



MFE-IT

Reference: YAS/EN/300

Training Course SC-300 — Identity and Access Management

with Azure AD and Microsoft Entra

Duration: 3.5 Days | Hours: 21 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

Identity and access management is an essential pillar of any cloud cybersecurity strategy. In a world where the network perimeter has dissolved, identity is the new control plane — and Microsoft Entra ID (formerly Azure AD) is the foundation of that control plane for organisations using Microsoft 365 and Azure.

This SC-300 operational training course provides you with the practical skills to effectively administer Microsoft Entra ID and prepare for the SC-300 Microsoft Identity and Access Administrator Associate certification. You will learn to implement, manage and secure user identities, conditional access policies, multi-factor authentication and Zero Trust architectures within Azure and Microsoft 365 environments.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Implement identities with Microsoft Entra ID (Azure AD)
- Configure multi-factor authentication (MFA), roles and governance
- Enforce conditional access and Zero Trust policies
- Integrate third-party applications with SSO and SCIM
- Monitor identities and detect risky behaviour

PREREQUISITES

- Basic knowledge of Microsoft 365 or Azure services
- Experience in managing users, groups or directories
- Understanding of IT security concepts (authentication, authorisation)

Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.

TARGET AUDIENCE

Cloud administrators, security technicians and IT managers responsible for securing Microsoft 365 and Azure environments.

DETAILED PROGRAMME

The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Introduction to Microsoft Entra ID

- IAM concepts and administrative roles
- Microsoft tools for identity management
- Entra ID positioning vs traditional Active Directory

Module 2 – Identity Creation and Management

- Users, groups and RBAC roles
- Synchronisation with AD DS via Azure AD Connect / Cloud Sync
- Automated provisioning and lifecycle workflows

Module 3 – Authentication and MFA

- Multi-factor authentication implementation
- Session security and authentication strength
- Enrolment policies and phishing-resistant methods

Module 4 – Conditional Access and Zero Trust Strategy

- Contextual access policies based on location and device
- Risk signals from Identity Protection
- Building a layered Conditional Access framework

Module 5 – Application Access Management

- SSO integration and federation
- SCIM provisioning and application proxy
- Application access security and consent governance

Module 6 – Monitoring, Reporting and Remediation

- Sign-in and audit logs
- Identity Protection alerts and risk policies
- Incident response and best practices

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts