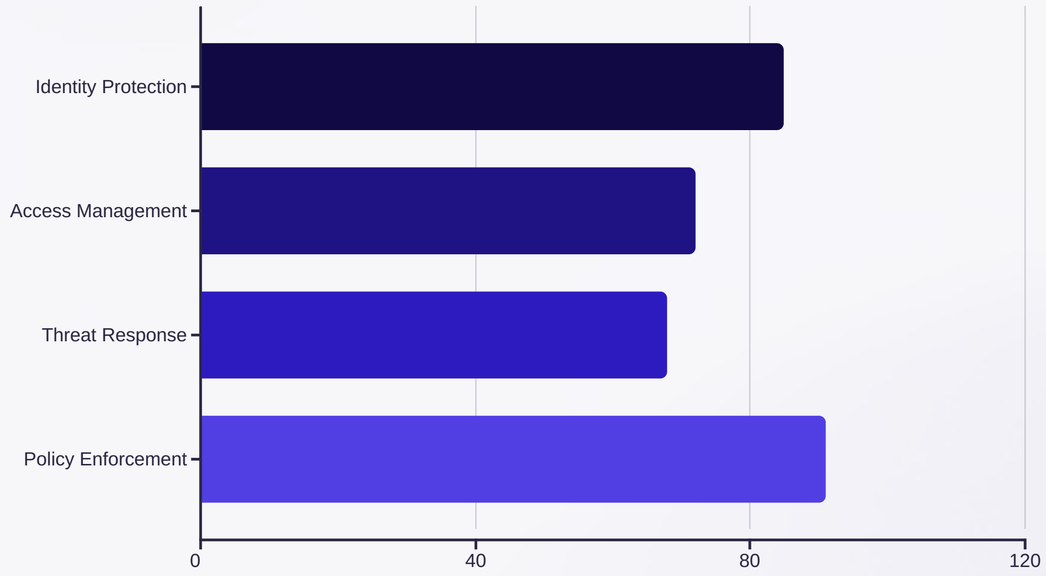
Align deployment with organisational security policies and compliance requirements

Prepare Scenarios

Prepare tailored strategies for both hybrid and cloud deployment scenarios

ASSESSMENT

Automated Security Assessment & Continuous Improvement



Continuous Security Posture

Leverage Microsoft's Zero Trust Assessment tool to automate comprehensive security posture checks and identify gaps proactively.

Continuously monitor identity risks and respond to emerging threats before they impact your organisation. Regular updates ensure configurations align with evolving best practices.

Foster a security-first culture through ongoing training, awareness programmes, and stakeholder engagement.

Conclusion: Secure Your Future with Microsoft Entra

Implement Rigorously

Apply least privilege principles and modern authentication across all systems

Govern Dynamically

Control access with PIM and entitlement management for adaptive security

Migrate Carefully

Plan transitions meticulously to unlock cloud benefits whilst maintaining security

Automate & Assess

Leverage continuous automation and assessment for long-term resilience

Microsoft Entra is your strategic partner for identity security in 2026 and beyond. By following these best practices, you'll build a robust, adaptable security foundation that protects your organisation whilst enabling innovation and growth.