

Configure and Govern Entitlement with Microsoft Entra ID (SC-5008)

Duration: 0,5 day

Audience: Professionnel TI

Who is this training for?

This course is targeted at people who want to implement an end-to-end entitlement management solution based on the principles of Zero Trust. Students should have experience with Azure and experience in the creation of identities and granting those identities access to resources.

Training objectives

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

- Configure and manage Microsoft Entra entitlement management to streamline user access while supporting Zero Trust security principles.
- Implement access reviews and privileged access controls to maintain least-privilege access and strengthen organizational security.
- Monitor and respond to identity and access-related security events using best practices to improve compliance and security posture.

Summary

In today's digital landscape, managing access and entitlements is crucial for safeguarding sensitive information and ensuring compliance. This intensive one-day course offers a deep dive into Microsoft Entra Entitlement Management, Access Reviews, Privileged Access, and Monitoring. Participants will learn how to streamline access management with Entitlement Management, conduct thorough Access Reviews to maintain least privilege, manage high-risk Privileged Access, and implement robust Monitoring strategies to detect and respond to security events promptly. By the end of the training, attendees will be equipped with the best practices and actionable insights to enhance their organization's security posture.

Course outline

Learning Path 1: Configure and Govern Entitlement with Microsoft Entra ID

- Module 1: Plan and Implement Entitlement Management
- Module 2: Plan, Implement, and Manage Access Review
- Module 3: Monitor and Maintain Microsoft Entra ID
- Module 4: Plan and Implement Privileged Access

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants progressively explore Microsoft Entra ID entitlement governance through hands-on exercises based on real-world identity and access management scenarios, promoting immediate application of the concepts learned.

They learn how to implement entitlement management, conduct access reviews, manage privileged access, and monitor identity-related security events using Microsoft Entra ID.

Led by a Microsoft Certified Trainer (MCT), the training emphasizes interactivity and the development of practical skills that can be directly applied to strengthen access governance and support Zero Trust security initiatives.

Prerequisites

Students should have the following knowledge and experience before attending this course:

- Understand security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, shared responsibility, and zero trust model.
- Be familiar with identity providers like Microsoft Entra ID, Microsoft Entra Domain Services, or other authentication providers.
- Have experience with Windows and/or Linux operating systems and minor scripting language experience. This course touches on the use of PowerShell and the CLI.

Recommendations

- Knowledge of security and access management concepts Be comfortable with Microsoft 365 / Azure environments
- Understand access governance concepts (lifecycle, permissions) Have experience in administration or IT security (asset)

Legal notices

© AFI Expertise inc