CompTIA A+ - Core 2

CompTIA A+ is a globally recognized IT certification that validates foundational IT skills necessary for entry-level IT roles, ensuring learners are prepared for a successful career in technology.

The latest version of CompTIA A+ (220-1201, 220-1202) reflects important updates to address the evolving needs of the IT industry and educational standards. These changes ensure that learners are equipped with the most relevant skills and knowledge to succeed in today's technology-driven world.

The certification validates that successful candidates have the knowledge and skills to:

- Install, configure, and maintain computer equipment, mobile devices, and software for end users.
- Service components based on customer requirements.
- Understand networking basics and apply basic cybersecurity methods to mitigate threats.
- Properly and safely diagnose, resolve, and document common hardware and software issues.
- Apply troubleshooting skills and provide customer support using appropriate communication skills.
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in corporate environments.

Exam Objectives Comparison

The following table aligns exam objectives from 1102 and 1202 for comparison. Skills are aligned by best match.

Domain	Domain name	1102 series	1202 series
1	Operating systems	31%	28%
2	Security	25%	28%
3	Software Troubleshooting	22%	23%
4	Operational Procedures	22%	21%

1102 Objective	1202 Objective	Added	Removed
1.1 - Identify basic features of Microsoft Windows editions	1.3 - Compare and contrast basic features of Microsoft Windows editions	**Windows 11 editions** - Home - Pro - Enterprise **N versions** **Hardware requirements** - Trusted Platform Module (TPM) - Unified Extensible Firmware Interface (UEFI)	
1.2 -Given a scenario, use the appropriate Microsoft command-line tool	1.5 - Given a scenario, use the appropriate Microsoft command-line tools	**Informational** -whoami	**Drive navigation inputs:** M 'C': or D: or x: **Command-line Tools** xcopy, copy,shutdown
1.3 -Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS)	1.4 - Given a scenario, use Microsoft Windows operating system features and tools		
1.4 -Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility	1.6 - Given a scenario, configure Microsoft Windows settings		
1.5 -Given a scenario, use the appropriate Windows settings			

1102 Objective	1202 Objective	Added	Removed
1.6 -Given a scenario, configure Microsoft Windows networking features on a client/ desktop	1.7 - Given a scenario, configure Microsoft Windows networking features on a client/ desktop		
1.7 - Given a scenario, apply application installation and configuration concepts	1.10 - Given a scenario, install applications according to requirements	**Distribution Methods** -Downloadable package - Image deployment	**OS requirements for applications** -Application to OS compatibility - 32-bit vs. 64-bit OS
1.8 - Explain common OS types and their purposes	1.1 - Explain common operating system (OS) types and their purposes	**File System types** - Extended filesystem (XFS)	**File System types** - Third extended filesystem (ext3)
1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment	1.2 - Identify common features and tools of the Linux client/desktop operating system	**Boot Methods** - Multiboot **Installation types** -Zero-touch deployment	
1.10 - Identify common features and tools of the macOS/desktop OS	1.8 - Explain common features and tools of the macOS/desktop operating system	**System folders** - /Applications - /Users - /Library - /System - /Users/Library **Features** -iCloud -iMessage -FaceTime -Drive -Continuity	
1.11 - Identify common features and tools of the Linux client/desktop OS	1.9 - Identify common features and tools of the Linux client/desktop operating system	**Filesystem management** - fsck - mount **Common configuration files** - /etc/passwd - /etc/shadow - /etc/hosts - /etc/fstab - /etc/resolv.conf **OS components** - systemd - kernel - bootloader **Root account**	**Common Commands** -yum **Best practices** - Backups - Antivirus - Updates/patches **Tools** - Shell/terminal - Samba

1101 Objective	1201 Objective	Added	Removed
New Content	1.11 - Given a scenario, install and configure cloud-based productivity tools	**Storage** - Sync/folder settings **Collaboration tools** - Spreadsheets - Videoconferencing - Presentation tools - Word processing tools - Instant messaging **Identity synchronization** **Licensing assignment**	
2.1 - Summarize various security measures and their purposes	2.1 - Summarize various security measures and their purposes	**Physical Access Security** -Mobile digital key -Facial recognition technology (FRT), Voice recognition technology **Logical Security** -Zero Trust model -Time-based one-time password (TOTP) -One time password (OTP) -Security Assertions Markup Language SAML -Single Sign On (SSO) -Just in time Access -Privileged access management (PAM), -Data loss prevention (DLP) - Identity access management (IAM)	**Removed but added to new 2.2** **Active Directory** - Login script - Domain - Group Policy/updates - Organizational units - Home folder - Folder redirection - Security groups
2.2 -Compare and contrast wireless security protocols and authentication methods	2.3 - Compare and contrast wireless security protocols and authentication methods		
2.3 - Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods	2.4 - Summarize types of malware and tools/methods for detection, removal, and prevention	**Malware** -Stalkerware -Fileless **Adware** Potentially unwanted program (PUP) **Tools and Methods** -Email security gateway - Software firewalls -Managed detection and response (MDR) - Extended detection and response (XDR) - Endpoint detection and response (EDR)	

1102 Objective	1202 Objective	Added	Removed
2.4 - Explain common social-engineering attacks, threats, and vulnerabilities	2.5 - Compare and contrast common social engineering attacks, threats, and vulnerabilities	**Social Engineering** -Smishing -QR code phishing -Spear phishing **Threats** -Business email compromise (BEC) - Supply chain/pipeline attack	
2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS	2.2 - Given a scenario, configure and apply basic Microsoft Windows OS security settings	**Login OS options** -Passwordless/Windows Hello **added from earlier version 2.1** **Active Directory** - Joining domain - Assigning log-in script - Moving objects within organizational units - Assigning home folders - Applying Group Policy - Selecting security groups - Configuring folder redirection	
2.6 - Given a scenario, configure a workstation to meet best practices for security	2.7 - Given a scenario, apply workstation security options and hardening techniques.	**Password Considerations** -Uniqueness - Complexity	
2.7 - Explain common methods for securing mobile and embedded devices	2.8 - Given a scenario, apply common methods for securing mobile devices	**Failed Log-in attempts restrictions** **Endpoint Security software** -Content Filtering **Policies and procedures** -MDM -Profile Security Requirements	
2.8 - Given a scenario, use common data destruction and disposal methods	2.9 - Compare and contrast common data destruction and disposal methods	**Regulatory and environmental requirements**	
2.9 - Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks	2.10 - Given a scenario, apply security settings on SOHO wireless and wired networks	**Router Settings** -Configure secure management access **Wireless specific** -Configuring guest access	Dynamic Host Configuration Protocol (DHCP) reservations Static wide-area network (WAN) IP Disabling guest access - Changing channels
2.10 - Given a scenario, install and configure browsers and relevant security settings	2.11 - Given a scenario, configure relevant security settings in a browser	**Browser patching** **Settings** -Proxy - Secure DNS **Browser feature management** - Enable/disable - Plug-ins - Extensions - Features	

1102 Objective	1202 Objective	Added	Removed
New Content	2.6 - Given a scenario, implement procedures for basic small office/ home office (SOHO) malware removal	1.Investigate and verify malware symptoms. 2. Quarantine infected system. 3. Disable System Restore in Windows Home. 4. Remediate infected systems. a. Update anti-malware software. b. Scan and removal techniques (e.g., safe mode, preinstallation environment) c. Reimage/reinstall. 5. Schedule scans and run updates. 6. Enable System Restore and create a restore point in Windows Home. 7. Educate the end user..	
3.1 - Given a scenario, troubleshoot common Windows OS problems	3.1 - Given a scenario, troubleshoot common Windows OS issues		**Common troubleshooting steps** - Reboot - Restart services - Uninstall/reinstall/update applications - Add resources - Verify requirements - System file check - Repair Windows - Restore - Reimage - Roll back updates - Rebuild Windows profiles
3.2 - Given a scenario, troubleshoot common personal computer (PC) security issues	3.4 - Given a scenario, troubleshoot common personal computer (PC) security issues	**Common Symptoms** -Inability to access files **Browser-Related Symptoms** -Degraded browser performance	
3.3 - Given a scenario, use best practice procedures for malware removal.	N/A	Removed	Given a Scenario, use best practices for malware removal. Investigate and verify malware symptoms 2.Quarantine infected systems 3.Disable System Restore in Windows 4.Remediate infected systems a. Update anti-malware software b.Scanning and removal techniques (e.g., safe mode, preinstallation environment) 5.Schedule scans and run updates 6.Enable System Restore and create a restore point in Windows 7. Educate the end user

1102 Objective	1202 Objective	Added	Removed
3.4 - Given a scenario, troubleshoot common mobile OS and application issues	3.2 - Given a scenario, troubleshoot common mobile OS and application issues	**Application fails to install**	**Connectivity Issue** -AirDrop
3.5 - Given a scenario, troubleshoot common mobile OS and application security issues	3.3 - Given a scenario, troubleshoot common mobile OS and application security issues	**Security Concerns** Application source/unofficial application stores -Unauthorized/malicious application	**Security Concerns** Android package (APK) source
4.1 - Given a scenario, implement best practices associated with documentation and support systems information management	4.1 - Given a scenario, implement best practices associated with documentation and support systems information management	**Asset Management** -Configuration management database (CMDB) **Types of Documentation** -Service-level agreements (SLAs) -Internal -External/third-party	**Asset Management** Database system **Types of Documentation** Network topology diagram (Moved to 4.6) - Acceptable use policy (AUP) - Regulatory compliance requirements - Splash screens
4.2 - Explain basic change-management best practices	4.2 -Given a scenario, apply change management procedures	**Documented business processes** -Backup plan **Change Management** - Change type -standard - normal - emergency - Change freeze - Maintenance windows Approvals -Implementation - Peer review	
4.3 - Given a scenario, implement workstation backup and recovery methods	4.3 -Given a scenario, implement workstation backup and recovery methods	**Recovery** - In-place/overwrite - Alternative location	
4.4 - Given a scenario, use common safety procedures	4.4 - Given a scenario, use common safety procedures	**Cable management**	**Proper power handling**
4.5 - Summarize environmental impacts and local environmental controls	4.5 - Summarize environmental impacts and local environmental controls	Uninterruptible power supply (UPS)	Battery backup

1102 Objective	1202 Objective	Added	Removed
4.6 - Explain the importance of prohibited content/ activity and privacy, licensing, and policy concepts	4.6 - Explain the importance of prohibited content/ activity and privacy, licensing, and policy concepts	Order of volatility Non-disclosure agreement	
4.7 - Given a scenario, use proper communication techniques and professionalism	4.7 - Given a scenario, use proper communication techniques and professionalism	same	same
4.8 - Identify the basics of scripting.	4.8 - Explain the basics of scripting.	same	same
4.9 - Given a scenario, use remote access technologies	4.9 - Given a scenario, use remote access technologies	**Methods and Tools** -Simple Protocol for Independent Computing Environments (SPICE) -Windows Remote Management (WinRM)	Microsoft Remote Assistance (MSRA)
New Content	4.10 - Explain basic concepts related to artificial intelligence (AI)	**Application Integration** **Policy** - Appropriate use - Plagiarism **Limitations** - Bias - Hallucinations - Accuracy **Private vs. public** - Data security - Data source - Data privacy	

CompTIA