Device Configuration and Management

Candidates for this exam have fundamental knowledge of computer hardware, connections, operation, and management. Candidates should have hands-on experience with Windows 10 or Windows 11 installation and configuration, network connections, application and peripheral device management, data access and management, and basic device security in a Windows business environment. Candidates should have at least 150 hours of instruction or hands-on experience with Windows device configuration and management.

1. Windows Installation and Configuration

1.1 Recognize basic computer components and explain their functions, including:

- RAM
- CPU/APU (x86 [32-bit and 64-bit], ARM)
- Graphics Card
- Physical Storage
- Motherboard

1.2 Describe the purpose of Active Directory services, including:

- Domain user account
- Domain administrator account
- Centralized management of users, computers, and groups
- Group policy
- Differentiate between local and group security policies and precedence

1.3 Install Windows using the default settings

- Time zone options, Microsoft account vs. local account, upgrade vs. custom install
- Installation scenarios include domain-joined and non-domain-joined computers.

1.4 Configure user account options

- User account (Microsoft, Domain, or local)
- Standard user and administrative account types,
- User profiles

1.5 Configure desktop settings

- Start menu
- Display settings
- Application shortcuts
- Time zone settings
- Taskbar settings
- Power settings
- Window management (minimize, close, snap)

INFORMATION TECHNOLOGY SPECIALIST

1.6 Configure accessibility settings to meet user's specific needs

- Mouse settings
- Color filters
- Contrast themes
- Audio settings
- Magnifier
- Narrator
- Sticky Keys
- On-screen keyboard
- Voice Access
- Voice Typing (dictation)
- Text cursor
- Eye control
- Live captions

1.7 Manage updates

- Windows Update settings
- Software updates and patches
- Optional OS updates
- Device driver updates (Microsoft and manufacturer)
- Update history

2. Windows Feature, Application and Peripheral Management

2.1 Manage applications and Windows features

- Identify user account requirements and permissions for application installation
- Modify application installations
- Remove desktop applications
- Locate and identify optional Windows features
- Describe the purpose of the Microsoft Store
- Understand default locations for applications based on architecture
- Remote Desktop

2.2 Explain the purpose and capabilities of Windows Copilot (Windows 11 Only)

- Direct users to troubleshooting tools within Windows 11
- Can open applications, access settings, generate content, translate text into different languages, generate programming code and retrieve information.
- Installed with Windows 11 by default
- Limitations of Copilot

2.3 Describe the purpose of the Windows Registry

- Database of user preferences, application settings, Windows settings

2.4 Compare and contrast capabilities of peripheral connection types

- HDMI (full, mini and micro)
- DisplayPort (full, mini)
- DVI family of connectors
- VGA
- USB-A, mini-A, micro-A, 3.0
- USB-B, mini-B, micro-B, 3.0
- USB-C
- Thunderbolt
- S/PDIF Optical
- Aux audio cable
- Converting between the various connection types

2.5 Configure projection and display properties

- Wireless casting
- Orientation
- Duplicating vs. extending
- Resolution and aspect ratio
- ClearType

3. Data Access and Management

3.1 Describe cloud services

- Cloud storage and collaboration concepts
- Identify common cloud storage and service providers, such as Azure, Microsoft 365 (to include but not limited to: SharePoint, OneDrive, Outlook, Teams, Windows 365)
- File sharing capabilities and permissions
- Offline file synchronization
- Describe and configure storage
- Understand when and why to use partitioning
- Partition and format a drive.
- Choose a file system to use when formatting the drive (NTFS, FAT32, and exFAT)
- Configure File and folder attributes
- Identify the effect on permissions and attributes when copying or moving data between file systems
- GPT and MBR partition style

3.2 Describe and configure local and network file sharing and permissions

- File and share permissions
- Effective permissions
- Basic and advanced permissions
- Public, basic, and advanced shares
- Map drives
- Describe taking ownership of files or folders

3.3 Manage backup and restore of user files and states

- Set file versioning/history settings
- Perform a full disk backup to the cloud
- Perform a full disk restore
- Restore previous versions of files

4. Device Security

4.1 Configure Windows Defender Firewall settings

- Allow an application or feature through the Windows Defender Firewall
- Compare and contrast private, public, and guest network profiles
- Turn firewall off and on (for troubleshooting)

4.2 Describe user authentication and configure Windows sign-in options

- Multifactor authentication (theory, how it works)
- Biometric authentication methods
- Windows Hello (Windows 11 only)
- Configure Windows sign-in options
- What makes a password “strong”
- Authenticator apps

4.3 Describe various security threats

- Computer viruses (worms, trojan horse, logic bombs, ransomware)
- Adware
- Spyware
- Denial of Service (DoS) attacks
- Social engineering attacks (to include, but not limited to Phishing, smishing, vishing, dumpster diving, spoofing, and clone phishing)
- Physical attacks (errant thumb drives, theft, shoulder surfing, screen scrapers)

4.4 Describe how to respond to various malware and social engineering attacks

- Computer viruses
- Adware
- Spyware
- Phishing
- Physical attacks (errant thumb drives)
- Antimalware program configuration options
- Analyze Antimalware scan results

4.5 Manage User Account Control (UAC) settings

- Describe the function of UAC
- Identify appropriate UAC settings for specific purposes
- Elevate permissions in UAC

5. Windows Management and Troubleshooting

5.1 Perform troubleshooting tasks

- Locate and identify Windows troubleshooting tools (such as event viewer, task manager, defragment and optimize drive)
- Gather data to describe issues and support troubleshooting
- Research how to remedy issues
- Identify when to escalate issues
- Force group policy application (gpupdate /force, gpresult)
- Recognize that an applied policy could cause a problem

5.2 Troubleshoot operating system and application issues

- Reset or roll back the operating system
- Advanced startup (System repair)
- Features of safe mode
- Use troubleshooting tools to identify application compatibility issues
- Resolve Store app installation issues
- Reinstall or repair desktop applications
- Escalate problems dealing with 'S' mode
- Troubleshoot services
- Use Task Manager to disable a startup app, end a task, manage a service

5.3 Manage and troubleshoot hardware and peripherals

- Hardware troubleshooting methods (connections, ports, power)
- Update or roll back drivers
- Uninstall or reinstall a device to reconfigure drivers
- Describe the purpose and capabilities of Device Manager and Disk Management
- Manage and troubleshoot peripheral device connections
  - Keyboard, mouse, display, headset, microphone, camera, local and network storage devices, printers, scanners, connection cables, Bluetooth

5.4 Manage and troubleshoot device connections to networks and domains

- Wired and wireless connections (Ethernet cable, wireless signal strength, SSID, ipconfig options [flushdns, release, renew, all], security key), ping, traceroute, nmap
- Remove or Join devices to domains