CompTIA A+ Certification Exam Objectives

EXAM NUMBER: CORE 2 (220-1202)

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA A+ 220-1202 certification exam. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1201) and Core 2 (220-1202). The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) certification exams will verify the successful candidate has the knowledge and skills required 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 ACCREDITATION

The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) exams are accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergo regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	A+ Core 2 (220-1202)
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience in an IT support specialist job role
Passing Score	700 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Operating Systems	28%
2.0	Security	28%
3.0	Software Troubleshooting	23%
4.0	Operational Procedures	21%
Total		**100%**

NOTE ON WINDOWS 11

Versions of Microsoft® Windows® that are not end of Mainstream Support (as determined by Microsoft), up to and including Windows 11, are intended content areas of the certification. As such, objectives in which a specific version of Microsoft Windows is not indicated in the main objective title can include content related to Windows 10 and Windows 11, as it relates to the job role.

1.0 Operating Systems

1.1 Explain common operating system (OS) types and their purposes.

- Workstation systems (OSs)
  - Windows
  - Linux
  - macOS
  - Chrome OS
- Mobile OSs
  - iPadOS
  - iOS
  - Android
- Various filesystem types
  - New Technology File System (NTFS)
  - Resilient File System (ReFS)
  - File Allocation Table 32 (FAT32)
  - Fourth extended filesystem (ext4)
  - Extended filesystem (XFS)
  - Apple File System (APFS)
  - Extensible File Allocation Table (exFAT)
- Vendor life-cycle limitations
  - End-of-life (EOL)
  - Update limitations
- Compatibility concerns between operating systems

1.2 Given a scenario, perform OS installations and upgrades in a diverse environment.

- Boot methods
  - Universal Serial Bus (USB)
  - Network
  - Solid-state/flash drives
  - Internet-based
  - External/hot-swappable drive
  - Internal hard drive (partition)
  - Multiboot
- Types of installations
  - Clean install
  - Upgrade
  - Image deployment
  - Remote network installation
  - Zero-touch deployment
  - Recovery partition
  - Repair installation
  - Other considerations
    - Third-party drivers
- Partitioning
  - GUID [globally unique identifier] Partition Table (GPT)
  - Master boot record (MBR)
- Drive format
- Upgrade considerations
  - Backup files and user preferences
  - Application and driver support/ backward compatibility
  - Hardware compatibility
- Feature updates
  - Product life cycle

1.3 Compare and contrast basic features of Microsoft Windows editions.

- Windows 10 editions
  - Home
  - Pro
  - Pro for Workstations
  - Enterprise
- Windows 11 editions
  - Home
  - Pro
  - Enterprise
- N versions
- Feature differences
  - Domain vs. workgroup
  - Desktop styles/user interface
  - Availability of Remote Desktop Protocol (RDP)
  - Random-access memory (RAM) support limitations
  - BitLocker
  - gpedit.msc
- Upgrade paths
  - In-place upgrade
  - Clean install
- Hardware requirements
  - Trusted Platform Module (TPM)
  - Unified Extensible Firmware Interface (UEFI)

1.4 Given a scenario, use Microsoft Windows operating system features and tools.

- Task Manager
  - Services
  - Startup
  - Performance
  - Processes
  - Users
- Microsoft Management Console (MMC) snap-in
  - Event Viewer (eventvwr.msc)
  - Disk Management (diskmgmt.msc)
  - Task Scheduler (taskschd.msc)
  - Device Manager (devmgmt.msc)
  - Certificate Manager (certmgr.msc)
  - Local User and Groups (lusrmgr.msc)
  - Performance Monitor (perfmon.msc)
  - Group Policy Editor (gpedit.msc)
- Additional tools
  - System Information (msinfo32. exe)
  - Resource Monitor (resmon.exe)
  - System Configuration (msconfig. exe)
  - Disk Cleanup (cleanmgr.exe)
  - Disk Defragment (dfrgui.exe)
  - Registry Editor (regedit.exe)

1.5 Given a scenario, use the appropriate Microsoft command-line tools.

- Navigation
  - cd
  - dir
- Network
  - ipconfig
  - ping
  - netstat
  - nslookup
  - net use
  - tracert
  - pathping
- Disk management
  - chkdsk
  - format
  - diskpart
- File management
  - md
  - rmdir
  - robocopy
- Informational
  - hostname
  - net user
  - winver
  - whoami
  - [command name] /?
- OS management
  - gpupdate
  - gpresult
  - sfc

1.6 Given a scenario, configure Microsoft Windows settings.

- Internet Options
- Devices and Printers
- Program and Features
- Network and Sharing Center
- System
- Windows Defender Firewall
- Mail
- Sound
- Device Manager
- Indexing Options
- Administrative Tools
- File Explorer Options
  - View hidden files
  - Hide extensions
  - General options
  - View options
- Power Options
  - Hibernate
  - Power plans
  - Sleep/suspend
  - Standby
  - Choose what closing the lid does
  - Turn on fast startup
  - USB selective suspend
- Ease of Access
- Time and Language
- Update and Security
- Personalization
- Apps
- Privacy
- Devices
- Network and Internet
- Gaming
- Accounts

1.7 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

- Domain joined vs. workgroup
  - Shared resources
  - Printers
  - File servers
  - Mapped drives
- Local OS firewall settings
  - Application restrictions and exceptions
  - Configuration
- Client network configuration
  - Internet Protocol (IP) addressing scheme
  - Domain Name System (DNS) settings
  - Subnet mask
  - Gateway
  - Static vs. dynamic
- Establish network connections
  - Virtual private network (VPN)
  - Wireless
  - Wired
  - Wireless wide area network (WWAN)/cellular network
- Proxy settings
- Public network vs. private network
- File Explorer navigation–network paths
- Metered connections and limitations

1.8 Explain common features and tools of the macOS/desktop operating system.

- Installation and uninstallation of applications
  - File types
    - .dmg
    - .pkg
    - .app
  - App Store
  - Uninstallation process
- System folders
  - /Applications
  - /Users
  - /Library
  - /System
  - /Users/Library
- Apple ID and corporate restrictions
- Best practices
  - Backups
  - Antivirus
  - Updates/patches
  - Rapid Security Response (RSR)
- System Settings
  - Displays
  - Networks
  - Printers
  - Scanners
  - Privacy
  - Accessibility
  - Time Machine
- Features
  - Multiple desktops
  - Mission Control
  - Keychain
  - Spotlight
  - iCloud
    - iMessage
    - FaceTime
    - Drive
  - Gestures
  - Finder
  - Dock
  - Continuity
- Disk Utility
- FileVault
- Terminal
- Force Quit

1.9 Identify common features and tools of the Linux client/desktop operating system.

- File management
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - grep
  - find
- Filesystem management
  - fsck
  - mount
- Administrative
  - su
  - sudo
- Package management
  - apt
  - dnf
- Network
  - ip
  - ping
  - curl
  - dig
  - traceroute
- Informational
  - man
  - cat
  - top
  - ps
  - du
  - df
- Text editors
  - nano
- Common configuration files
  - /etc/passwd
  - /etc/shadow
  - /etc/hosts
  - /etc/fstab
  - /etc/resolv.conf
- OS components
  - systemd
  - kernel
  - bootloader
- Root account

1.10 Given a scenario, install applications according to requirements.

- System requirements for applications
  - 32-bit vs. 64-bit dependent application requirements
  - Dedicated vs. integrated graphics card
  - Video random-access memory (VRAM) requirements
  - RAM requirements
  - Central processing unit (CPU) requirements
  - External hardware tokens
  - Storage requirements
  - Application to OS compatibility
- Distribution methods
  - Physical media vs. mountable ISO file
  - Downloadable package
  - Image deployment
- Impact considerations for new applications
  - Device
  - Network
  - Operation
  - Business

1.11 Given a scenario, install and configure cloud-based productivity tools.

- Email systems
- Storage
  - Sync/folder settings
- Collaboration tools
  - Spreadsheets
  - Videoconferencing
  - Presentation tools
  - Word processing tools
  - Instant messaging
- Identity synchronization
- Licensing assignment

2.0 Security

2.1 Summarize various security measures and their purposes.

- **Physical security**
  - Bollards
  - Access control vestibule
  - Badge reader
  - Video surveillance
  - Alarm systems
  - Motion sensors
  - Door locks
  - Equipment locks
  - Security guards
  - Fences
- **Physical access security**
  - Key fobs
  - Smart cards
  - Mobile digital key
  - Keys
  - Biometrics
    - Retina scanner
    - Fingerprint scanner
    - Palm print scanner
    - Facial recognition technology (FRT)
    - Voice recognition technology
  - Lighting
  - Magnetometers
- **Logical security**
  - Principle of least privilege
  - Zero Trust model
  - Access control lists (ACLs)
  - Multifactor authentication (MFA)
    - Email
    - Hardware token
    - Authenticator application
    - Short Message Service (SMS)
    - Voice call
    - Time-based one-time password (TOTP)
    - One-time password/ passcode (OTP)
  - Security Assertions Markup Language (SAML)
  - Single sign-on (SSO)
  - Just-in-time access
    - Privileged access management (PAM)
  - Mobile device management (MDM)
  - Data loss prevention (DLP)
  - Identity access management (IAM)
  - Directory services

2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.

- **Defender Antivirus**
  - Activate/deactivate
  - Update definitions
- **Firewall**
  - Activate/deactivate
  - Port security
  - Application security
- **User and groups**
  - Local vs. Microsoft account
  - Standard account
  - Administrator
  - Guest user
  - Power user
- **Log-in OS options**
  - Username and password
  - Personal identification number (PIN)
  - Fingerprint
  - Facial recognition
  - SSO
  - Passwordless/Windows Hello
- **NTFS vs. share permissions**
  - File and folder attributes
  - Inheritance
- **Run as administrator vs. standard user**
- **User Account Control (UAC)**
- **BitLocker**
- **BitLocker-To-Go**
- **Encrypting File System (EFS)**
- **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

2.3 Compare and contrast wireless security protocols and authentication methods.

- Protocols and encryption
  - Wi-Fi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- Authentication
  - Remote Authentication Dial-in User Service (RADIUS)
  - Terminal Access Controller Access-control System (TACACS+)
  - Kerberos
  - Multifactor

2.4 Summarize types of malware and tools/methods for detection, removal, and prevention.

- Malware
  - Trojan
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Boot sector virus
  - Cryptominer
  - Stalkerware
  - Fileless
- Adware
  - Potentially unwanted program (PUP)
- Tools and methods
  - Recovery Console/ environment/modes
  - Endpoint detection and response (EDR)
  - Managed detection and response (MDR)
  - Extended detection and response (XDR)
  - Antivirus
  - Anti-malware
  - Email security gateway
  - Software firewalls
  - User education regarding common threats
    - Antiphishing training
  - OS reinstallation

2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities.

- Social engineering
  - Phishing
    - Vishing
    - Smishing
    - QR code phishing
    - Spear phishing
    - Whaling
  - Shoulder surfing
  - Tailgating
  - Impersonation
  - Dumpster diving
- Threats
  - Denial of service (DoS)
  - Distributed denial of service (DDoS)
  - Evil twin
  - Zero-day attack
  - Spoofing
  - On-path attack
  - Brute-force attack
  - Dictionary attack
  - Insider threat
  - Structured Query Language (SQL) injection
  - Cross-site scripting (XSS)
  - Business email compromise (BEC)
  - Supply chain/pipeline attack
- Vulnerabilities
  - Non-compliant systems
  - Unpatched systems
  - Unprotected systems (missing antivirus/missing firewall)
  - EOL
  - Bring your own device (BYOD)

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.
5. Update anti-malware software.
6. Scan and removal techniques (e.g., safe mode, preinstallation environment)
7. Reimage/reinstall.
8. Schedule scans and run updates.
9. Enable System Restore and create a restore point in Windows Home.
10. Educate the end user.

2.7 Given a scenario, apply workstation security options and hardening techniques.

- Data-at-rest encryption
- Password considerations
  - Length
  - Character types
  - Uniqueness
  - Complexity
  - Expiration
- Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords
- End-user best practices
  - Use screensaver locks
  - Log off when not in use
  - Secure/protect critical hardware (e.g., laptops)
  - Secure personally identifiable information (PII) and passwords
  - Use password managers
- Account management
  - Restrict user permissions
  - Restrict log-in times
  - Disable guest account
  - Use failed attempts lockout
  - Use timeout/screen lock
  - Apply account expiration dates
- Change default administrator's user account/password
- Disable AutoRun
- Disable unused services

2.8 Given a scenario, apply common methods for securing mobile devices.

- Hardening techniques
  - Device encryption
  - Screen locks
    - Facial recognition
    - PIN codes
    - Fingerprint
    - Pattern
    - Swipe
  - Configuration profiles
- Patch management
  - OS updates
  - Application updates
- Endpoint security software
  - Antivirus
  - Anti-malware
  - Content filtering
- Locator applications
- Remote wipes
- Remote backup applications
- Failed log-in attempts restrictions
- Policies and procedures
  - MDM
  - BYOD vs. corporate-owned devices
  - Profile security requirements

2.9 Compare and contrast common data destruction and disposal methods.

- Physical destruction of hard drives
  - Drilling
  - Shredding
  - Degaussing
  - Incineration
- Recycling or repurposing best practices
  - Erasing/wiping
  - Low-level formatting
  - Standard formatting
- Outsourcing concepts
  - Third-party vendor
  - Certification of destruction/recycling
- Regulatory and environmental requirements

2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.

- **Router settings**
  - Change default passwords
  - IP filtering
  - Firmware updates
  - Content filtering
  - Physical placement/secure locations
  - Universal Plug and Play (UPnP)
  - Screened subnet
  - Configure secure management access
- **Wireless specific**
  - Changing the service set identifier (SSID)
  - Disabling SSID broadcast
  - Encryption settings
  - Configuring guest access
- **Firewall settings**
  - Disabling unused ports
  - Port forwarding/mapping

2.11 Given a scenario, configure relevant security settings in a browser.

- **Browser download/installation**
  - Trusted sources
    - Hashing
  - Untrusted sources
- **Browser patching**
- **Extensions and plug-ins**
  - Trusted sources
  - Untrusted sources
- **Password managers**
- **Secure connections/ sites–valid certificates**
- **Settings**
  - Pop-up blocker
  - Clearing browsing data
  - Clearing cache
  - Private-browsing mode
  - Sign-in/browser data synchronization
  - Ad blockers
  - Proxy
  - Secure DNS
- **Browser feature management**
  - Enable/disable
    - Plug-ins
    - Extensions
    - Features

3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS issues.

- Blue screen of death (BSOD)
- Degraded performance
- Boot issues
- Frequent shutdowns
- Services not starting
- Applications crashing
- Low memory warnings
- USB controller resource warnings
- System instability
- No OS found
- Slow profile load
- Time drift

3.2 Given a scenario, troubleshoot common mobile OS and application issues.

- Application fails to launch
- Application fails to close/crashes
- Application fails to update
- Application fails to install
- Slow to respond
- OS fails to update
- Battery life issues
- Random reboots
- Connectivity issues
  - Bluetooth
  - Wi-Fi
  - Near-field communication (NFC)
- Screen does not autorotate

3.3 Given a scenario, troubleshoot common mobile OS and application security issues.

- Security concerns
  - Application source/unofficial application stores
  - Developer mode
  - Root access/jailbreak
  - Unauthorized/malicious application
    - Application spoofing
- Common symptoms
  - High network traffic
  - Degraded response time
  - Data-usage limit notification
  - Limited internet connectivity
  - No internet connectivity
  - High number of ads
  - Fake security warnings
  - Unexpected application behavior
  - Leaked personal files/data

3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.

- Common symptoms
  - Unable to access the network
  - Desktop alerts
  - False alerts regarding antivirus protection
  - Altered system or personal files
    - Missing/renamed files
    - Inability to access files
  - Unwanted notifications within the OS
  - OS updates failures
- Browser-related symptoms
  - Random/frequent pop-ups
  - Certificate warnings
  - Redirection
  - Degraded browser performance

4.0 Operational Procedures

4.1 Given a scenario, implement best practices associated with documentation and support systems information management.

- **Ticketing systems**
  - User information
  - Device information
  - Description of issues
  - Categories
  - Severity
  - Escalation levels
  - Clear, concise written communication
    - Issue description
    - Progress notes
    - Issue resolution
- **Asset management**
  - Inventory lists
  - Configuration management database (CMDB)
  - Asset tags and IDs
  - Procurement life cycle
  - Warranty and licensing
  - Assigned users
- **Types of documents**
  - Incident reports
  - Standard operating procedures (SOPs)
    - Software package custom installation procedure
  - New user/onboarding setup checklist
  - User off-boarding checklist
  - Service-level agreements (SLAs)
    - Internal
    - External/third-party
  - Knowledge base/articles

4.2 Given a scenario, apply change management procedures.

- **Documented business processes**
  - Rollback plan
  - Backup plan
  - Sandbox testing
  - Responsible staff members
- **Change management**
  - Request forms
  - Purpose of the change
  - Scope of the change
  - Change type
    - Standard change
    - Normal change
    - Emergency change
  - Date and time of change
    - Change freeze
    - Maintenance windows
  - Affected systems/impact
  - Risk analysis
    - Risk level
  - Change board approvals
  - Implementation
  - Peer review
  - End-user acceptance

4.3 Given a scenario, implement workstation backup and recovery methods.

- **Backup**
  - Full
  - Incremental
  - Differential
  - Synthetic full
- **Recovery**
  - In-place/overwrite
  - Alternative location
- **Backup testing**
  - Frequency
- **Backup rotation schemes**
  - Onsite vs. offsite
  - Grandfather-father-son (GFS)
  - 3-2-1 backup rule

4.4 Given a scenario, use common safety procedures.

- Electrostatic discharge (ESD) straps
- ESD mats
- Electrical safety
  - Equipment grounding
- Proper component handling and storage
- Cable management
- Antistatic bags
- Compliance with government regulations
- Personal safety
  - Disconnect power before repairing PC
  - Lifting techniques
  - Fire safety
  - Safety goggles
  - Air filter mask

4.5 Summarize environmental impacts and local environment controls.

- Material safety data sheet (MSDS) documentation for handling and disposal
  - Proper battery disposal
  - Proper toner disposal
  - Proper disposal of other devices and assets
- Temperature, humidity-level awareness, and proper ventilation
  - Location/equipment placement
  - Dust cleanup
  - Compressed air/vacuums
- Power surges, under-voltage events, and power losses
  - Uninterruptible power supply (UPS)
  - Surge suppressor

4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

- Incident response
  - Chain of custody
  - Informing management/law enforcement as necessary
  - Copy of drive (data integrity and preservation)
  - Incident documentation
  - Order of volatility
- Licensing/digital rights management (DRM)/ end-user license agreement (EULA)
  - Valid licenses
  - Perpetual license agreement
  - Personal-use license vs. corporate-use license
  - Open-source license
- Non-disclosure agreement (NDA)/mutual non-disclosure agreement (MNDA)
- Regulated data
  - Credit card payment information
  - Personal government-issued information
  - PII
  - Healthcare data
  - Data retention requirements
- Acceptable use policy (AUP)
- Regulatory and business compliance requirements
  - Splash screens

4.7 Given a scenario, use proper communication techniques and professionalism.

- Present a professional appearance and wear appropriate attire.
  - Match the required attire of the given environment.
    - Formal
    - Business casual
- Use proper language and avoid jargon, acronyms, and slang, when applicable.
- Maintain a positive attitude/ project confidence.
- Actively listen and avoid interrupting the customer.
- Be culturally sensitive.
  - Use appropriate professional titles and designations, when applicable.
- Be on time (if late, contact the customer).
- Avoid distractions.
  - Personal calls
  - Texting/social media sites
  - Personal interruptions
- Appropriately deal with difficult customers or situations.
  - Do not argue with customer and/or be defensive.
  - Avoid dismissing customer issues.
  - Avoid being judgmental.
  - Clarify customer statements (i.e., ask open-ended questions to narrow the scope of the issue, restate the issue, or question to verify understanding).
  - Use discretion and professionalism when discussing experiences/encounters.
- Set and meet expectations/ timeline and communicate status with the customer.
  - Offer repair/replacement options, as needed.
  - Provide proper documentation on the services provided.
  - Follow up with customer/user at a later date to verify satisfaction.
- Appropriately handle customers' confidential and private materials.
  - Located on a computer, desktop, printer, etc.

4.8 Explain the basics of scripting.

- Script file types
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- Use cases for scripting
  - Basic automation
  - Restarting machines
  - Remapping network drives
  - Installation of applications
  - Automated backups
  - Gathering of information/data
  - Initiating updates
- Other considerations when using scripts
  - Unintentionally introducing malware
  - Inadvertently changing system settings
  - Browser or system crashes due to mishandling of resources

4.9 Given a scenario, use remote access technologies.

- Methods/tools
  - RDP
  - VPN
  - Virtual network computer (VNC)
  - Secure Shell (SSH)
  - Remote monitoring and management (RMM)
  - Simple Protocol for Independent Computing Environments (SPICE)
  - Windows Remote Management (WinRM)
  - Third-party tools
    - Screen-sharing software
    - Videoconferencing software
    - File transfer software
    - Desktop management software
- Security considerations of each access method

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 A+ Core 2 (220-1202) Acronym List

The following is a list of acronyms that appears on the CompTIA A+ Core 2 (220-1202) exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices, Inc.
AP	Access Point
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy
BEC	Business Email Compromise
BIOS	Basic Input/Output System
BNC	Bayonet Neill-Concelman
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAC	Calling-card Authorization Computer
CIFS	Common Internet File System
CMDB	Configuration Management Database
CNAME	Canonical Name
CPU	Central Processing Unit
DB-9	Serial Communications D-Shell Connector, 9 pins
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
ECC	Error-correcting Code
EDR	Endpoint Detection and Response
EFS	Encrypting File System
EOL	End-of-life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-user License Agreement
exFAT	Extended File Allocation Table

ACRONYM	DEFINITION
FAT	File Allocation Table
FRT	Facial Recognition Technology
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GUID	Globally Unique Identifier
HDD	Hard Disk Drive
HDMI	High-definition Media Interface
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity Access Management
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPS	In-plane Switching
ISO	International Organization for Standardization
ITX	Information Technology eXtended
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode
MAC	Media Access Control
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MDR	Managed Detection and Response
MFA	Multifactor Authentication
MMC	Microsoft Management Console
MNDA	Mutual Non-Disclosure Agreement
mSATA	Mini-serial Advanced Technology Attachment
MSDS	Material Safety Data Sheet
MX	Mail Exchange
NDA	Non-Disclosure Agreement
NetBIOS	Network Basic Input/Output System
NFC	Near-field Communication
NIC	Network Interface Card
NTFS	New Technology File System
NTP	Network Time Protocol
NVMe	Non-volatile Memory Express
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
OTP	One-time Password/Passcode
PaaS	Platform as a Service
PAM	Privileged Access Management
PAN	Personal Area Network
PC	Personal Computer
PCI	Peripheral Component Interconnect

ACRONYM	DEFINITION
PCIe	Peripheral Component Interconnect Express
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PoE	Power over Ethernet
POP	Post Office Protocol
POST	Power-on Self-test
PUP	Potentially Unwanted Program
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Independent Disks
RAM	Random-access Memory
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RFID	Radio-frequency Identification
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RSR	Rapid Security Response
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCSI	Small Computer System Interface
SIM	Subscriber Identity Module
SLA	Service-level Agreement
S.M.A.R.T	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SODIMM	Small Outline Dual In-line Memory Module
SOHO	Small Office/Home Office
SOP	Standard Operating Procedure
SPF	Sender Policy Framework
SPICE	Simple Protocol for Independent Computing Environments
SQL	Structured Query Language
SSD	Solid-state Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSO	Single Sign-on
ST	Straight Tip
TACACS	Terminal Access Controller Access-control System
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TN	Twisted Nematic
TOTP	Time-based One-time Password
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply

ACRONYM	DEFINITION
USB	Universal Serial Bus
UTM	Unified Threat Management
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random-access Memory
WAN	Wide Area Network
WAP	Wireless Access Point
WinRM	Windows Remote Management
WISP	Written Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network
XDR	Extended Detection and Response
XFS	Extended File System
XSS	Cross-site Scripting

CompTIA A+ Core 2 (220-1202) Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the A+ Core 2 (220-1202) certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet
- Chromebook
- Windows laptop/Mac laptop/Linux laptop
- Windows desktop/Mac desktop/Linux desktop
- Windows server with Active Directory and Print Manager
- Monitors
- Projectors
- SOHO router/switch
- Access point (AP)
- Voice over Internet Protocol (VoIP) phone
- Printer
  - Laser/inkjet
  - Wireless
  - 3-D printer
  - Thermal
- Surge suppressor
- UPS
- Smart devices [Internet of Things (IoT) devices]
- Server with a hypervisor
- Punchdown block
- Patch panel
- Webcams
- Speakers
- Microphones

SPARE PARTS/HARDWARE

- Motherboards
- RAM
- Hard drives
- Power supplies
- Video cards
- Sounds cards
- Network cards
- Wireless network interface cards (NICs)
- Fans/cooling devices/heat sink
- CPUs
- Assorted connectors/cables
  - USB
  - High-Definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital Visual Interface (DVI)
  - Video Graphics Array (VGA)
- Adapters
  - Bluetooth adapter
- Network cables
- Unterminated network cable/connectors
- AC adapters
- Optical drives
- Screws/stand-offs
- Cases
- Maintenance kit
- Mice/keyboards
- Keyboard-Video-Mouse (KVM)
- Console cable
- Solid-state drive (SSD)

TOOLS

- Screwdrivers
- Multimeter
- Wire cutters
- Punchdown tool
- Crimper
- Power supply tester
- Cable stripper
- Standard technician toolkit
- ESD strap
- Thermal paste
- Cable tester
- Cable toner
- Wi-Fi analyzer
- Serial Advanced Technology Attachment (SATA) to USB connectors

SOFTWARE

- Operating systems
  - Linux

CompTIA