

IMPLEMENTING AND MANAGING WINDOWS 10

DURATION: **5 DAYS**

COURSE OVERVIEW

This course is designed to provide students with the knowledge and skills required to install and configure Windows 10 desktops and devices in a Windows Server domain corporate environment. These skills include learning how to install and customize Windows 10 operating systems and apps, and configure local and remote network connectivity and storage. Students will also learn how to configure data security, device security, and network security, and maintain, update, and recover Windows 10.

TARGET AUDIENCE

This course is intended for IT professionals who administer and support Windows 10 desktops, devices, users, and associated network and security resources. Students who seek certification in the 70-697 Windows 10 Configuring exam will also benefit from this course. This course is also intended to provide skills for Enterprise Desktop/Device Support Technicians (EDSTs) who provide Tier 2 support to users who run Windows 10 desktops and devices within a Windows domain environment in medium to large enterprise organizations.

COURSE OBJECTIVES

1. Describe the important new features of Windows 10.
2. Install Windows 10.
3. Configure a device running Windows 10.
4. Configure network connectivity for a Windows 10 device.
5. Manage storage in Windows 10.
6. Manage folders and printers.
7. Manage apps.
8. Manage data security.
9. Manage device security.
10. Implement Windows 10 features to improve network security.
11. Monitor and update Windows 10 devices.
12. Restore files, roll back drivers, and recover Windows 10 devices.

COURSE CONTENT

Module 1: Overview of Windows 10

Introducing Windows 10

Navigating the User Interface

Lab: Navigating and Customizing the User Interface

Navigating Windows 10

Configuring the Start Menu

Configuring the Desktop

Module 2: Installing Windows 10

Preparing to Install Windows 10

Upgrading to Windows 10

Lab: Installing Windows 10

Upgrading Windows 7 to Windows 10

Migrating User Settings

Module 3: Configuring Your Device

Overview of Tools Used to Configure Windows 10

Common Configuration Options

Managing User Accounts

Using OneDrive

Lab: Configuring Windows 10

Using Settings

Using Control Panel

Using Windows PowerShell

Using GPOs

Lab: Synchronizing Settings with OneDrive

Connecting a Microsoft Account

Synchronizing Settings between Devices

Module 4: Configuring Network Connectivity

Configuring IP Network Connectivity

Implementing Name Resolution

Implementing Wireless Network Connectivity

Overview of Remote Access

Lab: Configuring Network Connectivity

Configuring IP Settings Manually

Configuring Automatic IP Settings

Configuring DNS Settings

Testing Name Resolution

Module 5: Managing Storage

Overview of Storage Options

Managing Disks, Partitions, and Volumes

Maintaining Disks and Volumes

Managing Storage Spaces

Lab: Managing Storage

Adding a Disk

Creating a Simple Volume

Compressing a Folder

Enabling Disk Quotas

Creating a Storage Space

Module 6: Managing Files and Printers

Overview of File Systems

Configuring and Managing File Access

Configuring and Managing Shared Folders

Work Folders

Managing Printers

Lab: Creating, Securing, and Sharing a Folder

Creating and Securing a Data Folder

Sharing the Data Folder

Lab: Enabling Work Folders

Configuring Work Folders

Lab: Installing and Sharing a Printer

Installing and Sharing a Printer

Module 7: Managing Apps in Windows 10

Overview of Methods Used to Provide Apps to Users

The Windows Store

Web Browsers

Lab: Installing and Updating Apps from the Windows Store

Installing Apps from the Windows Store

Updating Windows Store Apps

Controlling Access to the Windows Store

Side loading an App

Lab: Configuring Windows 10 Web Browsers

Configuring Web Browsers

Module 8: Managing Data Security

Overview of Data-Related Security Threats

Securing Data with EFS

Implementing and Managing BitLocker

Lab: Managing Data Security

Using EFS

Using BitLocker

Module 9: Managing Device Security

Using Security Settings to Mitigate Threats

Configuring User Account Control

Lab: Managing Device Security

Creating Security Policies

Testing Security Policies

Configuring UAC Prompts

Module 10: Managing Network Security

Overview of Network-Related Security Threats

Windows Firewall

Connection Security Rules

Windows Defender

Lab: Managing Network Security

Creating and Testing Inbound Rules

Creating and Testing Outbound Rules

Creating and Testing Connection Security Rules

Configuring Windows Defender

Module 11: Maintaining Windows 10

Updating Windows 10

Monitoring Windows 10

Optimizing Performance

Lab: Maintaining Windows 10

Configuring Updates for a Single Device

Configuring Updates with GPOs

Using the Action Center

Monitoring Events

Monitoring Reliability and Performance

Module 12: Troubleshooting and Recovery

Managing Devices and Drivers

Recovering Files

Recovering Devices

Lab: Troubleshooting and Recovery

Installing an Updated Device Driver

Rolling Back the Device Driver

Using File History to Recover Files

Using Previous Versions to Recover Files

Recovering a Device with a Restore Point

Using the Advanced Start-up Options to Recover a Device

COURSE PREREQUISITES

1. At least two years of experience in the IT field.
2. Knowledge of networking fundamentals, including Transmission Control Protocol /Internet Protocol (TCP/IP), User Datagram
3. Protocol (UDP), and Domain Name System (DNS).
4. Knowledge of Microsoft Active Directory Domain Services (AD DS) principles and fundamentals of AD DS management.
5. Understanding of Windows Server 2008 R2 or Windows Server 2012 fundamentals.
6. Understanding of Microsoft Windows Client essentials; for example, working knowledge of Windows 7, Windows 8 and/or Windows 10.
7. Basic understanding of Windows PowerShell syntax.