

## MD-101T00 Managing Modern Desktops

### Overview

---

In this course, students will learn how to plan and implement an operating system deployment strategy using modern deployment methods, as well as how to implement an update strategy. Students will be introduced to key components of modern management and co-management strategies. This course also covers what it takes to incorporate Microsoft Intune into your organization. Students will also learn about methods for deployment and management of apps and browser-based applications. Students will be introduced to the key concepts of security in modern management including authentication, identities, access, and compliance policies. Students will be introduced to technologies such as Azure Active Directory, Azure Information Protection and Windows Defender Advanced Threat Protection, as well as how to leverage them to protect devices and data.

### Prerequisite Comments

---

The Modern Desktop Administrator must be familiar with M365 workloads and must have strong skills and experience of deploying, configuring, and maintaining Windows 10 and non-Windows devices. The MDA role focuses on cloud services rather than on-premises management technologies.

### Target Audience

---

The Modern Desktop Administrator deploys, configures, secures, manages, and monitors devices and client applications in an enterprise environment. Responsibilities include managing identity, access, policies, updates, and apps. The MDA collaborates with the M365 Enterprise Administrator to design and implement a device strategy that meets the business needs of a modern organization.

### Course Objectives

---

After completing this course, learners should be able to:

- Plan, develop, and implement an Operating System deployment, upgrade, and update strategy.
- Understand the benefits and methods of co-management strategies.
- Plan and implement device enrollment and configuration.
- Manage and deploy applications and plan a mobile application management strategy.
- Manage users and authentication using Azure AD and Active Directory DS.
- Describe and implement methods used to protect devices and data.

### Course Outline

---

#### 1 - Planning an Operating System Deployment Strategy

The Enterprise Desktop  
Assessing Deployment Readiness  
Deployment Tools & Strategies

## 2 - Implementing Windows 10

Upgrading Devices to Windows 10  
Deploying New Devices and Refreshing  
Migrating Devices to Windows 10  
Alternate Deployment Methods  
Imaging Considerations

## 3 - Managing Updates for Windows 10

Updating Windows 10  
Windows Update for Business  
Introduction to Windows Analytics

## 4 - Device Enrollment

Device management options  
Microsoft Intune Overview  
Manage Intune device enrollment and inventory  
Managing devices with Intune

## 5 - Configuring Profiles

Configuring device profiles  
Managing user profiles  
Monitoring devices

## 6 - Application Management

Implement Mobile Application Management (MAM)  
Deploying and updating applications  
Administering applications

## 7 - Managing Authentication in Azure AD

Azure AD Overview  
Managing identities in Azure AD  
Protecting identities in Azure AD  
Managing device authentication

## 8 - Managing Device Access and Compliance

Microsoft Intune Overview  
Implement device compliance policies

## 9 - Managing Security

Implement device data protection  
Managing Windows Defender ATP  
Managing Windows Defender in Windows 10

---