

# MD-101T00 Managing Modern Desktops

## Course Overview

[View Course Dates & Register Today](#)

This is a 5-day class

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. This three-MOC packaged set aligned to Modern Desktop Exam: Modern Desktop Administrator Part 2 contains courseware that helps prepare students for exam MD-101. Passing this exam, along with exam MD-100, is required to earn the Modern Desktop Administrator certification.

## Who Should Attend

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: - Develop an Operating System deployment and upgrade strategy. - Understand the different methods of deployment. - Understand on-premise and cloud-based solutions. - Deploy and migrate desktops to Windows 10. - Plan and configure Windows Update policies. - Describe the benefits and capabilities of Azure AD. - Manage users using Azure AD with Active Directory DS. - Implement Windows Hello for Business. - Configure conditional access rules based on compliance policies. - Describe the various tools used to secure devices and data. - Implement Windows Defender Advanced Threat Protection.

## Course Outline

### 1 PLANNING AN OPERATING SYSTEM DEPLOYMENT STRATEGY

Overview of Windows as a service  
Windows 10 Deployment options  
Considerations for Windows 10 deployment

### 2 IMPLEMENTING WINDOWS 10

Implementing Windows 10 by using dynamic deployment  
Implementing Windows 10 by using Windows Autopilot  
Upgrading devices to Windows 10

### 3 MANAGING UPDATES FOR WINDOWS 10

Implementing Windows 10 by using dynamic deployment  
Implementing Windows 10 by using Windows Autopilot  
Upgrading devices to Windows 10



[nhls.com](http://nhls.com)



# MD-101T00 Managing Modern Desktops

## 4 DEVICE ENROLLMENT

Device management options  
Manage Intune device enrollment and inventory

## 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  
Enabling corporate access

## 8 MANAGING DEVICES AND DEVICE POLICIES

Microsoft Intune Overview  
Managing devices with Intune  
Implement device compliance policies

## 9 MANAGING SECURITY

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