

Microsoft MCSA: Windows 10 Certification Training Course

Course Length: 10 days (virtual)

[Click here to view the current class schedule!](#)

Overview:

Prove you have the expertise to configure, manage, and maintain a Windows 10 enterprise system.

Microsoft Course 20698: This course provides IT professionals with the knowledge and skills required to install and configure Windows 10 desktops in a Windows Server small to medium-sized AD DS domain environment.

Microsoft Course 20697-2: This course provides administrators with the knowledge and skills needed to deploy and manage Windows 10 desktops, devices, and applications in an enterprise environment. Students learn how to plan and implement Windows 10 deployments in large organizations.

Microsoft Course 20698

This instructor-led course provides IT professionals with the knowledge and skills required to install and configure Windows 10 desktops in a Windows Server small to medium-sized AD DS domain environment. These skills include learning how to install and customize Windows 10 operating systems and apps, configure local and remote network connectivity, and configure local and online storage. Students also will learn how to configure security in addition to how to maintain, update, and recover Windows 10.

Audience profile

This course is intended for IT professionals who administer and support Windows 10 desktops and devices in small to medium-sized networks.

The networks with which these professionals typically work are configured as AD DS domain-based environments with managed access to the Internet and cloud services.

Students who seek certification in **Exam 70-698: Installing and Configuring Windows 10** also will benefit from this course. In addition, this course is intended to provide skills for Enterprise Desktop/Device Support Technicians (EDSTs) who work in small to medium-sized organizations, and who provide Tier 1 or Tier 2 support to users running Windows 10 desktops and devices within a Windows domain environment.

At course completion

After completing this course, students will be able to:

- Plan, install, and upgrade to Windows 10.
- Perform post-installation configuration.
- Implement networking.
- Implement network security.
- Manage Windows 10 with Group Policy.
- Implement remote management.

- Manage local storage.
- Manage files and resources.
- Install and manage apps.
- Secure Windows 10.
- Implement remote connectivity.
- Maintain and update Windows 10.
- Recover and troubleshoot Windows 10.

Prerequisites

Before attending this course, students must have:

- Experience deploying and configuring Windows 8, Windows 8.1, or Windows 10.
- Experience deploying and configuring Windows Server 2012 or Windows Server 2016 Active Directory Domain Services (AD DS).
- Experience deploying and configuring network services, including DNS, in Windows Server 2012 or Windows Server 2016.
- Windows Client essentials, such as a working knowledge of Windows 8.1, Windows 8, or Windows 7.

Course Outline

Module 1: Installing Windows 10

This module describes the features of Windows 10 and the process for installing and deploying it. The module also describes how to upgrade to Windows 10, perform post-installation maintenance tasks, and manage volume activation.

- Overview of Windows 10
- Planning your Windows 10 deployment
- Installing and deploying Windows 10
- Upgrading to Windows 10
- Windows 10 installation maintenance
- Managing volume activation

After completing this module, students will be able to:

- Describe the features and editions of Windows 10.
- Plan to deploy Windows 10.
- Install and deploy Windows 10.
- Upgrade to Windows 10.
- Maintain Windows 10 installations.
- Manage Windows 10 activation.

Module 2: Performing post-installation configuration

This module provides an overview of the management tools in Windows 10. It describes how to customize the user interface, manage devices, drivers, and services, and configure several other features. The module also provides an overview of Client Hyper-V.

- Overview of management tools
- Customizing the user interface
- Managing devices, device drivers, and services
- Configuring features, mobility, and power options
- Overview of Client Hyper-V

After completing this module, students will be able to:

- Describe the different tools that you can use to configure Windows 10.
- Explain how to navigate and customize the user interface.
- Manage device drivers.
- Configure Windows features, mobility options, and power settings.
- Describe Client Hyper-V.

Module 3: Implementing networking

This module describes the homegroups, workgroups, and domains feature in Windows 10. It also describes how to configure IPv4 and IPv6 network connectivity, and how to implement name resolution. Additionally, the module describes how to troubleshoot network connectivity and implement wireless network connectivity.

- Homegroups, workgroups, and domains
- Configuring IPv4 network connectivity
- Configuring IPv6 network connectivity
- Implementing name resolution
- Troubleshooting network connectivity
- Implementing wireless network connectivity

After completing this module, students will be able to:

- Describe homegroups, workgroups, and domains.
- Describe how to configure IPv4 network connectivity.
- Describe how to configure IPv6 network connectivity.
- Implement name resolution.
- Troubleshoot network connections.
- Implement wireless network connectivity.

Module 4: Implementing network security

This module describes how to implement network security by using the Windows 10 features such as Windows Firewall, connection security rules, and Windows Defender.

- Implementing Windows Firewall
- Connection security rules
- Implementing Windows Defender

After completing this module, students will be able to:

- Describe Windows Firewall.
- Understand rules regarding connection security.
- Manage Windows Defender

Module 5: Managing Windows 10 with Group Policy

This module describes how to implement the Group Policy feature in Windows 10. The module also explains how you can configure Windows 10 devices by using Group Policy Objects (GPOs).

- Overview of Group Policy
- Configuring Windows 10 devices with GPOs

After completing this module, students will be able to:

- Describe Group Policy processing and management.
- Configure common settings for users and desktops by using Group Policy.

Module 6: Implementing remote management

This module describes how to implement remote management by using Windows 10 features such as Remote Desktop, Remote Assistance, and remoting with Windows PowerShell.

- Using Remote Desktop
- Using Remote Assistance
- Remoting with Windows PowerShell

After completing this module, students will be able to:

- Use Remote Desktop to manage remote computers.
- Use Windows Remote Assistance to manage remote computers.
- Use Windows PowerShell remoting to manage remote computers.

Module 7: Managing storage

This module describes how to manage storage in Windows 10 devices by using the available storage options. It also explains how to manage and maintain disks, partitions, and volumes. The modules then describes how you can use the Storage Spaces feature, Microsoft OneDrive, and virtual hard disks to manage storage.

- Overview of storage options
- Managing disks, partitions, and volumes
- Maintaining disks and volumes
- Implementing Storage Spaces
- Implementing and managing OneDrive
- Working with virtual hard disks

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.
- Explain how to implement Microsoft OneDrive.
- Explain how to implement virtual hard disks.

Module 8: Managing files and resources

This module describes how to manage files and resources in Windows 10. The module starts by providing an overview of file systems and how file access works. The module then describes shared folders and Work Folders features. Finally, it describes how to manage printers.

- Overview of file systems
- Configuring and managing file access
- Managing shared folders
- Implementing Work Folders
- Managing printers

After completing this module, students will be able to:

- Describe the file systems that Windows 10 supports.
- Configure and manage file permissions.
- Create and manage share folders.
- Create and use Work Folders.
- Configure and manage printers

Module 9: Deploying and managing apps

This module describes the various methods available to deploy and manage apps in Windows 10. The module provides an overview of the Windows Store and Windows Store for Business, and describes other options such as desktop apps and web browsers.

- Overview of apps in Windows 10
- The Windows Store and Windows Store for Business
- Automating app deployment
- Configure web browsers

After completing this module, students will be able to:

- Describe the available app types in Windows 10.
- Describe the Windows Store and Windows Store for Business.
- Deploy and manage Windows Store apps.
- Automate app deployment.
- Configure Windows 10 web browsers.

Module 10: Securing Windows 10

This module describes how to implement security in Windows 10 devices. It also describes how to manage user accounts and their permissions by using the User Account Control (UAC) feature. Additionally, the module explains how to implement and manage BitLocker Drive Encryption.

- Managing user accounts
- Configuring UAC
- Implementing and Managing BitLocker

After completing this module, students will be able to:

- Manage user accounts.
- Configure User Account Control (UAC).
- Implement and manage BitLocker drive encryption

Module 11: Implementing remote connectivity

This module describes how to implement remote connectivity by using the available options, including virtual private networks (VPNs) and DirectAccess.

- Overview of remote connectivity options
- Implementing VPNs
- Implementing DirectAccess

After completing this module, students will be able to:

- Describe remote connectivity options in Windows 10.
- Implement virtual private networks (VPNs) in Windows 10.
- Describe how to implement DirectAccess.

Module 12: Maintaining Windows 10

This module describes how maintain a Windows 10 environment by updating and monitoring the Windows 10 operating system. The module describes the Windows Update settings and how to use the Windows Server Update Services (WSUS), Microsoft System Center Configuration Manager, and Microsoft Intune to regularly update Windows 10. The module then explains how to monitor Windows 10 by using tools such as the Notifications & actions settings, Event Viewer, and Windows Performance Monitor.

- Updating Windows 10
- Monitoring Windows 10

After completing this module, students will be able to:

- Explain how to keep Windows 10 up to date.
- Monitor Windows 10.

Module 13: Recovering Windows 10

This module describes the recovery options for Windows 10. It also explains how to recover lost files, manage devices and device drives, and perform system recovery.

- Recovering files
- Performing system recovery

After completing this module, students will be able to:

- Configure file recovery and revert to previous versions of files.
- Describe and use system recovery features in Windows 10.

Microsoft Course 20697-2

Exam 70-697: This course provides administrators with the knowledge and skills needed to deploy and manage Windows 10 desktops, devices, and applications in an enterprise environment. Students learn how to plan and implement Windows 10 deployments in large organizations. Students also learn how to manage the Windows 10 installations after deployment to provide secure identity and data access using technologies related to Group Policy, Remote Access, and Device Registration. To support a variety of device and data management solutions, Microsoft Azure Active Directory, Microsoft Intune, and Microsoft Azure Rights Management are introduced. These services are part of the Enterprise Mobility Suite which provide identity and access management, cloud-based device, application, and update management, and secure data access to information stored both in the cloud and on any location within your corporate network.

Audience profile

This course is intended for IT Professionals who are interested in specializing in Windows 10 desktop and application deployments and managing the cloud-based application and data service environments for medium-to-large enterprise organizations. These professionals typically work with networks that are configured as Windows Server domain-based environments with managed access to the Internet and cloud services.

This course is also intended to provide skills for individuals who seek to pass the 70-697 Windows 10 Configuring exam.

At course completion

After completing this course, students will be able to:

- Describe the challenges and solutions for desktop and device management in an enterprise environment.
- Deploy Windows 10 Enterprise desktops.
- Manage user profiles and user state virtualization.
- Manage Windows 10 sign-in and identity.
- Manage desktop and application settings by using Group Policy.
- Manage data access for Windows-based devices.
- Manage remote access solutions.
- Configure and manage client Hyper-V.
- Manage Windows 10 devices by using enterprise mobility solutions.
- Manage desktop and mobile clients by using Microsoft Intune.
- Manage updates and endpoint protection by using Microsoft Intune.
- Manage application and resource access by using Microsoft Intune.

Prerequisites

Before attending this course, students should have:

- **Attended Microsoft Course 20697-1, OR Microsoft Course 20698, OR have equivalent knowledge.**
- At least two years of experience in the IT field.
- Basic awareness of Windows deployment tools.

Course Outline

Module 1: Managing Desktops and Devices in an Enterprise Environment

This module explains the most current trends and information related to desktop and device management in the enterprise. It also provides an overview on how to extend device management to the cloud.

- Managing Windows 10 in the Enterprise
- Managing a Mobile Workforce
- Supporting Devices in the Enterprise
- Extending IT Management and Services to the Cloud

After completing this module, students will be able to:

- Manage Windows 10 in the enterprise.
- Manage a mobile workforce.
- Support devices in the enterprise.
- Extend IT management and services to the cloud.

Module 2: Deploying Windows 10 Enterprise Desktops

This module explains the various deployment scenarios of Windows 10 and the considerations to keep in mind while performing these deployments. This module also explains how to deploy Windows 10 by using the Windows Assessment and Deployment Kit (WADK) and the Microsoft Deployment Toolkit (MDT). This module also explains how to maintain Windows 10 by using DISM and Windows Imaging and Configuration Designer (ICD).

- Overview of Windows 10 Enterprise Deployment
- Customizing Enterprise Desktop Deployments
- Deploying Windows 10 by Using the Microsoft Deployment Toolkit
- Maintaining a Windows 10 Installation
- Managing Volume License Activation for Windows 10

After completing this module, students will be able to:

- Describe the deployment options for Windows 10 desktops.
- Customize enterprise desktop deployments.
- Deploy Windows 10 by using the Microsoft Deployment Toolkit.
- Maintain a Windows 10 installation.
- Manage volume license activation for Windows 10.

Module 3: Managing User Profiles and User State Virtualization

This module explains user states and user state virtualization and explains how to deploy and maintain user experience virtualization (UE-V). This module also explains how to use tools such as ScanState and LoadState to migrate user states.

- Managing User Profile and User State
- Implementing User State Virtualization by Using Group Policy
- Configuring User Experience Virtualization
- Managing User State Migration

After completing this module, students will be able to:

- Manage user profile and user state.

- Implement user state virtualization by using Group Policy.
- Configure UE-V.
- Manage user state migration.

Module 4: Managing Windows 10 Sign-In and Identity

This module explains the concept of identity and the methods to enhance identity security. This module also explains cloud identities and the use of Azure Active Directory Premium in enterprise organizations.

- Overview of Enterprise Identity
- Planning for Cloud Identity Integration

After completing this module, students will be able to:

- Describe the concept of enterprise identity.
- Plan for cloud identity integration.

Module 5: Managing Desktop and Application Settings by Using Group Policy

This module explains how to manage Group Policy inheritance, administrative templates, and common enterprise desktop settings. This module also explains how to apply policies using targeting and filtering.

- Managing Group Policy Objects
- Configuring Enterprise Desktops Using Group Policy
- Overview of Group Policy Preferences

After completing this module, students will be able to:

- Manage Group Policy objects.
- Configure enterprise desktops by using Group Policy.
- Describe Group Policy preferences.

Module 6: Managing Data Access for Windows-based Devices

This module explains how to implement Device Registrations and Work Folders. This module also explains how to configure and share data stored in Microsoft OneDrive.

- Overview of Data Access Solutions
- Implementing Device Registration
- Implementing Work Folders
- Managing Online Data Using Cloud-Based Storage Solutions

After completing this module, students will be able to:

- Describe the solutions for accessing data.
- Implement Device Registration.
- Implement Work Folders.
- Manage online data by using cloud-based storage solutions.

Module 7: Managing Remote Access Solutions

This module explains how to configure a virtual private network (VPN) and DirectAccess in Windows 10. This module also explains how to publish applications in Microsoft Azure RemoteApp.

- Overview of Remote Access Solutions
- Configuring VPN Access to Remote Networks
- Using DirectAccess with Windows 10
- Supporting RemoteApp

After completing this module, students will be able to:

- Describe the types of remote access solutions.
- Configuring VPN access to remote networks.
- Use DirectAccess with Windows 10.
- Support RemoteApp.

Module 8: Configuring and Managing Client Hyper-V

This module explains how to create virtual switches, virtual hard disks, and virtual machines.

- Installing and Configuring Client Hyper-V
- Configuring Virtual Switches
- Creating and Managing Virtual Hard Disks
- Creating and Managing Virtual Machines

After completing this module, students will be able to:

- Install and configure client Hyper-V.
- Configure virtual switches.
- Create and manage virtual hard disks.
- Create and manage virtual machines.

Module 9: Managing Windows 10 Devices Using Enterprise Mobility Solutions

This module explains the use of the Enterprise Mobility Suite and its components, Azure Active Directory Premium, Azure Rights Management, and Microsoft Intune.

- Overview of the Enterprise Mobility Suite
- Overview of Azure Active Directory Premium
- Overview of Azure Rights Management
- Overview of Microsoft Intune

After completing this module, students will be able to:

- Describe the use and components of the Enterprise Mobility Suite.
- Manage directory services by using Azure Active Directory Premium.
- Protect devices by using Azure Rights Management.
- Explore the options in Microsoft Intune.

Module 10: Managing Desktop and Mobile Clients Using Microsoft Intune

This module explains how to configure and assign configuration policies. This module also explains how to create Mobile Device Management (MDM) policies and enroll mobile devices to Intune.

- Deploying the Intune Client Software
- Overview of Microsoft Intune Policies
- Mobile Device Management Using Intune

After completing this module, students will be able to:

- Deploying the Intune client software.
- Configure Intune policies.
- Manage mobile devices using Intune.

Module 11: Managing Updates and Endpoint Protection Using Microsoft Intune

This module explains how to configure updates and Endpoint Protection settings and reports.

- Managing Updates Using Microsoft Intune
- Managing Endpoint Protection

After completing this module, students will be able to:

- Manage updates by using Intune.
- Manage Endpoint Protection.

Module 12: Application and Resource Access Using Microsoft Intune

This module explains how to use the Microsoft Intune Software Publisher and deploy applications to managed clients. This module also explains the use of certificate profiles, Wi-Fi profiles, and VPN profiles to control access to company resources.

- Overview of Application Management Using Intune
- The Application Deployment Process
- Controlling Access to Company Resources

After completing this module, students will be able to:

- Describe application management by using Intune.
- Describe the application deployment process.
- Control access to company resources.