

# COURSE OVERVIEW

**Course Name:**  
(MS-102) Microsoft 365 Administrator Essentials

**COURSE DURATION: 5 Days**

**Gauteng:**

3rd Floor, 34 Whitely Road  
Melrose Arch  
Johannesburg  
2196

**Gauteng:**

192 on Bram  
192 Bram Fischer Drive  
Ferndale, Randburg  
Johannesburg  
2160

**Cape Town:**

3rd Floor, Thomas Pattullo Building  
19 Jan Smuts St  
Cape Town  
8000

**Durban:**

9 Mountview Close  
Broadlands  
Mount Edgecombe  
Durban  
4302

 **087 941 5764**

 **sales@impactful.co.za**

 **impactful.co.za**

## INTRODUCTION

This course covers the following key elements of Microsoft 365 administration: Microsoft 365 tenant management, Microsoft 365 identity synchronization, and Microsoft 365 security and compliance. In Microsoft 365 tenant management, you learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, security groups, and administrative roles. You then transition to configuring Microsoft 365, with a primary focus on configuring Office client connectivity. Finally, you explore how to manage user-driven client installations of Microsoft 365 Apps for enterprise deployments. The course then transitions to an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect and Connect Cloud Sync. You learn how to plan for and implement each of these directory synchronization options, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multifactor authentication and self-service password management. In Microsoft 365 security management, you begin examining the common types of threat vectors and data breaches facing organizations today. You then learn how Microsoft 365's security solutions

address each of these threats. You are introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you are introduced to the various reports that monitor an organization's security health. You then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint. Once you have this understanding of Microsoft 365's security suite, you then examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Microsoft Purview message encryption, and data loss prevention (DLP). You then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You then examine how to implement these compliance features by using data classification and sensitivity labels.

## INTENDED AUDIENCE

This course is designed for persons aspiring to the Microsoft 365 Administrator role and have completed at least one of the Microsoft 365 role-based administrator certification paths.

## PREREQUISITES

Before attending this course, students must have:

- Completed a role-based administrator course such as Messaging, Teamwork, Security, Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.
- A working knowledge of PowerShell.

## COURSE CONTENT

### Configure your Microsoft 365 experience

This module examines each of the tasks that an organization must complete to successfully configure its Microsoft 365 experience.

### Manage users, licenses, and mail contacts in Microsoft 365

This module provides instruction on how to create and manage user accounts, assign Microsoft 365 licenses to users, recover deleted user accounts, and create and manage mail contacts.

### Manage groups in Microsoft 365

This module provides instruction on how to create groups for distributing email to multiple users within Exchange Online. It also explains how to create groups to support collaboration in SharePoint Online.

### Add a custom domain in Microsoft 365

This module provides instruction on how to add a custom domain to your Microsoft 365 deployment. It also examines the DNS requirements that are necessary to support a new domain.

### Configure client connectivity to Microsoft 365

This module examines how clients connect to Microsoft 365. It also provides instruction on how to configure name resolution and Outlook clients, and how to troubleshoot client connectivity.

## **Configure administrative roles in Microsoft 365**

This module examines the key functionality that's available in the more commonly used Microsoft 365 admin roles. It also provides instruction on how to configure these roles.

## **Manage tenant health and services in Microsoft 365**

This module examines how to monitor your organization's transition to Microsoft 365 using Microsoft 365 tools. It also examines how to develop an incident response plan and request assistance from Microsoft.

## **Deploy Microsoft 365 Apps for enterprise**

This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.

## **Analyze your Microsoft 365 workplace data using Microsoft Viva Insights**

This module examines the workplace analytical features of Microsoft Viva Insights, including how it works, and how it generates insights and improves collaboration within an organization.

## **Explore identity synchronization**

This module examines identity synchronization and explores the authentication and provisioning options that can be used, and the inner-workings of directory synchronization.

## **Prepare for identity synchronization to Microsoft 365**

This module examines all the planning aspects that must be considered when implementing directory synchronization between on-premises Active Directory and Microsoft 365.

## **Implement directory synchronization tools**

This module examines the Azure AD Connect and Azure AD Connect Cloud Sync installation requirements, the options for installing and configuring the tools, and how to monitor synchronization services using Azure AD Connect Health.

## **Manage synchronized identities**

This module examines how to manage user identities when Azure AD Connect is configured, how to manage users and groups in Microsoft 365 with Azure AD Connect, and how to maintain directory synchronization.

## **Manage secure user access in Microsoft 365**

This module examines various password-related tasks for users and administrators, including:

- creating and configuring password policies
- configuring self-service password management
- configuring multifactor authentication
- implementing entitlement packages
- implementing conditional access policies

## **Examine threat vectors and data breaches**

This module examines the types of threat vectors and their potential outcomes that organizations must deal with on a daily basis and how users can enable hackers to access targets by unwittingly executing malicious content.

### **Explore the Zero Trust security model**

This module examines the concepts and principles of the Zero Trust security model, as well as how Microsoft 365 supports it, and how your organization can implement it.

### **Explore security solutions in Microsoft 365 Defender**

This module introduces you to several features in Microsoft 365 that can help protect your organization against cyberthreats, detect when a user or computer has been compromised, and monitor your organization for suspicious activities.

### **Examine Microsoft Secure Score**

This module examines how Microsoft Secure Score helps organizations understand what they've done to reduce the risk to their data and show them what they can do to further reduce that risk.

### **Examine Privileged Identity Management**

This module examines how Privileged Identity Management ensures users in your organization have just the right privileges to perform the tasks they need to accomplish.

### **Examine Azure Identity Protection**

This module examines how Azure Identity Protection provides organizations the same protection systems used by Microsoft to secure identities.

### **Examine Exchange Online Protection**

This module examines how Exchange Online Protection (EOP) protects organizations from phishing and spoofing. It also explores how EOP blocks spam, bulk email, and malware before they arrive in users' mailboxes.

### **Examine Microsoft Defender for Office 365**

This module examines how Microsoft Defender for Office 365 extends EOP protection by filtering targeted attacks such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs.

### **Manage Safe Attachments**

This module examines how to manage Safe Attachments in your Microsoft 365 tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

### **Manage Safe Links**

This module examines how to manage Safe Links in your tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

### **Explore threat intelligence in Microsoft 365 Defender**

This module examines how Microsoft 365 Threat Intelligence provides admins with evidence-based knowledge and actionable advice that can be used to make informed decisions about protecting and responding to cyber-attacks against their tenants.

### **Implement app protection by using Microsoft Defender for Cloud Apps**

This module examines how to implement Microsoft Defender for Cloud Apps, which identifies and combats cyberthreats across all your Microsoft and third-party cloud services.

### **Implement endpoint protection by using Microsoft Defender for Endpoint**

This module examines how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats by using endpoint behavioural sensors, cloud security analytics, and threat intelligence.

### **Implement threat protection by using Microsoft Defender for Office 365**

This module examines the Microsoft Defender for Office 365 protection stack and its corresponding threat intelligence features, including Threat Explorer, Threat Trackers, and Attack simulation training.

## **DELIVERY METHOD**

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
  - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client