Hands-On

CompTIA A+ Core Series Core 1 (220-1001) and Core 2 (220-1002) Certification Test Prep (Live Virtual Instructor-Led)

Virtual Live Instructor-led or Available On-Site

Course Description

This extensive Virtual Live Instructor-led CompTIA course meets the NEW DoD Directive 8140 requirements.

The Virtual Option course Includes

-Testing Voucher with Virtual Testing and Certification on Last Day unless more study time is required, test can be taken at a VUE location.

Will Department of Defense (DoD) Directive 8140 replace DoDD 8570? Yes.

When will DoD 8140 take effect? It is already in effect.

Why Change from 8570 to 8140?

DoD 8140 is designed to be more flexible and inclusive than DoD 8570. DoD 8140 includes initiatives such as NIST NICE (National Initiative for Cybersecurity Education), which identifies critical KSAs (Knowledge, Skills, and Abilities) and places cybersecurity positions into 7 categories (1. Security Provision, 2. Operate & Maintain, 3. Protect & Defend, 4. Analyze, 5. Operate & Collect, 6. Oversight & Development, and 7. Investigate) consisting of 31 specialty areas.

A+ from CompTIA is the most recognized and trusted for entry-level service technicians.

CompTIA's A+ is the industry standard for validating the foundation skills needed by today's computer support technicians. This international vendor-neutral certification requires that you pass two exams CompTIA A+ Exams Core 1 (220-1001) and Core 2 (220-1002).

The CompTIA A+ Core Series Core 1 (220-1001) and Core 2 (220-1002) covering the following new content

-Demonstrate baseline security skills for IT support professionals
-Configure device operating systems, including Windows, Mac, Linux, Chrome OS, Android and iOS and administer client-based as well as cloud-based (SaaS) software
-Troubleshoot and problem solve core service and support challenges while applying best practices for documentation, change management, and scripting
-Support basic IT infrastructure and networking
-Configure and support PC, mobile and IoT device hardware

-Implement basic data backup and recovery methods and apply data storage and management best practices

We focus on CompTIA A+ certification exam preparation, you'll gain the needed knowledge of basic computer hardware and operating systems. You'll cover the essential principles of installing, building, upgrading, repairing, configuring, troubleshooting, optimizing, diagnosing, and preventive maintenance, and you'll learn elements of customer service and communication skills necessary to work with clients. Instructor-led practice exams and quizzes help reinforce course concepts and exam readiness.

This course meets the NEW DoD 8140 training requirements.

CompTIA A+ certification is an international, vendor-neutral certification that proves a technician's competency in installation, preventative maintenance, networking, security, and troubleshooting. CompTIA A+ certification also validates that technicians have excellent customer service and communication skills.

CompTIA A+ certified professionals are proven problem solvers. They support todays core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into todays digital world

-The only credential with performance-based items to prove pros can think on their feet to perform critical IT support tasks in the moment
-Trusted by employers around the world to identify the go-to person in end point management & technical support roles
-Regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace

This course is geared to give students Real-World Experience in networking hardware & software by providing Hands-On labs on these converging technologies throughout this training.

Students Will Learn

- **Prepare for the latest edition A+ certification**
- **Support basic IT infrastructure, including endpoint management, advanced device connectivity troubleshooting, and basic networking**
- **Configure and support PC, mobile and IoT device hardware, including components, connectors and peripherals**
- **Implement basic data backup and recovery methods and apply data storage and management best practices**
- **Demonstrate baseline security skills for IT support professionals, including detecting and removing malware, addressing privacy concerns, physical security and device hardening**
- **Configure device operating systems, including Windows, Mac, Linux, Chrome OS, Android and iOS and administer client-based as well as cloud-based (SaaS) software**
- **Troubleshoot and problem solve core service and support challenges while applying best practices for documentation, change management, and the use of scripting in IT support**
- **And more...**

Target Audience

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician.

This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ 220-1001 Certification Exam and the CompTIA 220-1002 Certification Exam.

Prerequisites

Some end-user skills with Windows-based personal computers and basic knowledge of computing concepts would be helpful.

Course Outline

CompTIA A+ Core 1 (220-1001) covers PC hardware and peripherals, mobile device hardware, networking and troubleshooting hardware and network connectivity issues.

- Mobile Devices
- Given a scenario, install and configure laptop hardware and components
- Hardware/device replacement
- Given a scenario, install components within the display of a laptop
- Types
- WiFi antenna connector/placement
- Webcam
- Microphone
- Inverter
- Digitizer/touchscreen
- Given a scenario, use appropriate laptop features
- Special function keys
- Docking station
- Port replicator
- Physical laptop lock and cable lock
- Rotating/removable screens
- Compare and contrast characteristics of various types of other mobile devices
- Tablets
- Smartphones
- Smartphones
- Wearable technology devices
- E-readers
- GPS
- Given a scenario, connect and configure accessories and ports of other mobile devices
- Connection types
- Accessories
- Given a scenario, configure basic mobile device network connectivity and application support
- Wireless/cellular data network (enable/disable)
- Bluetooth
- Corporate and ISP email configuration
- Integrated commercial provider email configuration
- PRI updates/PRL updates/ baseband updates
- Radio firmware
- IMEI vs. IMSI
- VPN

- Given a scenario, use methods to perform mobile device synchronization
- Synchronization methods
- Types of data to synchronize
- Mutual authentication for multiple services (SSO)
- Software requirements to install the application on the PC
- Connection types to enable synchronization
- Networking
- Compare and contrast TCP and UDP ports, protocols, and their purposes
- Ports and protocols
- TCP vs. UDP
- Compare and contrast common networking hardware devices
- Routers
- Switches
- Access points
- Cloud-based network controller
- Firewall
- Network interface card
- Repeater
- Hub
- Cable/DSL modem
- Bridge
- Patch panel
- Power over Ethernet (PoE)
- Ethernet over Power
- Given a scenario, install and configure a basic wired/wireless SOHO network
- Router/switch functionality
- Access point settings
- IP addressing
- NIC configuration
- End-user device configuration
- IoT device configuration
- Cable/DSL modem configuration
- Firewall settings
- QoS
- Wireless settings
- Compare and contrast wireless networking protocols
- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac
- Frequencies
- Channels
- Bluetooth
- NFC
- RFID
- Zigbee
- Z-Wave
- 3G
- 4G
- 5G
- LTE
- Summarize the properties and purposes of services provided by networked hosts
- Server roles
- Internet appliance
- Legacy/embedded systems

- Explain common network configuration concepts
- IP addressing
- DNS
- DHCP
- IPv4 vs. IPv6
- Subnet mask
- Gateway
- VPN
- VLAN
- NAT
- Compare and contrast Internet connection types, network types, and their features
- Internet connection types
- Network types
- Given a scenario, use appropriate networking tools
- Crimper
- Cable stripper
- Multimeter
- Tone generator and probe
- Cable tester
- Loopback plug
- Punchdown tool
- WiFi analyzer
- Hardware
- Explain basic cable types, features, and their purposes
- Network cables
- Video cables
- Multipurpose cables
- Peripheral cables
- Hard drive cables
- Adapters
- Identify common connector types
- RJ-11
- RJ-45
- RS-232
- BNC
- RG-59
- RG-6
- USB
- Micro-USB
- Mini-USB
- USB-C
- DB-9
- Lightning
- SCSI
- eSATA
- Molex
- Given a scenario, install RAM types
- RAM types
- Single channel
- Dual channel
- Triple channel
- Error correcting
- Parity vs. non-parity
- Given a scenario, select, install and configure storage devices
- Optical drives
- Solid-state drives

- Magnetic hard drives
- Hybrid drives
- Flash
- Configurations
- Given a scenario, install and configure motherboards, CPUs, and add-on cards
- Motherboard form factor
- Motherboard connectors types
- BIOS/UEFI settings
- CMOS battery
- CPU features
- Compatibility
- Cooling mechanism
- Expansion cards
- Explain the purposes and uses of various peripheral types
- Printer
- ADF/flatbed scanner
- Barcode scanner/QR scanner
- Monitors
- VR headset
- Optical
- DVD drive
- Mouse
- Keyboard
- Touchpad
- Signature pad
- Game controllers
- Camera/webcam
- Microphone
- Speakers
- Headset
- Projector
- External storage drives
- KVM
- Magnetic reader/chip reader
- NFC/tap pay device
- Smart card reader
- Summarize power supply types and features
- Input 115V vs. 220V
- Output 5.5V vs. 12V
- 24-pin motherboard adapter
- Wattage rating
- Number of devices/types of devices to be powered
- Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs
- Graphic/CAD/CAM design workstation
- Audio/video editing workstation
- Virtualization workstation
- Gaming PC
- Standard thick client
- Thin client
- Network attached storage device
- Given a scenario, install and configure common devices
- Desktop
- Laptop/common mobile devices
- Given a scenario, configure SOHO multifunction devices/printers and settings
- Use appropriate drivers for a given operating system

- Device sharing
- Public/shared devices
- Given a scenario, install and maintain various print technologies
- Laser
- Inkjet
- Thermal
- Impact
- Virtual
- 3D printers
- Virtualization and Cloud Computing
- Compare and contrast cloud computing concepts
- Common cloud models
- Shared resources
- Rapid elasticity
- On-demand
- Resource pooling
- Measured service
- Metered
- Off-site email applications
- Cloud file storage services
- Virtual application streaming/ cloud-based applications
- Virtual desktop
- Given a scenario, set up and configure client-side virtualization
- Purpose of virtual machines
- Resource requirements
- Emulator requirements
- Security requirements
- Network requirements
- Hypervisor
- Hardware and Network Troubleshooting
- Given a scenario, use the best practice methodology to resolve problems
- Always consider corporate policies, procedures, and impacts before implementing changes
- Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power
- Common symptoms
- Given a scenario, troubleshoot hard drives and RAID arrays
- Common symptoms
- Given a scenario, troubleshoot video, projector, and display issues
- Common symptoms
- Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures
- Common symptoms
- Disassembling processes for proper reassembly
- Given a scenario, troubleshoot printers
- Common symptoms
- Given a scenario, troubleshoot common wired and wireless network problem
- Common symptoms
- Operating Systems
- Compare and contrast common operating system types and their purposes
- 32-bit vs. 64-bit
- Workstation operating systems
- Cell phone/tablet operating systems
- Vendor-specific limitations
- Compatibility concerns between operating systems
- Compare and contrast features of Microsoft Windows versions
- Windows 7
- Windows 8
- Windows 8.1

- Windows 10
- Corporate vs. personal needs
- Desktop styles/user interface
- Summarize general OS installation considerations and upgrade methods.
- Boot methods
- Type of installations
- Partitioning - Dynamic
- File system types/formatting
- Load alternate third-party drivers when necessary
- Workgroup vs. Domain setup
- Time/date/region/language settings
- Driver installation, software, and Windows updates
- Factory recovery partition
- Properly formatted boot drive with the correct partitions/format
- Prerequisites/hardware compatibility
- Application compatibility
- OS compatibility/upgrade path
- Given a scenario, use appropriate Microsoft command line tools
- Navigation
- ipconfig
- ping
- tracert
- netstat
- nslookup
- shutdown
- dism
- sfc
- chkdsk
- diskpart
- taskkill
- gpupdate
- gpresult
- format
- copy
- xcopy
- robocopy
- net use
- net user
- [command name] /?
- Commands available with standard privileges vs. administrative privileges
- Given a scenario, use Microsoft operating system features and tools
- Administrative
- MSConfig
- Task Manager
- Disk Management
- System utilities
- Given a scenario, use Microsoft Windows Control Panel utilities
- Internet Options
- Display/Display Settings
- User Accounts
- Folder Options
- System
- Windows Firewall
- Power Options
- Credential Manager
- Programs and features

- HomeGroup
- Devices and Printers
- Sound
- Troubleshooting
- Network and Sharing Center
- Device Manager
- Bitlocker
- Sync Center
- Summarize application installation and configuration concepts
- System requirements
- OS requirements
- Methods of installation and deployment
- Local user permissions
- Security considerations
- Given a scenario, configure Microsoft Windows networking on a client/desktop
- HomeGroup vs. Workgroup
- Domain setup
- Network shares/administrative shares/mapping drives
- Printer sharing vs. network printer mapping
- Establish networking connections
- Proxy settings
- Remote Desktop Connection
- Remote Assistance
- Home vs. Work vs. Public network settings
- Firewall settings
- Configuring an alternative IP address in Windows
- Network card properties
- Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems
- Best practices
- Tools
- Features
- Basic Linux commands
- Security
- Summarize the importance of physical security measures
- Mantrap
- Badge reader
- Smart card
- Security guard
- Door lock
- Biometric locks
- Hardware tokens
- Cable locks
- Server locks
- USB locks
- Privacy screen
- Key fobs
- Entry control roster
- Explain logical security concepts
- Active Directory
- Software tokens
- MDM policies
- Port security
- MAC address filtering
- Certificates
- Antivirus/Anti-malware
- Firewalls

- User authentication/strong passwords
- Multifactor authentication
- Directory permissions
- VPN
- DLP
- Access control lists
- Smart card
- Email filtering
- Trusted/untrusted software sources
- Principle of least privilege
- Compare and contrast wireless security protocols and authentication methods
- Protocols and encryption
- Authentication
- Given a scenario, detect, remove, and prevent malware using appropriate tools and methods
- Malware
- Tools and methods
- Compare and contrast social engineering, threats, and vulnerabilities
- Social engineering
- DDoS
- DoS
- Zero-day
- Man-in-the-middle
- Brute force
- Dictionary
- Rainbow table
- Spoofing
- Non-compliant systems
- Zombie
- Compare and contrast the differences of basic Microsoft Windows OS security settings
- User and groups
- NTFS vs. share permissions
- Shared files and folders
- System files and folders
- User authentication
- Run as administrator vs. standard user
- BitLocker
- BitLocker To Go
- EFS
- Given a scenario, implement security best practices to secure a workstation
- Password best practices
- Account management
- Disable autorun
- Data encryption
- Patch/update management
- Given a scenario, implement methods for securing mobile devices
- Screen locks
- Remote wipes
- Locator applications
- Remote backup applications
- Failed login attempts restrictions
- Antivirus/Anti-malware
- Patching/OS updates
- Biometric authentication
- Full device encryption
- Multifactor authentication
- Authenticator applications

- Trusted sources vs. untrusted sources
- Firewalls
- Policies and procedures
- Given a scenario, implement appropriate data destruction and disposal methods
- Physical destruction
- Recycling or repurposing best practices
- Given a scenario, configure security on SOHO wireless and wired networks
- Wireless
- Change default usernames and passwords
- Enable MAC filtering
- Assign static IP addresses
- Firewall settings
- Port forwarding/mapping
- Disabling ports
- Content filtering/parental controls
- Update firmware
- Physical security
- Software Troubleshooting
- Given a scenario, troubleshoot Microsoft Windows OS problems
- Common symptoms
- Common solutions
- Given a scenario, troubleshoot and resolve PC security issues
- Common symptoms
- Given a scenario, use best practice procedures for malware removal
- Identify and research malware symptoms.
- Quarantine the infected systems.
- Disable System Restore (in Windows).
- Remediate the infected systems.
- Schedule scans and run updates.
- Enable System Restore and create a restore point (in Windows).
- Educate the end user
- Given a scenario, troubleshoot mobile OS and application issues
- Common symptoms
- Given a scenario, troubleshoot mobile OS and application security issues
- Common symptoms
- Operational Procedures
- Compare and contrast best practices associated with types of documentation
- Network topology diagrams
- Knowledge base/articles
- Incident documentation
- Regulatory and compliance policy
- Acceptable use policy
- Password policy
- Inventory management
- Given a scenario, implement basic change management best practices
- Documented business processes
- Purpose of the change
- Scope the change
- Risk analysis
- Plan for change
- End-user acceptance
- Change board
- Backout plan
- Document changes
- Given a scenario, implement basic disaster prevention and recovery methods
- Backup and recovery

- Backup testing
- UPS
- Surge protector
- Cloud storage vs. local storage backups
- Account recovery options
- Explain common safety procedures
- Equipment grounding
- Proper component handling and storage
- Toxic waste handling
- Personal safety
- Compliance with government regulations
- Explain environmental impacts and appropriate controls
- MSDS documentation for handling and disposal
- Temperature, humidity level awareness, and proper ventilation
- Power surges, brownouts, and blackouts
- Protection from airborne particles
- Dust and debris
- Compliance to government regulations
- Explain the processes for addressing prohibited content/ activity, and privacy, licensing, and policy concepts
- Incident response
- Licensing/DRM/EULA
- Regulated data
- Follow all policies and security best practices
- Given a scenario, use proper communication techniques and professionalism
- Use proper language and avoid jargon, acronyms, and slang, when applicable
- Maintain a positive attitude/ project confidence
- Actively listen (taking notes) and avoid interrupting the customer
- Be culturally sensitive - Use appropriate professional titles, when applicable
- Be on time (if late, contact the customer)
- Avoid distractions
- Dealing with difficult customers or situations
- Set and meet expectations/timeline and communicate status with the customer
- Deal appropriately with customer's confidential and private materials
- Identify the basics of scripting
- Script file types
- Environment variables
- Comment syntax
- Basic script constructs
- Basic data types
- Given a scenario, use remote access technologies
- RDP
- Telnet
- SSH
- Third-party tools
- Security considerations of each access method

Notes

Course Length

5

This course can be delivered as the standard A+ Certification Track over 5 days. Our BTS Accelerated course was developed per numerous companies and can be delivered in a shorter or longer day Accelerated format (to also include Network+ and Security+) depending on the experience level of the students attending, this format requires longer training days plus required study time and materials, available upon request.

Delivery Method

Virtual or On-Site Instructor-led with numerous "Hands-On demonstrations and exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

5 Days