

MICROSOFT ENTRA

QUICK WINS for government



What is Microsoft Entra?

Microsoft Entra (formerly Azure Active Directory) is Microsoft's cloud-based Identity and Access Management (IAM) service — a cornerstone for modern public administration.



For government bodies, it enables:

- Secure workforce and partner access → one login for employees, agencies, and contractors across Microsoft 365, SaaS, and line-of-business systems.
- Trusted authentication → MFA, passwordless, passkeys, and national eID integrations to protect against phishing and impersonation.
- Policy-driven access → Conditional Access and risk-based rules that adapt to citizen services, location, and device security.
- Governance and accountability → visibility into privileged accounts, supplier access, and audit logs aligned to EU regulations.

Why it matters for government in the EU:

- Regulations like NIS2, GDPR, and eIDAS 2.0 mandate strong identity security.
- Government IT increasingly depends on cross-agency collaboration and secure third-party access.
- Sovereignty and data residency requirements demand careful governance of cloud identity platforms.
- Weak misconfigurations risk not only data breaches, but also public trust.

In short - Microsoft Entra is the gatekeeper for digital government services.

Get it right, and you enable secure, citizen-focused administration
Get it wrong, and critical services — from tax to healthcare — are exposed.

The good news? You can discover the weak spots yourself. Keep on reading...

MICROSOFT ENTRA

QUICK WINS for government



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: Are all staff, contractors, and external partners covered by MFA?
- Action: Still see “per user MFA”? → Replace with centralized policies.

Conditional Access Basics

- Where to look: Entra → Security → Conditional Access → Policies
- What to check: Do you enforce:
 - Block legacy authentication?
 - Require MFA for risky sign-ins?
 - Baseline protections for admin roles?
- Action: Align rules with NIS2 minimum-security standards.

Supplier & partner Access Review

- Where to look: Entra → Users → External users
- What to check: Dormant supplier/partner accounts with unnecessary privileges?
- Action: Disable or review with sponsoring agency.

Privileged Role Assignments

- Where to look: Entra → Roles & administrators
- What to check: Are admins permanently assigned or using PIM (Privileged Identity Management)?
- Action: Implement PIM for sensitive roles to improve accountability.

MICROSOFT ENTRA

QUICK WINS for government



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

If you spotted gaps above, you're not alone. EU governments need to go further by:

- Enforcing phishing-resistant authentication (smartcards, passkeys, national eIDs).
- Applying risk-based Conditional Access across agencies and jurisdictions.
- Governing cross-border collaboration with EU institutions and partners.
- Securing break-glass accounts for critical continuity scenarios.
- Monitoring and reporting for NIS2 and eIDAS 2.0 compliance.
- Aligning Entra with EU sovereignty and data residency requirements.



These aren't "checklist fixes", they require careful design, licensing strategy, and cross-agency governance.

ACEN helps **government 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

