

MS-SC5008: CONFIGURE AND GOVERN ENTITLEMENT WITH MICROSOFT ENTRA ID



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Security	Instructor-led	NA

INTRODUCTION

Use Microsoft Entra to manage access by using entitlements, access reviews, privileged access tools, and monitor access events.

AUDIENCE PROFILE

This course is designed for individuals who want to implement an end-to-end entitlement management solution based on Zero Trust principles.

PREREQUISITES

Before attending this course, delegates must know:

- Basic Azure administration knowledge.
- Ability to create users and groups using Microsoft Entra.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Understand machine learning, computer vision, natural language processing, document intelligence, and knowledge mining.
- Learn about generative AI and its challenges and risks.
- Understand responsible AI practices.
- Understand the role of copilots and how to use them effectively.
- Explore considerations for Copilot prompts and extending/developing copilots.
- Plan and develop responsible generative AI solutions.
- Identify, measure, and mitigate potential harms.
- Operate a responsible generative AI solution.
- Get acquainted with Microsoft Copilot for Security and its terminology.
- Learn how to enable Microsoft Copilot for Security.
- Explore the features available in the standalone experience.
- Learn about Microsoft and non-Microsoft plugins, custom promptbooks, and knowledge base connections.
- Understand how Microsoft Copilot integrates with Microsoft Defender XDR, Microsoft Purview, Microsoft Entra, Microsoft Intune, and Microsoft Defender for Cloud.
- Experience the first run and standalone experiences.
- Configure plugins and explore file uploads as a knowledge base.
- Create custom promptbooks and explore capabilities in various Microsoft security products.

COURSE CONTENT

Module 1: Plan and implement entitlement management

When new users or external users join your site, quickly assigning them access to Azure solutions is a must. Explore how to entitle users to access your site and resources.

Lessons

- Introduction
- Define access packages
- Exercise create and manage a resource catalog with Microsoft Entra entitlement management
- Configure entitlement management
- Exercise add terms of use acceptance report

- Exercise manage the lifecycle of external users with Microsoft Entra identity governance
 - Configure and manage connected organizations
 - Review per-user entitlements
 - Knowledge check
 - Summary and resources
- By the end of this module, you will be able to:
- Define catalogs.
 - Define access packages.
 - Plan, implement and manage entitlements.
 - Implement and manage terms of use.

- Manage the lifecycle of external users in Microsoft Entra Identity Governance settings.

Module 2: Plan, implement, and manage access review

Once identity is deployed, proper governance using access reviews is necessary for a secure solution. Explore how to plan for and implement access reviews.

- Lessons
- Introduction
- Plan for access reviews
- Create access reviews for groups and apps
- Create and configure access review programs

- Monitor access review findings
 - Automate access review management tasks
 - Configure recurring access reviews
 - Knowledge check
 - Summary and resources
- By the end of module, you will be able to:
- Plan for access reviews
 - Create access reviews for groups and apps
 - Monitor the access review findings
 - Manage licenses for access reviews
 - Automate management tasks for access review
 - Configure recurring access reviews

Module 3: Monitor and maintain Microsoft Entra ID

Audit and diagnostic logs within Microsoft Entra ID provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyse sign-in data.

Lessons

- Introduction
- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- Exercise connect data from Microsoft Entra ID to Microsoft Sentinel
- Export logs to third-party security information and event management system

- Analyze Microsoft Entra workbooks and reporting
 - Monitor security posture with Identity Secure Score
 - Knowledge check
 - Summary and resources
- By the end of this module, you'll be able to:
- Analyse and investigate sign in logs to troubleshoot access issues
 - Review and monitor Microsoft Entra audit logs
 - Enable and integrate Microsoft Entra diagnostic logs with Log Analytics / Azure Sentinel
 - Export sign in and audit logs to a third-party SIEM (security information and event management)
 - Review Microsoft Entra activity by using Log Analytics / Azure Sentinel, excluding KQL (Kusto Query Language) use
 - Analyse Microsoft Entra workbooks / reporting
 - Configure notifications

Module 4: Plan and implement privileged access

Ensuring that administrative roles are protected and managed to increase your Azure solution security is a must. Explore how to use PIM to protect your data and resources.

Lessons

- Introduction

- Define a privileged access strategy for administrative users
 - Configure Privileged Identity Management for Azure resources
 - Exercise configure Privileged Identity Management for Microsoft Entra roles
 - Exercise assign Microsoft Entra roles in Privileged Identity Management
 - Exercise assign Azure resource roles in Privileged Identity Management
 - Plan and configure Privileged Access Groups
 - Analyze Privileged Identity Management audit history and reports
 - Create and manage emergency access accounts
 - Knowledge check
 - Summary and resources
- By the end of this module, you'll be able to:
- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds)
 - Configure Privileged Identity Management for Microsoft Entra roles
 - Configure Privileged Identity Management for Azure resources
 - Assign roles
 - Manage PIM requests
 - Analyse PIM audit history and reports
 - Create and manage emergency access accounts

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or exam for this course.