20697–1B Installing and Configuring Windows 10

Course Content

Course Description:

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.

Audience Profile:

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.

At Course Completion:

After completing this course, students will be able to:

- Describe the important new features of Windows 10.
- Install Windows 10.
- Configure a device running Windows 10.
- Configure network connectivity for a Windows 10 device.
- Manage storage in Windows 10.
- Manage folders and printers.
- Manage apps.
- Manage data security.
- Manage device security.
- Implement Windows 10 features to improve network security.
- Monitor and update Windows 10 devices.
- Restore files, roll back drivers, and recover Windows 10 devices.

20697–1B Installing and Configuring Windows 10

Course ID#: 1401-600-10-W

Hours: 35

Prerequisites:

Before attending this course, students must have:

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

Topics:

Module 1: Overview of Windows 10

This module introduces the Windows 10 operating system. It describes the new features in Windows 10, and the important changes since Windows 8.1. It describes the use, navigation, and customization of the new, enhanced user interface. This module also mentions the features of Windows 10 that make it beneficial for organizations of different sizes.

Lessons
- Introducing Windows 10
- Navigating the User Interface

Lab: Navigating and Customizing the User Interface
- Navigating Windows 10
- Configuring the Start Menu
- Configuring the Desktop

After completing this module, students will be able to:
- Describe the important new features of Windows 10.
- Navigate and customize the Windows 10 interface.

Module 2: Installing Windows 10

This module introduces the different editions of Windows 10, and the differences between them. It describes the requirements and available options for installing Windows 10 on a device. It also provides instructions on installing Windows 10 and upgrading to it. This module discusses points to consider when deciding between an upgrade or migration to Windows 10, and the supported upgrade paths from older versions of the Windows operating system.

Lessons
- Preparing to Install Windows 10
- Upgrading to Windows 10

Lab: Installing Windows 10
- Upgrading Windows 7 to Windows 10
- Migrating User Settings

After completing this module, students will be able to:
- Describe the different editions of Windows 10 and the features of each.
- Install and upgrade to Windows 10.

Module 3: Configuring Your Device

This module explains how to configure Windows 10 by using tools such as the Settings app, Control Panel, Windows PowerShell, Remote Server Administration Tools (RSAT) and Group Policy Objects (GPOs). It describes the different types of user accounts, and the benefits of using a Microsoft account. This module also describes Microsoft OneDrive, and how it integrates with Windows 10.

Lessons
- 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

After completing this module, students will be able to:
- Describe the use of various tools to configure Windows 10.
- Explain common configuration options.
- Manage user accounts.
- Use OneDrive with Windows 10.

Module 4: Configuring Network Connectivity

This module explains the use of tools such as the Settings app, Network and Sharing Center, and Windows PowerShell to configure network settings. It describes the differences between IPv4 and IPv6 settings, and the benefits of IPv6. It also describes name resolution and provides an overview of the Domain Name System (DNS) service. This module describes the configuration of wireless connectivity in Windows 10, and explains remote access methods available in Windows 10, such as Virtual Private Networks (VPNs), DirectAccess, and Remote Desktop.

Lessons
- 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

After completing this module, students will be able to:
- Describe how to configure IP network connectivity.
- Implement name resolution.
- Implement wireless network connectivity.
- Describe options for remote access in Windows 10.

Module 5: Managing Storage

This module provides an overview of storage options such as hard disks, server-based storage, and virtual hard disks. It describes network storage options such as Network Attached Storage (NAS) and Storage Area Network (SAN), and cloud-based storage options such as OneDrive and Azure Storage. This module describes the management and maintenance of disks, partitions, and volumes. It also describes the Storage Spaces feature, and the process of configuring it.

Lessons
- 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

After completing this module, students will be able to:
- Explain the different storage options in Windows 10.
- Manage disks, partitions, and volumes.
- Maintain disks, partitions, and volumes.
- Manage Storage Spaces.

Module 6: Managing Files and Printers

This module provides an overview of the file systems supported by Windows 10. It explains how to configure file permissions, the effect of file permissions, how explicit and inherited permissions work, and how to include user and device claims in access permissions. This module also explains how to share folders, the tools to use for sharing a folder, and the effective permissions when a user tries to access data in a shared folder that is protected by file permissions. The last lesson in the module describes how to add and share a printer, and how to manage client and server side printing.

Lessons
- 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

After completing this module, students will be able to:
- Describe and create file systems that are supported by Windows 10.
- Configure file permissions and limit access to files and folders.
- Configure and manage shared folders.
- Create and use Work Folders.
- Configure and manage printers.

Module 7: Managing Apps in Windows 10

This module describes how to install and configure both desktop apps and Windows Store apps in Windows 10. It explains how to install apps manually and automatically, and how to use Microsoft Systems Center Configuration Manager and Microsoft Intune to deploy apps. It describes the Windows Store, and how to manage access to it. This module also describes the Internet Explorer 11 and Edge browsers, and explains how to configure and manage both.

Lessons

- 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
- Sideloading an App

Lab: Configuring Windows 10 Web Browsers

- Configuring Web Browsers

After completing this module, students will be able to:
- Describe app deployment options in Windows 10.
- Install and manage Windows Store apps.
- Configure Windows 10 web browsers.

Module 8: Managing Data Security

This module explains how the technologies available with Windows 10 work together to protect against data-related security threats. It provides an overview of these threats, and discusses possible mitigations and best practices for dealing with them. It describes defense-in-depth and Encrypting File System (EFS), and their usage in countering security threats. This module also describes how to configure, administer, and monitor BitLocker.

Lessons

- Overview of Data-Related Security Threats
- Securing Data with EFS
- Implementing and Managing BitLocker

Lab: Managing Data Security

- Using EFS
- Using BitLocker

After completing this module, students will be able to:
- Explain data-related security threats.
- Secure data with EFS.
- Implement and manage BitLocker.

Module 9: Managing Device Security

This module explains how to mitigate security threats with the use of Security Compliance Manager, Enhanced Mitigation Experience Toolkit, and security settings in GPOs. It also describes User Account Control (UAC), and how to configure it.

Lessons

- Using Security Settings to Mitigate Threats
- Configuring User Account Control

Lab: Managing Device Security
- Creating Security Policies
- Testing Security Policies
- Configuring UAC Prompts

After completing this module, students will be able to:
- Use security settings to mitigate threats.
- Configure user account control.

Module 10: Managing Network Security
This module describes common network-related security threats, and describes options to mitigate them. It describes Windows Firewall, IPsec connection security rules, and Windows Defender, and how to configure these tools to manage network security.

Lessons
- 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

After completing this module, students will be able to:
- Describe network-related security threats and options for mitigating them.
- Use Windows Firewall to mitigate security threats.
- Configure IPsec connection security rules.
- Use Windows Defender to protect devices from network-related threats.

Module 11: Maintaining Windows 10
This module describes Windows Update, and Windows Update for Business, and how to configure settings for updates. It describes how to use Windows Server Update Services (WSUS), Configuration Manager, or Intune to distribute updates within organizations. This module also explains how to use the Action Center, Event Viewer, and Performance Monitor in Windows 10.

Lessons
- 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

After completing this module, students will be able to:
- Explain how to update Windows 10.
- Monitor Windows 10.
- Optimize Windows 10 performance.

Module 12: Troubleshooting and Recovery
This module describes device drivers, and how to use the Device Manager to view, configure, update, and roll back device drivers. It explains file recovery methods in Windows 10, such as Backup and Restore, File History, and Previous Versions. This module also explains features such as System Restore, Startup Recovery, and System Image Recovery, and describes how to use restore points to roll back device configuration.

20697–1B Installing and Configuring Windows 10

Course ID#: 1401-600-10-W

Hours: 35

Lessons

- 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

After completing this module, students will be able to:

- Describe and manage device drivers.
- Configure file recovery and revert to previous versions of files.
- Use device recovery features in Windows 10.