Microsoft 365 Tenant Deployment, Configuration, and Monitoring

This course examines the Microsoft 365 platform and includes lessons and lab exercises on the key skills you'll need for deploying, configuring, and managing a Microsoft 365 environment. You'll learn how to plan, deploy, and manage a Microsoft 365 tenant by using the Microsoft 365 admin portal, Microsoft Entra admin center, and Windows PowerShell. You'll also learn how to provision and configure a new Microsoft 365 tenant, create new identities or connect to an existing identity infrastructure, and monitor and support a Microsoft 365 tenant.

Required Prerequisites

- Basic experience with on-premises Windows Active Directory
- Basic experience with business email systems such as Microsoft Exchange
- Basic experience with Domain Name System (DNS)
- Basic understanding of cloud services

Table of contents

Lesson 1: Introducing and provisioning Microsoft 365

- Overview of Microsoft 365 workloads
- Microsoft 365 subscriptions for personal or home use
- Microsoft 365 subscriptions for business use
- Microsoft 365 subscriptions for enterprise use
- Initial Microsoft 365 tenant provisioning
- Adding products and licenses to your tenant
- Managing payments and billing accounts

Lesson 2: Configuring your Microsoft 365 tenant

- Adding and configuring a custom domain
- Configuring organizational settings
- Managing integrated apps
- Managing partner relationships
- Configuring Microsoft 365 app installation options

Lesson 3: Microsoft 365 for end-users

- Overview of the Microsoft 365 end-user portal
- Installing Microsoft 365 apps
- Overview of Microsoft 365 end-user account management

Lab Provisioning and configuring a Microsoft 365 tenant

- Exercise 1: Provisioning a Microsoft 365 trial tenant
- Exercise 2: Adding products and licenses to a Microsoft 365 tenant

- Exercise 3: Configuring Org Settings for the Microsoft 365 tenant
- Exercise 4: Configuring integrated apps and Microsoft 365 app installation options

Day 2: Module 2 helps to create and manage the most used objects in Microsoft 365, such as users, groups, and teams. We'll also learn about resources and devices from the perspective of Microsoft 365.

Module 2 Managing users, groups, teams, devices, and resources in Microsoft 365

Lesson 1: Administering Microsoft 365

- Overview of administrative consoles for Microsoft 365
- Connecting Windows PowerShell to Microsoft 365

Lesson 2: Managing users

- Adding and managing user accounts
- Adding and managing guest users
- Adding and managing contacts
- Synchronizing on-premises identities

Lesson 3: Managing groups

- Overview of group types and teams
- Adding and managing groups
- Policies for groups and teams

Lesson 4: Managing email and collaboration services

- Configuring email services
- Overview of shared mailboxes
- Overview of rooms and equipment
- Overview of mail users
- Managing sites in Microsoft 365
- Using Outlook as a tool for email and collaboration

Lab Managing user, resource, and group objects in Microsoft 365

- Exercise 1: Adding and configuring a new user
- Exercise 2: Creating a user template
- Exercise 3: Creating and managing groups
- Exercise 4: Creating and managing email and collaboration in Microsoft 365

Day 3 - to configure role delegation to maintain administrative tasks and how to use administrative units in Microsoft 365 to delegate administration.

Module 3 Managing role delegation in Microsoft 365

Lesson 1: Roles and role assignments

- Roles and role groups
- Managing role assignments
- Applying the least privileged concept

Lesson 2: Administrative units

- Overview of administrative units

- Creating and managing administrative units
- Managing role assignments on administrative units
- Examine Privileged Identity Management

Lab Managing roles and permissions in Microsoft 365

- Exercise 1: Configuring roles and role assignments
- Exercise 2: Configuring administrative units
- Exercise 3: Privileged Identity Management

Day 4: ***From Module 3*** **we will** ***learn about the Microsoft Defender and how you can use them to provide security*** ***through advanced threat protection, ensuring that apps, endpoints, and email systems are protected from various types of cyber threats.***

Lesson 3: Security and compliance

- Examine Exchange Online Protection
- Examine Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- What is Secure Score?
- Explore threat intelligence in Microsoft 365 Defender
- Implement app protection by using Microsoft Defender for Cloud Apps
- Implement endpoint protection by using Microsoft Defender for Endpoint
- Implement threat protection by using Microsoft Defender for Office 365

Lab activity:

- Implement a Safe Attachments policy
- Implement a Safe Links policy
- Implement Threat Intelligence

Day 5: From *Module 3 we will learn about Microsoft Purview platforms and how you can use them to manage, protect, and govern data across your organization using Microsoft Purview, while also ensuring compliance with legal and regulatory standards.*

Lesson 3: Security and compliance

- Overview of Microsoft Purview
- Examine data governance solutions in Microsoft Purview
- Explore archiving and records management in Microsoft 365
- Explore retention in Microsoft 365
- Explore Microsoft Purview Data Loss Prevention
- Implement Microsoft Purview Data Loss Prevention

Lab activity: -

- Implement Data Governance
- Implement DLP policy

Day 6: Module 4 helps to learn about Microsoft Entra ID (previously known as Microsoft Azure Active Directory or Azure AD), which is a cloud-based identity and access management solution that provides authentication and authorization when users require access to cloud based resources, such as Microsoft 365

services or Microsoft Defender. We'll learn how to use the Microsoft 365 admin center to manage Entra ID objects and configure settings and functionalities available in Entra ID

Module 4 Managing Entra ID as a directory service for Microsoft 365

Lesson 1: Managing Microsoft 365 objects in Entra ID

- Overview of Entra ID
- Managing user objects and user settings
- Managing external user access
- Managing group objects and group settings
- Managing device objects and device settings
- Managing licenses and self-service sign-up products

Lesson 2: Managing authentication and password options in Entra ID

- Managing MFA and conditional access
- Managing authentication methods
- Managing self-service password reset
- Managing password protection

Lesson 3: Managing integration between AD DS and Entra ID

- Options to integrate authentication with AD DS and Entra ID
- Overview of Entra Connect
- Entra Connect configuration options
- Entra Connect customized synchronization
- Entra Connect Health

- Overview of Entra Cloud Sync

Lab Managing objects and authentication in Entra ID

- Exercise 1: Managing user, group, and device objects in Microsoft Entra ID
- Exercise 2: Configuring self-password reset
- Exercise 3: Enforcing multifactor authentication by using conditional access policy

Module 5 helps to use monitoring and reporting capabilities in Microsoft 365 and Entra ID. You'll also learn how to troubleshoot typical issues in Microsoft 365, and determine what help and support options are available

Module 5 Monitoring and troubleshooting Microsoft 365

Lesson 1: Monitoring and reporting in Microsoft 365

- Overview of Adoption Score
- Usage reports in the Microsoft 365 admin portal
- Health monitoring in the Microsoft 365 admin portal

Lesson 2: Monitoring and health in

- Reviewing Entra ID sign-in logs
- Reviewing Entra ID audit logs
- Integrating Log Analytics

Lesson 3: Troubleshooting Microsoft 365 services

- Overview of typical issues and troubleshooting methods
- Implementing Help & support options

- Managing service requests in Microsoft 365

Lab Monitoring and reporting in Microsoft 365 and Microsoft Entra ID

- Exercise 1: Reviewing usage reports and health by using the Microsoft 365 admin portal
- Exercise 2: Reviewing logs by using the Microsoft Entra admin center