MICROSOFT ENTRA
QUICK WINS for corporate

What is Microsoft Entra?

Microsoft Entra (formerly Azure Active Directory) is Microsoft's cloud-based Identity and Access Management (IAM) service, better known as **the backbone** of many corporate IT environments.

Microsoft Entra

For corporate organizations, it enables:

- Secure workforce access → one login for employees across Office 365, SaaS, and line-of-business apps.
- Stronger authentication → MFA, passwordless, passkeys, and biometrics to protect against phishing.
- Smarter access control → Conditional access and risk-based policies that adapt to how and where people work.
- Governance and compliance → visibility into privileged accounts, guest access, and audit trails that matter to regulators and customers alike.

Why it matters for corporates:

- Hybrid work and SaaS sprawl mean Microsoft Entra is your new perimeter.
- Audit and compliance requirements (NIS2, ISO, GDPR, etc.) increasingly start with identity.
- Misconfigurations, legacy policies, and poor governance are leading causes of breaches and audit findings.

In short - Microsoft Entra is the gatekeeper for your corporate IT environment.

Get it right, and you unlock secure, scalable business.
Get it wrong, and every system connected to it is at risk.
Most corporate tenants show the same weak spots.

The good news? You can check them yourself in minutes. Keep on reading...

MICROSOFT ENTRA QUICK WINS for corporate

We identified a few different levels in implementation difficulty, level 1 are quick wins you can tackle yourself, from level 2 and beyond we suggest contacting a professional...

Level 1: Quick wins you can check today

MFA Baseline

- Where to look: Entra → Security → Authentication methods → Policies
- What to check: Verify all users (incl. execs & contractors) are covered by MFA.
- Action: Still see “per user MFA”? → Time to modernize.

Conditional Access Basics

- Where to look: Entra → Security → Conditional Access → Policies
- What to check: Do you have at least:
  - Block legacy auth policy?
  - Require MFA for risky sign-ins?
  - Baseline admin-role protection
- Action: Implement updated policies as needed

Guest Access Review

- Where to look: Entra → Users → External users
- What to check: Sort by last sign-in date. Dormant guests hanging around?
- Action: disable accounts or review access together with business sponsors.

Privileged Role Assignments

- Where to look: Entra → Roles & administrators
- What to check: Are admins permanently assigned or using PIM? (Hint: permanent assignments = big audit finding.)
- Action: Implement PIM for your riskiest roles

MICROSOFT ENTRA QUICK WINS for corporate

Level 2 & beyond: Where you'll need expert help

If you spotted gaps above, you're not alone. But the real test of maturity is in:

- Enforcing phishing-resistant authentication strengths
- Using risk-based Conditional Access (Identity Protection)
- Managing break-glass accounts safely
- Governing app registrations & enterprise apps
- Integrating monitoring & alerts into your SOC
- Using Microsoft Entra alongside other tools like SAP, Atlassian and many more.

> These are not "checklist fixes", they require architecture, licensing, and governance know-how.

ACEN helps **corporate organizations** move from "we enabled MFA" to a fully governed, risk-based Microsoft Entra posture.

We secure access without slowing down your business. Make an appointment today for a one-on-one conversation and some free advice you can use immediately.

Sit down with our experts for a focused walkthrough of Entra.

In a 30-minute, one-on-one session, we will show you a current real-life setup, show key Entra capabilities and discuss quick wins for security and compliance.

Book a demo now

→ www.acen.eu/en/microsoft-entra-demo