

**Microsoft 365 Enterprise Mobility and Security**

**Course Number:** OFC-104  
**Duration:** 5 days

**Overview**

[Microsoft Enterprise Mobility and Security (EMS)](https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security) is an intelligent mobility management and security suite that protects employees across their devices, whether they are using on-prem or Azure-based applications. In this training, attendees learn how to use Microsoft EMS to ensure the security of their organization in-cloud and on-prem.

**Prerequisites**

General knowledge of the Microsoft 365 environment and admin suite is required.

**Materials**

All Microsoft 365 training students receive comprehensive courseware.

**Software Needed on Each Student PC**

Microsoft 365, EMS Licensing

**Objectives**

All students learn how to:

* Secure identity in their Microsoft 365 Environment
* Setup active security monitoring for their environment
* Deploy MDM and Endpoint protection to their end-users and devices
* Protect their organization's information with Azure Information Protection
* Prevent malicious email activity with Advanced Threat Protection

**Outline**

* Introduction
* Azure Active Directory
  + Enabling SSO with organization applications
  + Setting up MFA for Admins and Users
  + Configuring Conditional Access Policies
  + Configuring Reporting
  + Risk-based conditional access
  + Privileged Identity Management
* Microsoft Intune
  + Configuring Device and User Policies
  + Enrolling New users and devices
  + Advanced Device Management
  + Managing Device Endpoint Protection
  + Reporting on Assets
  + Deploying Applications
  + Managing Update Policies
* Azure Information Protection
  + Configure Information Protection Templates
  + Configuring Labels
  + Setting Classifications
  + Day to Day Integration
  + Email Encryption
* Microsoft Cloud App Security
  + Setting up cloud discovery for shadow IT
  + Creating Custom Alerts for Discovery
  + Setting up third party app connections
  + Connecting your on-premise (Firewall) network
  + Connecting your Endpoint Protection
  + Active Reporting and Assessing Compliance of your apps
  + Setting custom score metrics for applications
* Microsoft Advanced Threat Analytics
  + Setup and Configure ATA Gateways
  + ATA Database Management
  + Reporting with ATA
  + Setting ATA Role groups
  + Setting Domain Connectivity Password
  + Excluding Entities from Detection
  + Exporting/Importing Configurations
  + Managing System Generated Logs
  + Setting ATA Notifications
  + Setting Syslog and Email Server Settings
  + Tagging Sensitive Accounts
  + Preventing Lateral Movements
  + Troubleshooting Issues
* Azure Advanced Threat Protection
  + Setting up Azure ATP
  + Connecting to your Active Directory
  + Configuring the Azure ATP Sensor Package
  + Investigating Alerts
  + Investigating Computers and Users
  + Understanding Entity Profiles
  + Understanding Network Name Resolution
  + Reporting with Azure ATP
  + User Roles with Azure ATP
* Microsoft Secure Score
  + Understanding Microsoft Secure Score
  + Find your Score
  + Taking action on recommendations
  + Best practices without hindering productivity
* Conclusion