

Introduction to Information Technology

IT Specialist: Device Configuration and Management

Introduction to Information Technology is aligned to the skills assessed in Certiport's **Device Configuration and Management Exam**. The following includes the Exam Objectives covered on the certification exam and the correlating page(s) in which the objectives are taught.

Obj Number	Description	Chapter/Page Number(s)
1. Windows Installation and Configuration		
1.1	Recognize basic computer components and explain their functions, including:	
	<ul style="list-style-type: none"> • RAM • CPU/APU (x86 [32-bit and 64-bit], ARM) • Graphics Card • Physical Storage • Motherboard 	Ch. 2, p. 29-39 Basic Hardware Components, Inside the Computer Case
1.2	Describe the purpose of Active Directory services, including:	
	<ul style="list-style-type: none"> • Domain user account • Domain administrator account • Centralized management of users, computers, and groups • Group policy • Differentiate between local and group security policies and precedence 	Ch. 4, p. 92-96 Active Directory Services; Ch. 9, p. 193-194 Group Policy Management
1.3	Install Windows using the default settings	
	<ul style="list-style-type: none"> • Time zone options, Microsoft account vs. local account, upgrade vs. custom install • Installation scenarios include domain-joined and non-domain-joined computers 	Ch. 3, p. 65-71 Preparing to Install the Windows Operating System, Performing the Windows 11 Installation
1.4	Configure user account options	
	<ul style="list-style-type: none"> • User account (Microsoft, Domain, or local) • Standard user and administrative account types • User profiles 	Ch. 3 p. 70-75 Configuring User Accounts and Settings; Ch. 4, p. 92-96 Active Directory Services
1.5	Configure desktop settings	
	<ul style="list-style-type: none"> • Start menu • Display settings • Application shortcuts • Time zone settings • Taskbar settings • Power settings • Window management (minimize, close, snap) 	Ch. 4, p. 79-84 Desktop Settings and Customization
1.6	Configure accessibility settings to meet user's specific needs	
	<ul style="list-style-type: none"> • 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 	Ch. 4, p. 84-88 Accessibility Features
1.7	Manage updates	
	<ul style="list-style-type: none"> • Windows Update settings • Software updates and patches • Optional OS updates • Device driver updates (Microsoft and manufacturer) • Update history 	Ch. 4, p. 89-92 Updating and Patching Windows 11; Ch. 5, p. 115-116 Updating and Managing Apps and Microsoft Store Apps vs. Desktop Applications

Obj Number	Description	Chapter/Page Number(s)
2. Windows Feature, Application and Peripheral Management		
2.1	Manage applications and Windows features	
	<ul style="list-style-type: none"> 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 	Ch. 5, p. 112-116 Using Windows Application Features, The Microsoft Store, p. 118-120 Default Locations for Applications; Ch. 7, p. 159-160 Remote Desktops
2.2	Explain the purpose and capabilities of Windows Copilot (Windows 11 Only)	
	<ul style="list-style-type: none"> 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 	Ch. 5, p. 116 Troubleshooting Using Windows Copilot
2.3	Describe the purpose of the Windows Registry	
	<ul style="list-style-type: none"> Database of user preferences, application settings, Windows settings 	Ch. 4, p. 97-99 Understanding the Windows Registry
2.4	Compare and contrast capabilities of peripheral connection types	
	<ul style="list-style-type: none"> 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 	Ch. 2, p. 44-48 Peripheral Connection Types
2.5	Configure projection and display properties	
	<ul style="list-style-type: none"> Wireless casting Orientation Duplicating vs. extending Resolution and aspect ratio ClearType 	Ch. 4, p. 81-82 Display Settings
3. Data Access and Management		
3.1	Describe cloud services	
	<ul style="list-style-type: none"> 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 	Ch. 3, p. 69 Partition the Hard Drive; Ch. 9, p. 200-202 File and Folder Encryption; Ch. 10, p. 227-238 Cloud Services, Configuring Storage and File Sharing
3.2	Describe and configure local and network file sharing and permissions	
	<ul style="list-style-type: none"> File and share permissions Effective permissions Basic and advanced permissions Public, basic, and advanced shares Map drives Describe taking ownership of files or folders 	Ch. 3, p. 72-73 User Permissions; Ch. 4, p. 92-96 Active Directory Services; Ch. 10, p. 234-238 Configuring Storage and File Sharing
3.3	Manage backup and restore of user files and states	
	<ul style="list-style-type: none"> Set file versioning/history settings Perform a full disk backup to the cloud Perform a full disk restore Restore previous versions of files 	Ch. 10, p. 239-244 Backup and Restore Strategies

Obj Number	Description	Chapter/Page Number(s)
4. Device Security		
4.1	Configure Windows Defender Firewall settings	
	<ul style="list-style-type: none"> • 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) 	Ch. 8, p. 181-182 Firewalls; Ch. 9, p. 210-211 Installing Antimalware Software
4.2	Describe user authentication and configure Windows sign-in options	
	<ul style="list-style-type: none"> • 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 	Ch. 3, p. 64-65 Windows 10 vs. Windows 11; Ch. 9, p. 195-199 User Authentication
4.3	Describe various security threats	
	<ul style="list-style-type: none"> • 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) 	Ch. 9, p. 205-209 Identifying and Preventing Attacks
4.4	Describe how to respond to various malware and social engineering attacks	
	<ul style="list-style-type: none"> • Computer viruses • Adware • Spyware • Phishing • Physical attacks (errant thumb drives) • Antimalware program configuration options • Analyze Antimalware scan results 	Ch. 9, p. 208-213 Responding to Phishing and Physical Attacks, Antivirus and Antimalware Software
4.5	Manage User Account Control (UAC) settings	
	<ul style="list-style-type: none"> • Describe the function of UAC • Identify appropriate UAC settings for specific purposes • Elevate permissions in UAC 	Ch. 9, p. 194-195 UAC Settings and Secure DNS Updates
5. Windows Management and Troubleshooting		
5.1	Perform troubleshooting tasks	
	<ul style="list-style-type: none"> • 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 	Ch. 4, p. 99-101 Troubleshooting OS Issues; Ch. 9, p. 193-194 Group Policy Management; Ch. 11, p. 264-274 Tools and Utilities, Advanced Troubleshooting Techniques, Escalating IT Issues
5.2	Troubleshoot operating system and application issues	
	<ul style="list-style-type: none"> • 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 	Ch. 4, p. 99-101 Troubleshooting OS Issues; Ch. 5, p. 116-118 Troubleshooting Using Windows Copilot; Ch. 11, p. 268-271 Advanced Troubleshooting Techniques
5.3	Manage and troubleshoot hardware and peripherals	
	<ul style="list-style-type: none"> • 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 	Ch. 2, p. 44-48 Peripheral Connection Types; Ch. 4, p. 90-91 Device Driver Updates; Ch. 11, p. 264-267 Tools and Utilities
5.4	Manage and troubleshoot device connections to networks and domains	
	<ul style="list-style-type: none"> • 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 	Ch. 7, p. 162-164 Command-Line Tools; Ch. 9, p. 215 Network Identification Settings; Ch. 11, p. 264-267 Tools and Utilities

Introduction to Information Technology IT Specialist: Networking

Introduction to Information Technology is aligned to the skills assessed in Certiport's **Networking Exam**. The following includes the Exam Objectives covered on the certification exam and the correlating page(s) in which the objectives are taught.

Obj Number	Description	Chapter/Page Number(s)
1. Networking Fundamentals		
1.1	Define network concepts	
	<ul style="list-style-type: none"> Internet, intranet, extranet, client-server, peer-to-peer, transmission types (unicast, multicast, broadcast), network devices including IoT 	Ch. 6, p. 129-133 Introduction to Networking, p. 141-143 Networking Devices; Ch. 7, p. 154-157 Wireless Networking
1.2	Define cloud and virtualization concepts	
	<ul style="list-style-type: none"> Hypervisors, virtual machines, virtual switches 	Ch. 6, p. 137 Virtualization in Networks; Ch. 10 p. 230-232 Hosted Virtual Machines
1.3	Describe remote access methods	
	<ul style="list-style-type: none"> Virtual Private Network (VPN), Remote Desktop 	Ch. 7, p. 158-160 Remote Access Methods; Ch. 9, p. 198 Remote Access
2. Network Infrastructures		
2.1	Define the characteristics of local area networks (LANs)	
	<ul style="list-style-type: none"> Perimeter networks (security zones, DMZ), VLANs, wired LAN and wireless LAN 	Ch. 6, p. 134 LAN Characteristics, p. 141 Switches; Ch. 8, p. 176-177, Honeynets & Perimeter Networks, p. 179-180 VLANs for Segmentation
2.2	Define the characteristics of wide area networks (WANs)	
	<ul style="list-style-type: none"> DSL, site-to-site, cable modem, satellite, cellular (3G, 4G, 5G) 	Ch. 6, p. 135 WAN Characteristics
2.3	Identify wireless networking methods and characteristics	
	<ul style="list-style-type: none"> Types of wireless networking standards and their characteristics (802.11, Bluetooth), types of network security (WPA, WPA2, WEP, 802.1X, and others), point-to-point (P2P) wireless, ad hoc networks, wireless bridging, wireless interference 	Ch. 7, p. 154-157 Wireless Networking
2.4	Compare and contrast network topologies and access methods	
	<ul style="list-style-type: none"> Star, mesh, ring, bus, logical and physical topologies 	Ch. 6, p. 138-140 Network Topologies
3. Network Hardware		
3.1	Describe characteristics of switches	
	<ul style="list-style-type: none"> Number and type of Ethernet ports (access vs. trunk), number of devices supported, managed or unmanaged switches, VLAN capabilities, Layer 2 and Layer 3 switches and security options, potential for single point of failure, switching types and MAC table, capabilities of hubs vs. switches (collision domain, broadcast domain, half- and full-duplex), prevention of switch loops by using spanning tree protocol 	Ch. 6, p. 141 Switches, p. 142-143 Access Points and Specialized Network Devices
3.2	Describe characteristics of routers	
	<ul style="list-style-type: none"> Potential for network bottlenecks, directly connected routes, static routing, dynamic routing (routing protocols), default routes, routing table and how it selects best route(s), port forwarding, Quality of Service (QoS), network segmentation, convergence 	Ch. 6, p. 141-143 Routers, Access Points and Specialized Network Devices; Ch. 7, p. 178-180 Remote Access Methods
3.3	Describe characteristics of physical media	
	<ul style="list-style-type: none"> Cable types and their characteristics, including media segment length and speed; fiber optic, twisted pair shielded or unshielded (CAT5–CAT7 cabling); configuration (crossover vs. straight-through); susceptibility to electromagnetic interference (EMI), cross-talk, and interception 	Ch. 7, p. 147-148 Network Media and Protocols

Obj Number	Description	Chapter/Page Number(s)
4. Protocols and Services		
4.1	Describe the Open Systems Interconnection (OSI) model	
	<ul style="list-style-type: none"> • Identification and purpose of each layer; examples of devices, protocols, and applications at each layer; MAC address 	Ch. 7, p. 149 OSI Model Layers
4.2	Describe the Transmission Control Protocol (TCP) model	
	<ul style="list-style-type: none"> • Identification and purpose of each layer; examples of devices, protocols, and applications at each layer 	Ch. 7, p. 150-152 TCP/IP Model and Core Protocols
4.3	Describe IPv4 concepts	
	<ul style="list-style-type: none"> • Classful vs. classless addressing, subnetting (purpose and why to use), characteristics of IPv4 addressing (subnet mask, default gateway, sockets, broadcast), private addresses (Class A (including loopback), Class B, and Class C) 	Ch. 7, p. 152-153 IPv4 and IPv6
4.4	Describe IPv6 concepts	
	<ul style="list-style-type: none"> • Characteristics of IPv6 addressing (subnet mask, default gateway, sockets, abbreviation), transitioning from IPv4 to IPv6 (tunneling protocols, tunnel brokers, dual IP stack), address types (link-local vs. global), multicast groups (all routers/all nodes), loopback 	Ch. 7, p. 152-153 IPv4 and IPv6
4.5	Identify well-known ports	
	<ul style="list-style-type: none"> • HTTP, HTTPS, FTP, SMTP, IMAP, DNS, RDP, SSH 	Ch. 7, p. 150-152 TCP/IP Model and Core Protocols; Ch. 8, p. 185-186 Network Sniffing & Well-Known Ports
4.6	Describe name resolution concepts	
	<ul style="list-style-type: none"> • Static name resolution (HOSTS file, LMHOSTS file), dynamic name resolution (DNS, WINS), DNS resource records (A, AAAA, MX, PTR, SRV, CNAME, SOA), forward vs. reverse lookups, steps in the name resolution process 	Ch. 7, p. 152-153 IPv4 and IPv6 and Name Resolution, p. 162-164 Command-Line Tools; Ch. 9, p. 194-195 UAC Settings and Secure DNS Updates
4.7	Identify the roles of networking services	
	<ul style="list-style-type: none"> • Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT) (dynamic vs. static, public vs. private, port address translation), firewalls 	Ch. 7, p. 160-162 Network Services and Troubleshooting; Ch. 9, p. 213-216 Wireless Security; Ch. 10, p. 227-233 Cloud Services
5. Troubleshooting		
5.1	Given a scenario, describe the troubleshooting process in a small-medium business network	
	<ul style="list-style-type: none"> • Steps in the troubleshooting process, etiquette/professional conduct 	Ch. 7, p. 160-165 Network Services and Troubleshooting; Ch. 11, p. 257-264 Basic Troubleshooting Steps
5.2	Given a scenario, use the appropriate hardware troubleshooting tools	
	<ul style="list-style-type: none"> • Appropriate tool selection, multimeter, cable tester, toner, time-domain reflectometer (TDR), optical TDR (OTDR) 	Ch. 2, p. 51-54 Troubleshooting Hardware Issues; Ch. 7, p. 160-165 Network Services and Troubleshooting; Ch. 11, p. 257-264 Basic Troubleshooting Steps
5.3	Given a scenario, use the appropriate Windows software tools to troubleshoot a problem	
	<ul style="list-style-type: none"> • Appropriate tool selection, syntax (ping, ipconfig, tracert, pathping, nslookup, hostname, netstat, arp), local loopback IP, protocols 	Ch. 7, p. 150-152, TCP/IP Model and Core Protocols, p. 160-165 Network Services and Troubleshooting; Ch. 11, p. 257-264 Basic Troubleshooting Steps
5.4	Given a scenario, use the appropriate Linux software tools to troubleshoot a problem	
	<ul style="list-style-type: none"> • Appropriate tool selection, syntax (ping, ip addr, traceroute, tracepath, dig, host, netstat, arp) 	Ch. 7, p. 160-165 Network Services and Troubleshooting; Ch. 11, p. 257-264 Basic Troubleshooting Steps

Introduction to Information Technology IT Specialist: Network Security

Introduction to Information Technology is aligned to the skills assessed in Certiport's **Network Security Exam**. The following includes the Exam Objectives covered on the certification exam and the correlating page(s) in which the objectives are taught.

Obj Number	Description	Chapter/Page Number(s)
1. Defense in Depth		
1.1	Identify core security principles	
	<ul style="list-style-type: none"> Confidentiality, integrity, availability, non-repudiation, threat, risk, vulnerability, principle of least privilege, attack surfaces including IoT 	Ch. 8, p. 171-173 Introduction to Network Security; Ch. 9, p. 192-194 OS Security and Hardening
1.2	Define and enforce physical security	
	<ul style="list-style-type: none"> Site security, computer security, removable devices and drives, mantraps 	Ch. 8, p. 173-175 Physical Security Measures
1.3	Identify security policy types	
	<ul style="list-style-type: none"> Administrative controls, technical controls 	Ch. 8, p. 176-184 Network Isolation and Protection Devices and Logical Defense Strategies; Ch. 9, p. 219 Audit Policies
1.4	Identify attack types	
	<ul style="list-style-type: none"> Buffer overflow, viruses, polymorphic viruses, worms, Trojan horses, spyware, ransomware, adware, rootkits, backdoors, zero day attacks/vulnerabilities, denial-of-service (DoS) attacks, common attack methods, types of vulnerability, cross-site scripting (XSS), SQL injection, brute force attack, man-in-the-middle (MITM) and man-in-the-browser (MITB), social engineering, keyloggers (software and hardware), logic bombs 	Ch. 9, p. 205-208 Identifying and Preventing Attacks
1.5	Identify backup and restore types	
	<ul style="list-style-type: none"> Full, incremental, differential 	Ch. 10, p. 239-244 Backup and Restore Strategies
2. Operating System Security		
2.1	Identify client and server protection	
	<ul style="list-style-type: none"> Separation of services, hardening, patch management, reducing the attack surface, group policy (gpupdate and gpresult), secure dynamic Domain Name System (DNS) updates, User Account Control (UAC), keeping client operating system and software updated, encrypting offline folders, software restriction policies 	Ch. 4, p. 89-92 Updating and Patching Windows 11, p. 95-96 Group Policy; Ch. 9, p. 192-195 OS Security and Hardening
2.2	Configure user authentication	
	<ul style="list-style-type: none"> Multifactor authentication, enforcing password policies, remote access, using secondary sign-on to perform administrative tasks (Run As, sudo), domain and local user and group creation, Kerberos 	Ch. 3, p. 70-75 Configuring User Accounts and Settings; Ch. 9, p. 195-199 User Authentication
2.3	Manage permissions in Windows and Linux	
	<ul style="list-style-type: none"> File and folder permissions, share permissions, inheritance, moving or copying files within the same disk or on another disk, multiple groups with different permissions, take ownership, delegation 	Ch. 3, p. 74-75 Setting File and Folder Permissions; Ch. 9, p. 217-219 Permissions and Auditing; Ch. 10, p. 238 Taking Ownership of Files and Folders
2.4	Facilitate non-repudiation using audit policies and log files	
	<ul style="list-style-type: none"> Types of auditing, what can be audited, enabling auditing, what to audit for specific purposes, where to save audit information, reviewing log files 	Ch. 8, p. 173 Non-Repudiation; Ch. 9, p. 219 Auditing; Ch. 11, p. 264-266 Tools and Utilities
2.5	Demonstrate knowledge of encryption	
	<ul style="list-style-type: none"> File and folder encryption, how encryption impacts moving/copying files and folders, drive encryption, TPM, secure communication processes (email, texting, chat, social media), virtual private network (VPN) encryption methods, public key/private key, certificate properties and services, Bitlocker 	Ch. 7, p. 158-160 Remote Access Methods; Ch. 9, p. 199-204 Encryption and Secure Communications; Ch. 10, p. 244 Encryption for Stored Data

Obj Number	Description	Chapter/Page Number(s)
3. Network Device Security		
3.1	Implement wireless security	
	<ul style="list-style-type: none"> Wireless security types (strength of encryption), service set identifiers (SSIDs), MAC filtering, default configuration (OOBE) 	Ch. 7, p. 156 Wireless Security; Ch. 9, p. 213-216 Wireless Security
3.2	Identify the role of network protection devices	
	<ul style="list-style-type: none"> Purpose of firewalls, hardware vs. software firewalls, network vs. host firewalls, stateful vs. stateless firewall inspection, security baselines, intrusion detection system (IDS), intrusion prevention system (IPS), security information and event manager (SIEM), content filtering, blacklisting/whitelisting 	Ch. 8, p. 181-184 Logical Defense Strategies
3.3	Identify network isolation methods	
	<ul style="list-style-type: none"> Routing, honeynet, perimeter networks (DMZ), NAT/PAT, VPN, IPsec, air gap network, DirectAccess, virtual LAN (VLAN) 	Ch. 6, p. 134 LAN Characteristics, p. 141-142 Routers; Ch. 7, p. 158-159 Virtual Private Networks (VPNs); Ch. 8, p. 176-180 Network Isolation and Protection Devices
3.4	Identify protocol security concepts	
	<ul style="list-style-type: none"> Tunneling, DNSSEC, network sniffing, well-known ports (FTP, HTTP, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LDAPS, SNMP, SMTP, IMAP, SFTP) 	Ch. 7, p. 158-159 Virtual Private Networks (VPNs); Ch. 8, p. 184-186 Protocol Security
4. Secure Computing		
4.1	Implement email protection	
	<ul style="list-style-type: none"> Antispam, spoofing, phishing, and pharming, client protection, user training 	Ch. 9, p. 205-213 Attack Types, Attack Methods, Responding to Phishing and Physical Attacks, and Antivirus and Antimalware Software, p. 220 Email and Browser Security
4.2	Manage browser security	
	<ul style="list-style-type: none"> Browser settings, cache management, private browsing 	Ch. 9, p. 220-222 Email and Browser Security
4.3	Install and configure anti-malware and antivirus software	
	<ul style="list-style-type: none"> Installing, uninstalling, reinstalling, and updating; remediation, scheduling scans, investigating alerts 	Ch. 9, p. 210-213 Antivirus and Antimalware Software