CompTIA Mobility+ Certification Exam Objectives

EXAM NUMBER: MB0-001
About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Mobility+ MB0-001 exam. The CompTIA Mobility+ certification is an internationally recognized validation of skills and knowledge required of IT practitioners working in mobile computing environments.

The CompTIA Mobility+ Certification Exam will certify that the successful candidate has the knowledge and skills required to:

• Understand and research capabilities of mobile devices and features of over-the-air technologies
• Deploy, integrate, support and manage a mobile environment, ensuring proper security measures are implemented for devices and platforms while maintaining usability

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level 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”), he/she should perform a search using CertGuard’s engine, found here.

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**: MB0-001
- **Number of questions**: 100 questions
- **Type of questions**: Multiple choice
- **Length of test**: 90 minutes
- **Recommended experience**:
  - Network+ Certification or equivalent working knowledge
  - At least 18 months of work experience in administration of mobile devices in the enterprise
- **Passing score**: 720 (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.

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Over-the-Air Technologies</td>
<td>13%</td>
</tr>
<tr>
<td>2.0 Network Infrastructure</td>
<td>15%</td>
</tr>
<tr>
<td>3.0 Mobile Device Management</td>
<td>28%</td>
</tr>
<tr>
<td>4.0 Security</td>
<td>20%</td>
</tr>
<tr>
<td>5.0 Troubleshooting</td>
<td>24%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
1.0 Over-the-Air Technologies

1.1 Compare and contrast different cellular technologies.
- CDMA
- TDMA
- GSM
  - Edge
  - GPRS
- WiMAX
- UMTS
- CSD
- EVDO
- HSPA
- HSPA+
- LTE
- Roaming and switching between network types

1.2 Given a scenario, configure and implement WiFi client technologies using appropriate options.
- Bluetooth
- PAN
- 802.11a, b, g, n, ac
  - Relevant operating frequencies and channels
- SSID
  - Broadcast/hidden system
  - Authentication methods
  - Portable hotspots

1.3 Compare and contrast RF principles and their functionality.
- RF characteristics
  - Frequencies
  - Modulation
  - Bandwidth
  - Wavelength
  - Amplitude
  - Phase
- Propagation theory
  - Absorption
  - Refraction
  - Reflection
  - Attenuation
  - Interference
- Antennas
  - Omni-directional
  - Semi-directional
  - Bi-directional
  - Yagi
  - Parabolic dish
  - Faraday cage

1.4 Interpret site survey to ensure over the air communication.
- Capacity
- Coverage
- Signal strength
- Received signal strength indicator
- Spectrum analysis
- Frequency analysis
- Site survey documentation/site map
  - Wireless vs. cellular site survey
- Post-site survey
# 2.0 Network Infrastructure

## 2.1 Compare and contrast physical and logical infrastructure technologies and protocols.

<table>
<thead>
<tr>
<th>Topologies</th>
<th>Devices</th>
<th>Services and settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Mesh</td>
<td>- Gateways</td>
<td>- ActiveSync</td>
</tr>
<tr>
<td>- Point-to-point</td>
<td>- Proxies</td>
<td>- Dynamic VLAN</td>
</tr>
<tr>
<td>- Point-to-multipoint</td>
<td>- VPN concentrator</td>
<td>- Subnetting</td>
</tr>
<tr>
<td>- Ad hoc</td>
<td>- Autonomous APs</td>
<td></td>
</tr>
<tr>
<td>Firewall settings</td>
<td>- Wireless LAN</td>
<td></td>
</tr>
<tr>
<td>- Port configuration</td>
<td>- Controller</td>
<td></td>
</tr>
<tr>
<td>- Protocols</td>
<td>- Lightweight AP</td>
<td></td>
</tr>
<tr>
<td>- Filtering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- DMZ</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 2.2 Explain the technologies used for traversing wireless to wired networks.

<table>
<thead>
<tr>
<th>Bandwidth and user limitations</th>
<th>IP addressing</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Backhauling traffic</td>
<td>- TCP</td>
<td>- SNMP</td>
</tr>
<tr>
<td>- QoS</td>
<td>- UDP</td>
<td>- ICMP</td>
</tr>
<tr>
<td>- Traffic shaping</td>
<td>- NAT</td>
<td>- PoE for APs to switches</td>
</tr>
<tr>
<td>Hardware differences</td>
<td>- DNS</td>
<td></td>
</tr>
<tr>
<td>Traffic routing</td>
<td>- DHCP</td>
<td></td>
</tr>
</tbody>
</table>

## 2.3 Explain the layers of the OSI model.

<table>
<thead>
<tr>
<th>Layer 1 – Physical</th>
<th>Layer 5 – Session</th>
<th>Layer 2 – Data link</th>
<th>Layer 6 – Presentation</th>
<th>Layer 3 – Network</th>
<th>Layer 7 – Application</th>
<th>Layer 4 – Transport</th>
</tr>
</thead>
</table>
2.4 Explain disaster recovery principles and how they affect mobile devices.

- Server backups
- Device backups
- Directory services server
- Frequency of backups
- High availability
- DR locations

2.5 Compare and contrast common network ports and protocols for mobile devices.

- 20/21 – FTP
- 22 – SFTP
- 23 – Telnet
- 25 – SMTP
- 53 – DNS
- 80 – HTTP
- 110 – POP3
- 135 – MAPI
- 143 – IMAP
- 389 – LDAP/AD
- 443 – SSL
- 465 – SSMTp
- 587 – Alternate SMTP
- 990 – FTPS
- 993 – IMAP over SSL
- 2175 – AirSync
- 2195 – APNS
- 2196 – Feedback
- 3389 – RDP
- 4101 – SRP
- 5223 – Jabber
- 5228-5230 – GCM
# 3.0 Mobile Device Management

## 3.1 Explain policy required to certify device capabilities.

- Adherence to IT policies and security policies
  - Balance security with usability
- Differences between vendor default applications
- OS modifications and customization
  - OS vendor
  - OEM
  - Telecommunication vendor
- Backup, restore and recovery policies

## 3.2 Compare and contrast mobility solutions to enterprise requirements.

- Mobile device management
  - Password strength
  - Remote wipe
  - Remote lock/unlock
  - Application store
- Mobile application management
  - Application store
- Pushing content
- Device platform support
- Infrastructure support
  - On-premise vs. SaaS
  - Administrative permissions
  - Multi-instance
  - High availability
  - Device groupings
  - Location-based services
    - Geolocation
    - Geofencing
- Monitoring and reporting capabilities and features
- Interoperability with other products/devices
- Telecommunication expense management
- Self-service portal
- Captive portal

## 3.3 Install and configure mobile solutions based on given requirements.

- Liaise with appropriate personnel to ensure infrastructure can accept solutions
- Profile creation
- Directory services setup
- Initial certificate issuance
- EULA
- Sandboxing
- Containerization
- Group profiles based on given requirements
  - Corporate-owned
  - BYOD
  - Executive
  - Management
  - Consultant
  - B2B
- Initiate pilot, testing and evaluation
- Create and update documentation
- Report feedback post-pilot
- SDLC
- Approve, train and launch
3.0 Mobile Device Management

### 3.4 Implement mobile device on-boarding and off-boarding procedures.

- Device activation on cellular networks
- Mobile hardware that facilitates OTA access
  - Wireless cards, cellular cards, SD cards
- On-boarding and provision process
  - Manual
  - Self-service
  - Batch
  - Remote
  - IMEI or ICCID
  - Device enrollment (SCEP)
  - Profile installations
- Off-boarding and de-provisioning
  - Employee terminations
  - Migrations
  - Applications
  - Content
  - Recycle
  - Proper asset disposal
  - Deactivation

### 3.5 Implement mobile device operations and management procedures.

- Centralized content and application distribution and content management system
  - Distribution methods
    - Server-based
    - Content updates/changes
    - Application changes
    - Permissions
- Deployment best practices
  - Number of devices
  - Number of users
- Remote capabilities
  - Lock/unlock
  - Remote wipe
  - Remote control
  - Location services
  - Reporting
- Life cycle operations
  - Certificate expiration/renewal
  - Updates
  - Upgrades
  - Patches
- Change management
- End of life
  - OSs
  - Devices
  - Applications

### 3.6 Execute best practice for mobile device backup, data recovery and data segregation.

- Device backup for corporate data to corporate server
- Device backup of personal data to vendor/third-party server
- Backup to local device: internal storage, SD card, SIM
- Data recovery
  - Testing backups
  - Restoring corporate data
  - Restoring personal data
3.7 **Use best practices to maintain awareness of new technologies including changes that affect mobile devices.**

- OS vendors
- OEMs (hardware)
- Telecommunication vendors
- Third-party application vendors
- New risks and threats

3.8 **Configure and deploy mobile applications and associated technologies.**

- **Messaging standards**
  - MAPI
  - IMAP
  - POP
  - SMTP
- **Vendor proxy and gateway server settings**
- **Information traffic topology**
  - Third-party NOC vs. on-premise vs. hosted
- **Push notification technologies**
  - APNS
  - GCM
  - ActiveSync
- **In-house application requirements**
  - App publishing
  - Platforms
  - Vendor requirements
  - Certificates
  - Data communication
- **Types of mobile applications**
  - Native app
  - Web app
  - Hybrid app
4.0 Security

4.1 Identify various encryption methods for securing mobile environments.

- Data in transit
  - IPSEC
  - VPN
  - SSL
  - HTTPS
  - WPA/TKIP
  - WPA2
  - TLS
  - SRTP
  - RSA
  - WEP
  - SSH
  - RC4
  - CCMP
  - EAP methods

- Data at rest
  - AES
  - DES
  - 3DES
  - Twofish
  - ECC
  - Full disk encryption
  - Block-level encryption
  - File-level encryption
  - Folder-level encryption
  - Removable media encryption

4.2 Configure access control on the mobile device using best practices.

- Authentication concepts
  - Multifactor
    - Biometric
    - Credentials
    - Tokens
    - Pin
  - Device access
  - Wireless networks
    - Enterprise vs. personal
    - Application access

- PKI concepts
  - Certificate management
  - Software-based container access and data segregation

4.3 Explain monitoring and reporting techniques to address security requirements.

- Device compliance and report audit information
- Third-party device monitoring applications (SIEM)
- Monitor appropriate logs pertaining to mobile device activity/traffic
Explain risks, threats and mitigation strategies affecting the mobile ecosystem.

- **Wireless risks**
  - Rogue access points
  - DoS
  - Tower spoofing
  - Jamming
  - War driving
  - Man-in-the-middle
  - Weak keys

- **Software risks**
  - App store usage
  - Virus
  - Trojans
  - Worm
  - Malware
  - Spyware
  - Jailbreak
  - Rooting
  - Keylogging
  - Unsupported OS

- **Organizational risks**
  - BYOD ramifications
  - Securing personal devices
  - Removable media
  - Wiping personal data
  - Unknown devices on network/server

- **Hardware risks**
  - Device cloning
  - Device theft
  - Device loss

- **Mitigation strategies**
  - Antivirus
  - Software firewalls
  - Access levels
  - Permissions
  - Host-based and network-based IDS/IPS
  - Anti-malware
  - Application sandboxing
  - Trusted platform modules
  - Data containers
  - Content filtering
  - DLP
  - Device hardening
  - Physical port disabling

Given a scenario, execute appropriate incident response and remediation steps.

- **Incident identification**
  - Determine and perform policy-based response

- **Report incident**
  - Escalate
  - Document
  - Capture logs
5.0 Troubleshooting

5.1 Given a scenario, implement the following troubleshooting methodology.

- Identify the problem
  - Information gathering
  - Identify symptoms
  - Question users
  - Determine if anything has changed
- Establish a theory of probable cause
  - Question the obvious
- Test the theory to determine cause
  - Once theory is confirmed, determine next steps to resolve problem
  - If theory is not confirmed, re-establish new theory or escalate
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality
- Document findings, actions and outcomes

5.2 Given a scenario, troubleshoot common device problems.

- Battery life
- Sync issues
- Power supply problems
- Password reset
- Device crash
- Power outage

5.3 Given a scenario, troubleshoot common application problems.

- Missing applications
- Configuration changes
- App store problems
- Email issues
- Location services problems
- OS and application upgrade issues
- Profile authentication and authorization issues

5.4 Given a scenario, troubleshoot common over-the-air connectivity problems.

- Latency
- No cellular signal
- No network connectivity
- Roaming issues
- Cellular activation
- Email issues
- VPN issues
- Certificate issues
- APN issues
- Port configuration issues
- Network saturation

5.5 Given a scenario, troubleshoot common security problems.

- Expired certificate
- Authentication failure
- Firewall misconfiguration
- False positives
- False negatives
- Non-expiring passwords
- Expired passwords
- Content filtering misconfigured
CompTIA Mobility+ Acronyms

The following is a list of acronyms that appear on the CompTIA Mobility+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
<td>GSM</td>
<td>Global Standard for Mobility</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
<td>HSPA</td>
<td>High Speed Packet Access</td>
</tr>
<tr>
<td>APNS</td>
<td>Apple Push Notification Service</td>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to Business</td>
<td>IASE</td>
<td>Info Assurance Support Environment</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority or Certification Authority</td>
<td>IMAP</td>
<td>Internet Message Address Protocol</td>
</tr>
<tr>
<td>CCE</td>
<td>Common Configuration Enumeration</td>
<td>IMAPS</td>
<td>IMAP Secure</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
<td>IMS</td>
<td>Industrial, Medical, Scientific</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Data Recording</td>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>CME</td>
<td>Coronal Mass Ejection</td>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
<td>KCD</td>
<td>Kerberos Constrained Delegation</td>
</tr>
<tr>
<td>CSD</td>
<td>Circuit Switch Data</td>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>CSMA/CD</td>
<td>Carrier Sense Multiple Access with Collision Detection</td>
<td>LTE</td>
<td>Long-Term Evolution</td>
</tr>
<tr>
<td>CUE</td>
<td>Common User Environment</td>
<td>MaaS</td>
<td>Mobility as a Service</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td>MAM</td>
<td>Mobile Application Management</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
<td>MAPI</td>
<td>Messaging Application Programming Interface</td>
</tr>
<tr>
<td>DM</td>
<td>Device Manager</td>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
<td>MEAP</td>
<td>Mobile Enterprise Application Platform</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>EAS</td>
<td>Exchange Active Solution</td>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
<td>MMCA</td>
<td>Multiple Mobile Channel Access</td>
</tr>
<tr>
<td>EUA</td>
<td>End-User License Agreement</td>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>EVDO</td>
<td>Evolution Data Optimized</td>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>FTPS</td>
<td>FTP over SSL</td>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois/Counter Mode or Google Cloud Messaging for Android</td>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OCSP</td>
<td>Online Certificate Security Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
<td>---------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnect</td>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
<td>SMTP</td>
<td>Simple Mail Transport Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
<td>SOHO</td>
<td>Small Office, Home Office</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
<td>SRP</td>
<td>Server Router Protocol</td>
</tr>
<tr>
<td>PIM</td>
<td>Personal Information Manager</td>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>PLE</td>
<td>Power Line Ethernet</td>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
<td>SSMTIP</td>
<td>Secure SMTP</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
<td>SSP</td>
<td>Self-Service Portal</td>
</tr>
<tr>
<td>PRL</td>
<td>Preferred Roaming List</td>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
<td>TEM</td>
<td>Telecom Expense Management</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>RPT</td>
<td>Recovery Point Objective</td>
<td>UMTS</td>
<td>Universal Mobile Telecommunications Standards</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
<td>USCC</td>
<td>United States CyberCom</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>SDLC</td>
<td>System Development Life Cycle</td>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure FTP</td>
<td>VPP</td>
<td>Volume Purchase Program</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
<td>WiFi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
<td>WiMAX</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CompTIA Mobility+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Mobility+ exam. This list may also be helpful for training companies who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

**EQUIPMENT**
- Messaging server
- MDM server
- High-powered laptop
- Tablets
- Smartphone
- Access point
- Router
- Switch
- Air cards
- Hotspots
- Project/large screen with adapters
- Wireless LAN controller
- PoE injector
- Pico cell
- VPN concentrator
- Firewall
- Hardware tokens (secure IDs)

**TOOLS**
- Spectrum analyzer
- Crimpers

**SOFTWARE**
- Android
- iOS
- Various operating systems:
  - OSx, Windows, Linux, Unix
- Messaging client software
- Certificate management software
- MDM, MAM, MCM software

**OTHER**
- Internet connection

**SPARE PARTS/HARDWARE**
- Cables (CAT5)
- Removable media
- Various antenna types
- Power adapters
- Sync cables
- SD cards

© 2015 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 02155-Oct2015.