Supporting and Troubleshooting Mobile Devices

CompTIA

Supporting and Troubleshooting Mobile Devices

- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Mobile Devices

- Smartphones and tablets used in the workplace need support, too.
- Mobile OSs (iOS, Android, or Windows Mobile).
- Store-based software ecosystems.

Smartphones

- One-handed operation
- Touchscreen displays
- Screen sizes range from 4.5” to 5.7”
- Multicore CPUs
- 2 to 6 GB system memory
- 16 GB+ flash memory storage
- Features:
  - Digital cameras
  - Input sensors
  - Networking via Wi-Fi or cellular data

Tablets

- Usually 7” or 10” screen
- Might be able to connect to a removable physical keyboard
- Some laptops can also function as a tablet by flipping the screen
- Usually connect to a Wi-Fi network; some have cellular option
- Phablets—cross between a phone and a tablet with 5.5” to 7” screen

Mobile Devices vs. Laptops

Factor	Description
Processors	Mobile devices: • CPUs and chipsets are based on ARM microarchitecture. • Dual- and quad-core CPUs are common, with some 64-bit CPUs available. • Provide more power and thermal efficiency. PCs and laptops: • CPUs and chipsets are based on CISC and RISC microarchitecture. • Dual- and quad-core CPUs are widespread, with many 64-bit CPUs available.
System memory	Tablet RAM is a low power DDR SDRAM variant. Works similarly to PC/laptop RAM.
Storage	SSDs used in mobile devices instead of HDDs.
Component replacements and upgrades	More FRUs for PCs and laptops. Tablet components are soldered and glued, making it necessary to replace the entire device.
OSs	More OS options for PCs and laptops. Mobile devices limited to the mobile OS they were designed to run.

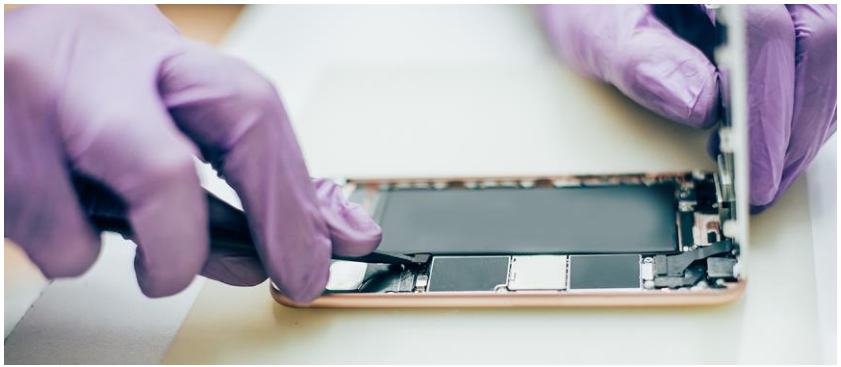
Mobile Display/Touch Interface

Touchscreen: A display screen combined with a digitizer that is responsive to touch input.

- Capacitive touchscreens support multitouch (sweep, pinch, etc.).
- Haptic feedback provides a more realistic feel to the user.
- Protected by scratch- and shock-resistant tempered glass.
- Screen orientation is changeable.

Mobile Device Form Factors

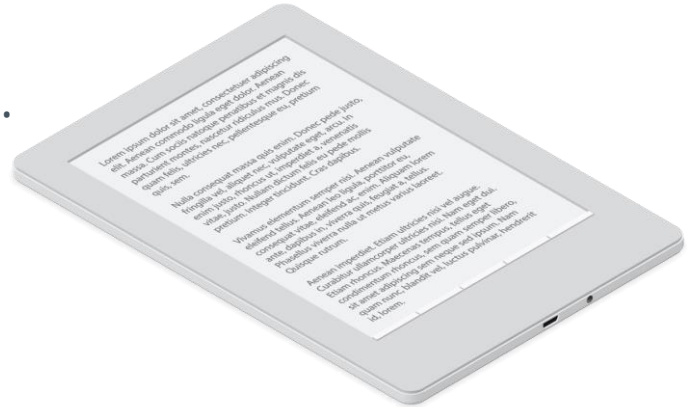
- Fewer field serviceable parts than PCs and laptops.
- Return to manufacturer for replacing screens, storage devices, and possibly batteries.
- Some batteries can be replaced by the user.
- Some devices will have a SIM card port.



E-Readers

e-reader: A tablet-sized device designed for reading, rather than for general-purpose computing.

- E-ink technology creates EPD.
- Low-power, high-contrast display.
- Backlights often not needed, saving power.
- USB chargers.
- Wi-Fi connectivity for downloading e-books.



Wearable Technology

- Smart watches
- Fitness monitors
- VR/AR headsets and smart glasses

GPS Navigation Devices

Global Positioning System (GPS): Means of determining a receiver's position on the Earth based on information received from GPS satellites. The receiver must have line-of-sight to the GPS satellites.

- Built into smartphones and other devices.
- Dedicated units for vehicles, cyclists, or walkers.
- Geolocation system, map, and local traffic information.
- Route planning and directions.
- Some provide live traffic information.
- Touch and voice controls available.

Activity

Discussing Mobile Device Types

Supporting and Troubleshooting Mobile Devices

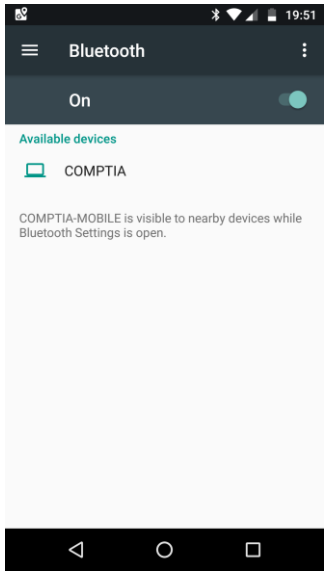
- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Wired Connections for Accessories

- Apple devices:
  - Apple Dock for older devices.
  - Apple Lightning connector.
- Android devices:
  - Micro-B USB connectors for most devices.
  - Mini-B for older devices.
  - USB-C on newer devices.

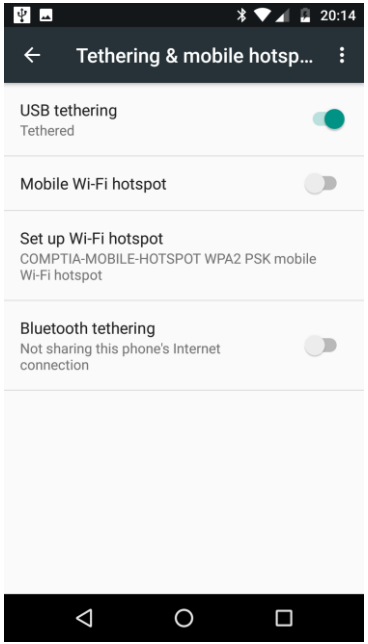
Wireless Connections for Accessories (slide 1 of 2)

- Bluetooth
- NFC
- IR

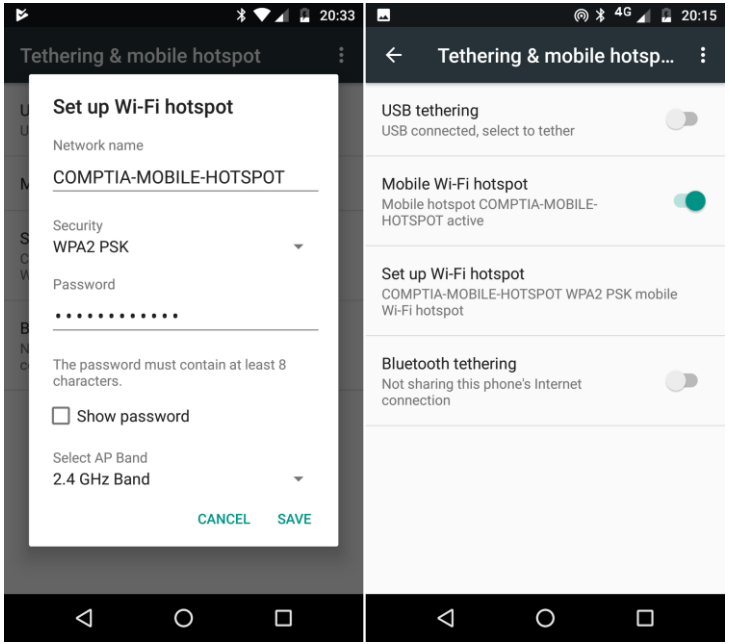


Wireless Connections for Accessories (slide 2 of 2)

Tethering

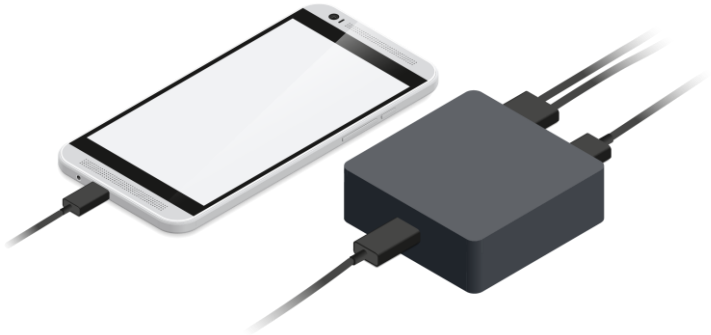


Mobile hotspots



Common Mobile Device Accessories

- External keyboard
- Headset
- Speaker dock
- Micro-SD slot
- Docking stations
- Protective covers and waterproofing
- Credit card readers
- Mobile power



Activity

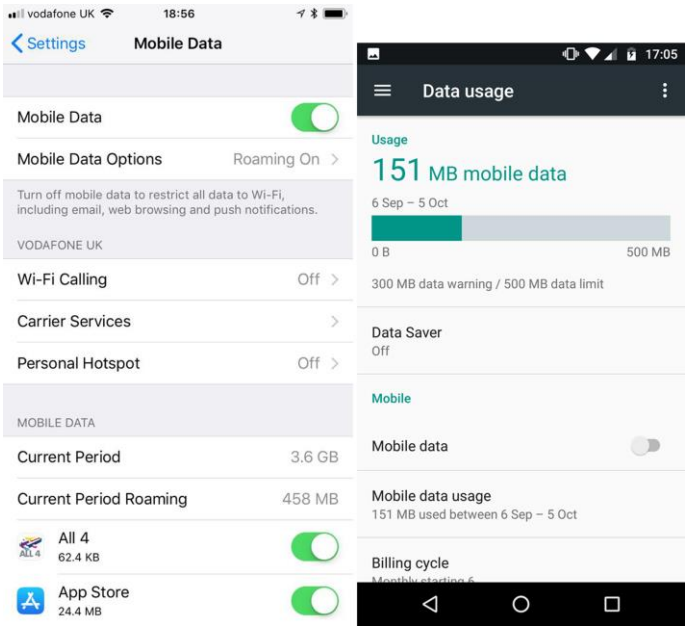
Discussing Mobile Device Accessory Connection and Configuration

Supporting and Troubleshooting Mobile Devices

- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

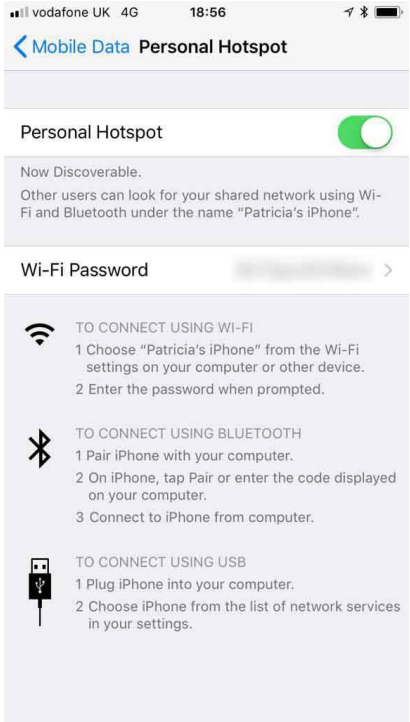
Cellular Data Networks (Slide 1 of 4)

Cellular data: Connecting to the Internet via the device's cell phone radio and the handset's cellar network provider.



Cellular Data Networks (Slide 2 of 4)

- Mobile hotspots and tethering
- Cellular radios:
  - Base station effective range up to 5 miles
  - Transmitter connects phone to mobile and landline phone networks
  - Works in the 850 and 1900 MHz frequency bands in Americas
  - Works in the 900 and 1800 MHz frequency bands in the rest of the world
  - GSM deployed worldwide
  - CDMA used in the Americas



Cellular Data Networks (Slide 3 of 4)

- GSM networks and SIM cards:
  - GSM works with SIM cards
  - Handsets are identified by IMEI number
  - Users are identified by IMSI number
- SIM card number format:
  - 3-digit mobile country code
  - 2-digit mobile network code
  - Up to 10-digit mobile station identification number

Cellular Data Networks (Slide 4 of 4)

- CDMA networks:
  - Locks handset to original provider
  - Does not require use of a SIM card
  - Handsets are identified by MEID number
  - Uses PRI and PRL databases for information needed to connect cellular radio to the network
  - If the handset contains a SIM card, it is to connect to 4G networks, which are GSM-based networks

Baseband Updates and Radio Firmware

Baseband update: Modification of the firmware of a cellular modem.

Radio firmware: An operating system that is separate from the end-user operating system in a mobile device.

Realtime Operating System (RTOS): An OS that is optimized for use in embedded or real-time apps.

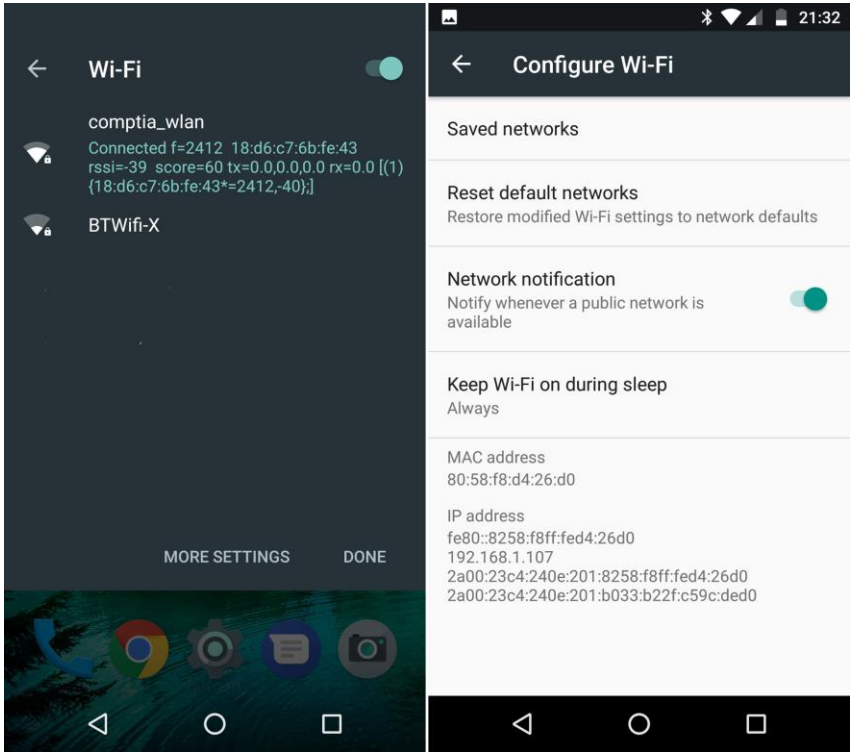
- Baseband updates modify the radio firmware.
  - Firmware OS is separate from the user OS.
  - Controls low-level timing-dependent functions (USB, network, and GPS).
  - Runs all available radio functions (cellular, Wi-Fi, and Bluetooth).
- Updates usually pushed by device vendor as part of an OS upgrade.

Wi-Fi Networks and Hotspots (slide 1 of 2)

Hotspot: A mobile device setting or access point that enables using the cellular data plan of the mobile device to connect a PC or laptop to the Internet.

- All smartphones and tablets support Wi-Fi communication.
  - In iOS, select **Settings→Wi-Fi** to connect.
  - In Android, use the notification shade or open the **Settings→Wi-Fi** menu.
- Hotspot implementations:
  - Public access point (free or paid).
  - Smartphone or tablet.
  - Wireless router designed for personal hotspots.

Wi-Fi Networks and Hotspots (slide 2 of 2)



Mobile VPN Configuration

Virtual Private Network (VPN): A secure tunnel created between two endpoints connected via an unsecure network (typically the Internet).

Mobile VPN: A VPN that can maintain the VPN link across multiple carrier networks, where the IP address assigned to the mobile device may change often.

- Tunnel contents often encrypted to secure communications.
- Mobile VPN assigns virtual IP address for connecting to VPN server.
- Links maintained even in sleep mode.
- Available as third-party apps for Android and iOS.

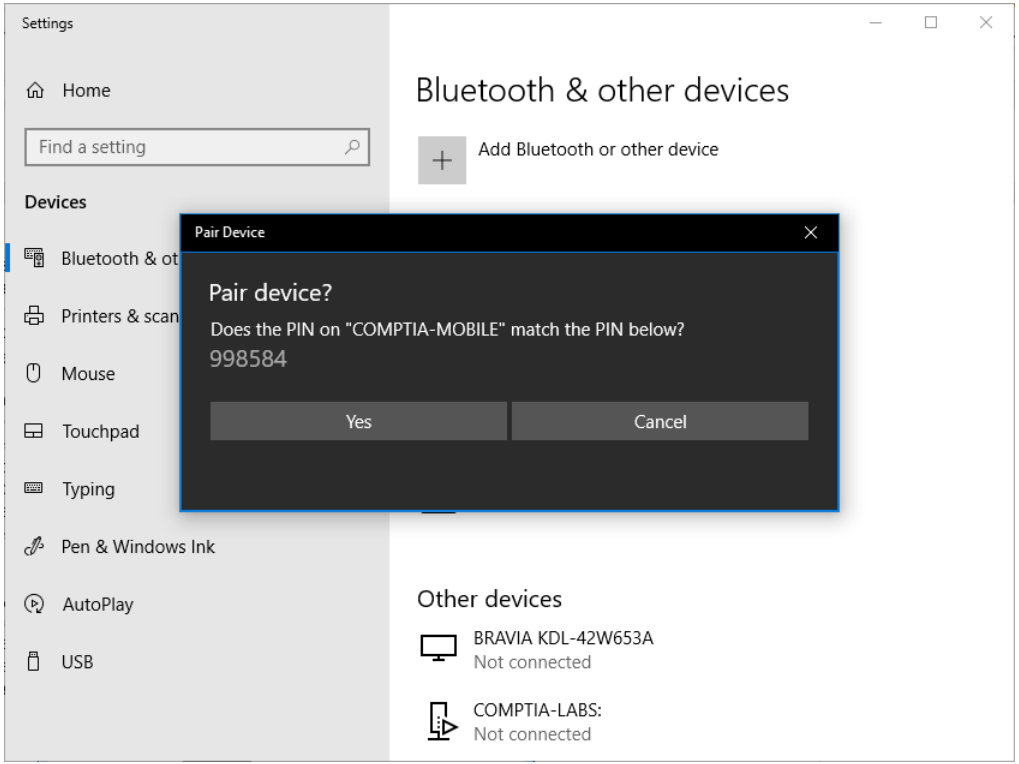
Bluetooth (slide 1 of 3)

Bluetooth: Short-range radio-based technology, working at up to 10 m (30 feet) at up to 1 Mbps, used to connect peripherals for communication between two devices.

- Latest versions support 24 Mbps data rate.
- Used for PANs (Personal Area Networks).
  - Share data with a PC.
  - Connect to a printer, wireless headset, or other peripheral.
- Pairing connects the devices.
  - In iOS, select **Settings→General→Bluetooth.**
  - In Android, access through the notification shade.
  - In Windows, access through Control Panel, Windows Settings, or the Bluetooth icon in the notification area.

Bluetooth (slide 2 of 3)

Bluetooth (slide 3 of 3)



Airplane Mode (slide 1 of 2)

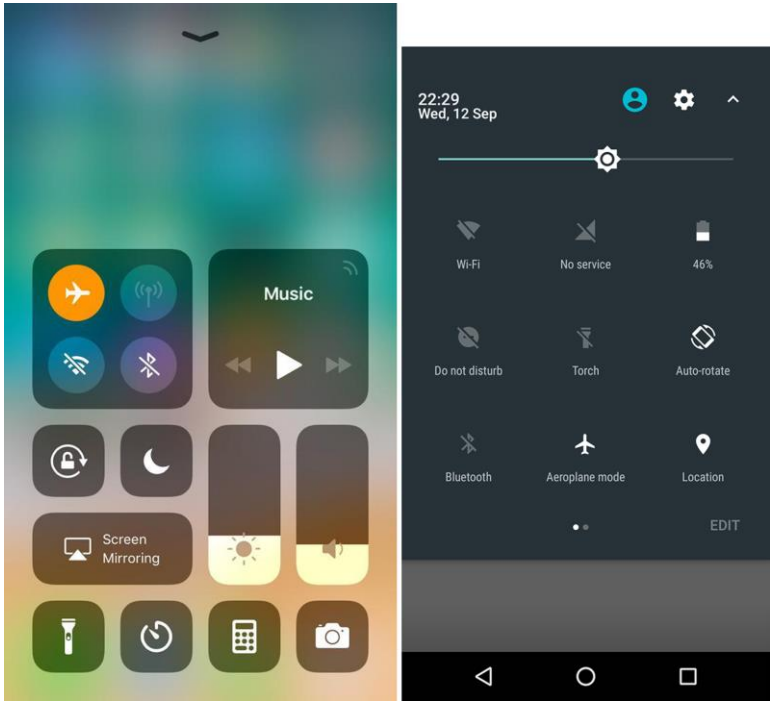
Control Center: An iOS feature that is accessed by swiping up from the bottom of the display to access iOS feature settings.

Notification shade: An Android feature that is accessed by swiping down from the top of the display to access Android OS feature settings.

Airplane mode: A toggle found on mobile devices enabling the user to disable and enable wireless functionality quickly.

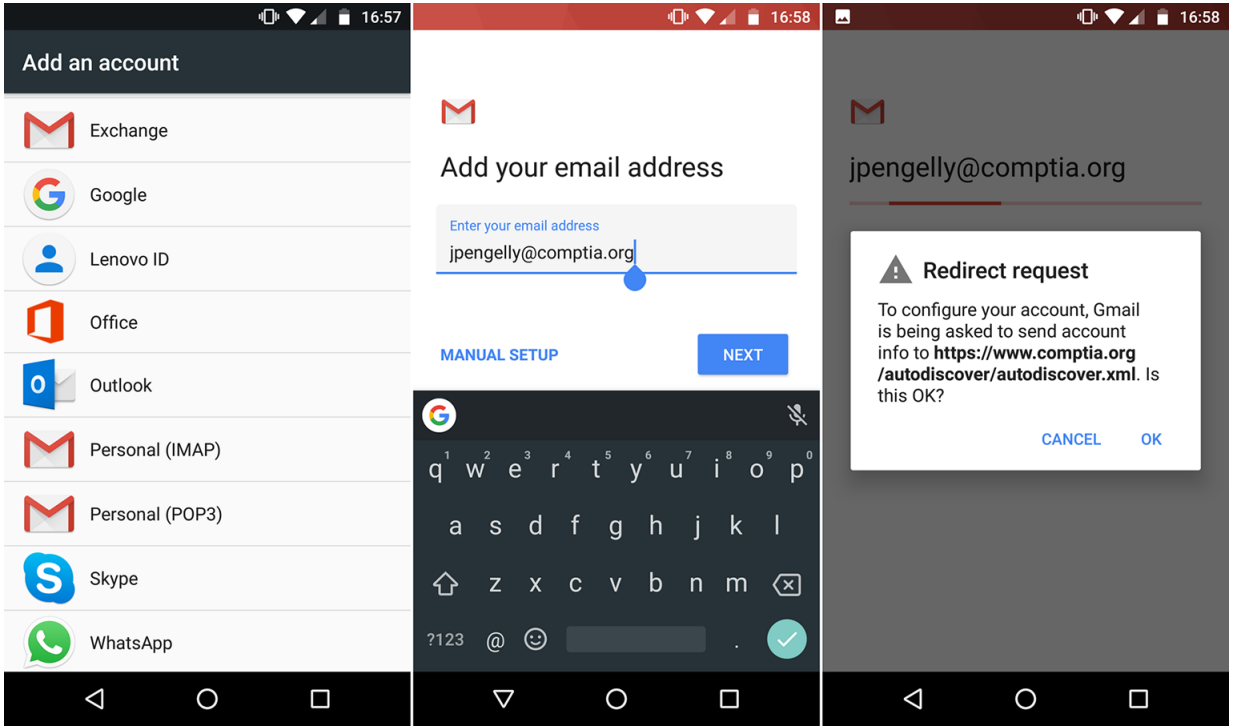
Airplane Mode (slide 2 of 2)

- Disables all wireless features.
  - Cellular data
  - Wi-Fi
  - GPS
  - Bluetooth
  - NFC



Email Configuration Options (Slide 1 of 4)

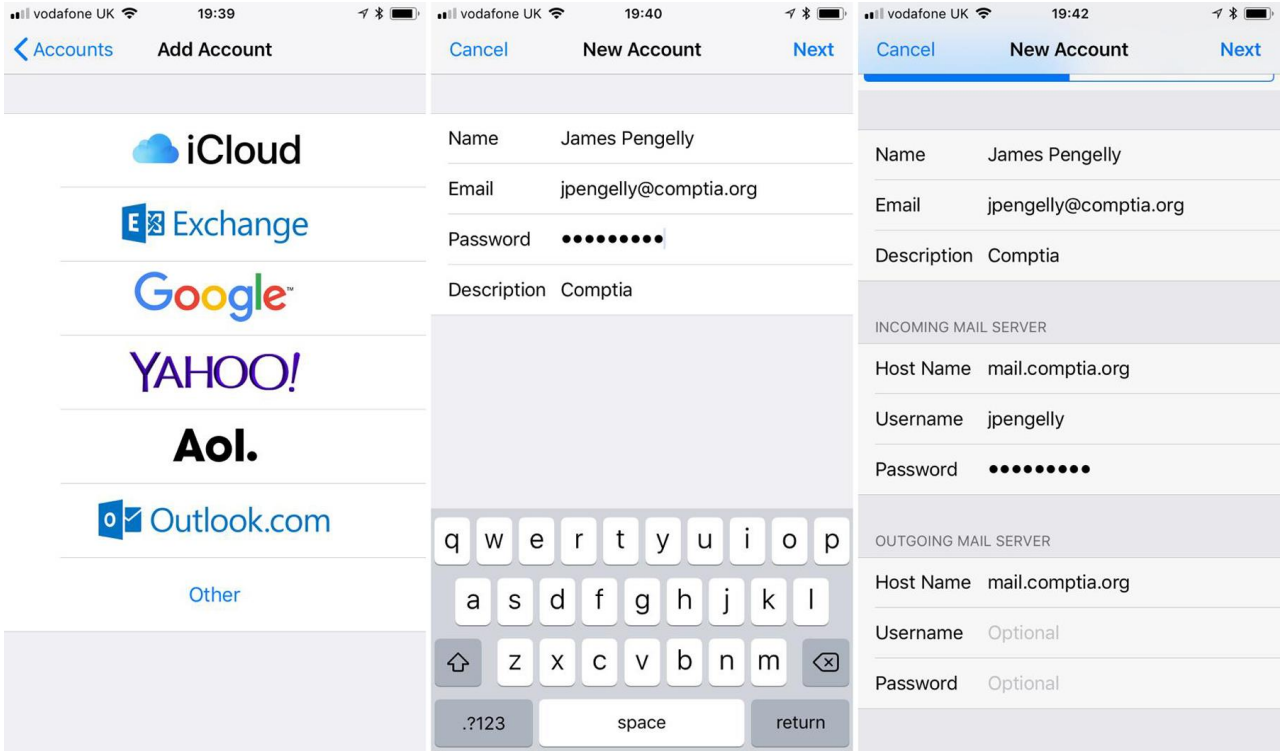
- Commercial Provider Email Configuration



Email Configuration Options (Slide 2 of 4)

- Corporate and ISP Email Configuration:
  - Autodiscover with Exchange and Exchange ActiveSync.
  - For ISPs and corporate mail gateways that don't support Autodiscover, manually enter the mail server address information:
    - Incoming mail server type (IMAP or POP3)
    - Outgoing mail server type (SMTP)
    - SSL setting (enable or disable)
    - Ports

Email Configuration Options (Slide 3 of 4)



Email Configuration Options (Slide 4 of 4)

- S/MIME:
  - Using secure ports does not provide end-to-end encryption for messages.
  - Encryption with digital certificates and digital signatures does.
  - PGP and S/MIME use digital certificates and public/private key pairs.
    - When you sign a message, your private key validates who you are and the public key related to that private key goes to the recipients. The public key allows the recipient to verify who you are.
    - When you want to receive secure messages, the sender uses your public key to encrypt the message. Once encrypted, only your private key can decrypt it (your public key cannot be used to reverse the encryption).
  - Digital and root certificates are often added to the device by using MDM software.

Activity

Discussing Mobile Device Network Connectivity Configuration

Activity

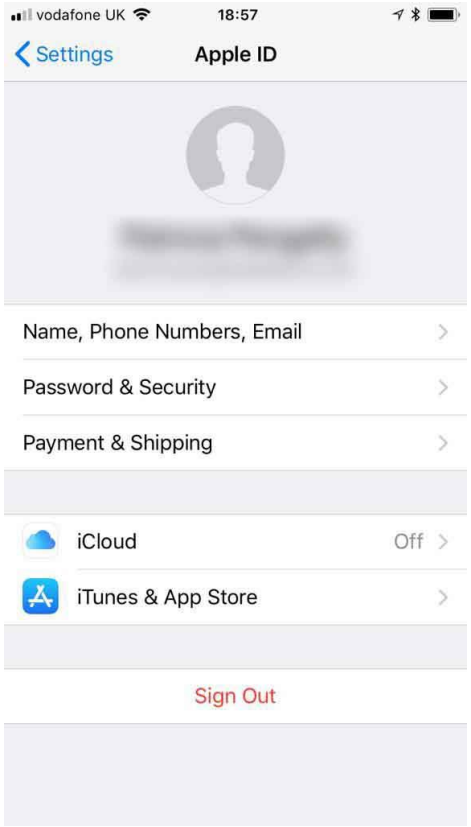
Configuring Bluetooth

Supporting and Troubleshooting Mobile Devices

- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Mobile Account Setup

- User accounts:
  - Normally 1 per device, created at initial use.
  - For iOS: Apple ID.
  - For Android: Google account, Samsung account, or similar.
  - Unique ID and credentials required.
  - Provides access to app store, email, cloud storage.
- Sub-accounts for additional services and apps:
  - Corporate email or messaging.
  - Facebook.
  - LinkedIn.



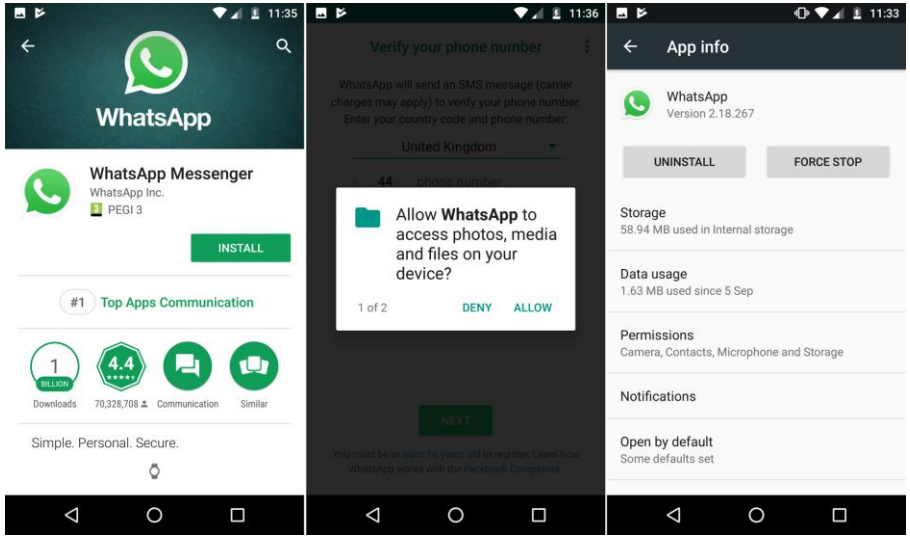
Mobile Applications and App Stores (slide 1 of 2)

App: Installable programs the extend the functionality of a mobile device.

- iOS apps:
  - Get from App Store.
  - Free or paid.
  - Walled garden model—all apps reviewed and approved by Apple.

Mobile Applications and App Stores (slide 2 of 2)

- Android apps:
  - Get from Google Play Store or third-party sites.
  - Free or paid.
  - More open model for app acquisition: store model, or APKs.

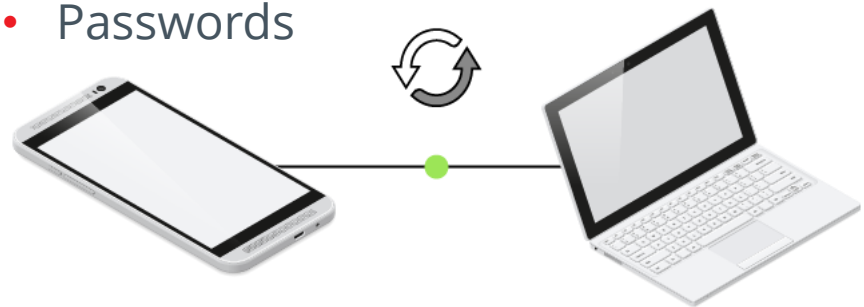


Types of Data to Synchronize

Mobile device synchronization: The act of copying data back and forth between devices to keep the information up-to-date on all of the devices.

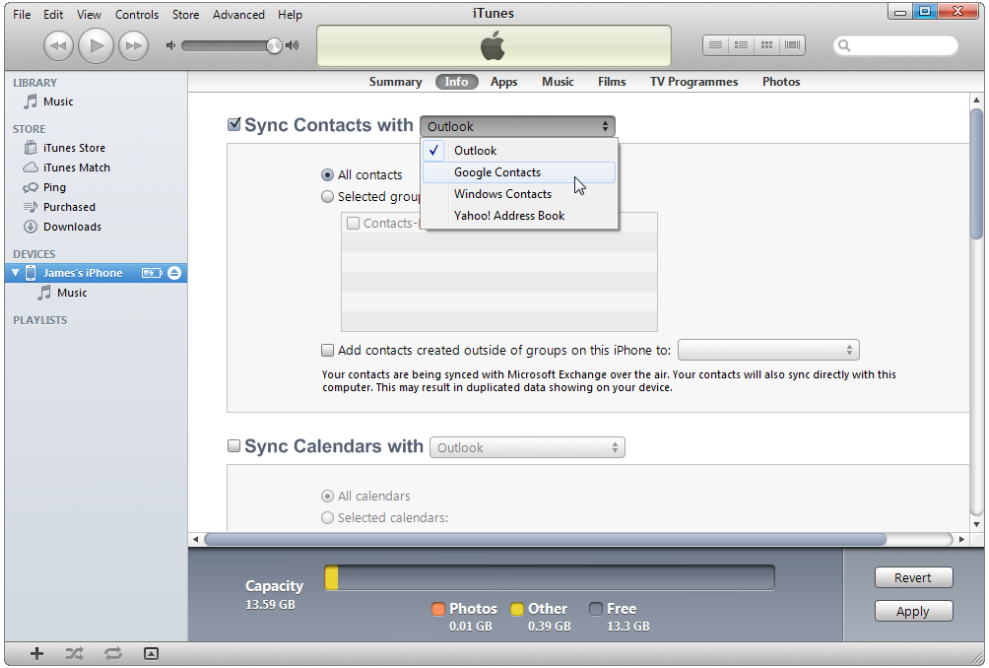
- Contacts
- Calendar
- Email
- Pictures, music, and video
- Documents
- E-books

- Location data
- Social media data
- Apps
- Bookmarks
- Passwords



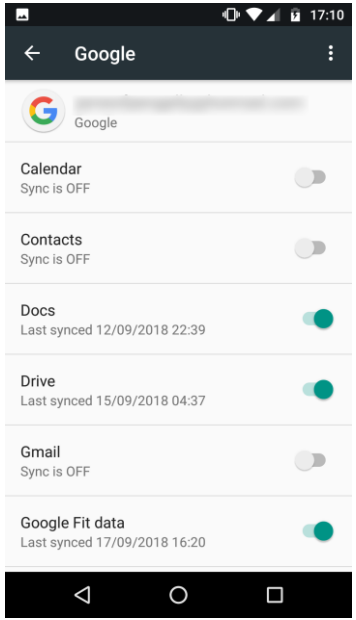
Synchronization Methods (Slide 1 of 3)

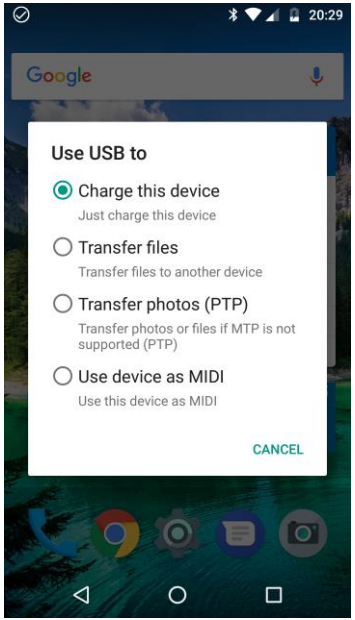
- iOS syncs to desktop via iTunes
- iOS syncs to cloud via iCloud



Synchronization Methods (Slide 2 of 3)

- Android uses the gmail account to sync with cloud storage and Google Play Store.
- You can connect to a PC via USB to transfer data directly.





Synchronization Methods (Slide 3 of 3)

- Microsoft synchronization products
  - OneDrive
  - Outlook.com
  - Office 365
- Third-party synchronization products
  - Vendor-based cloud services
  - Dropbox
- Sync to automobiles.
  - Newer vehicles use head unit to manage entertainment and navigation.
  - Smartphone can be attached to head unit.
  - Apple CarPlay
  - Android Auto

Mutual Authentication for Multiple Service

Single Sign On: (SSO) One service accepts the credentials from another service. Also known as **federated identity management.**

- Sign in once to authenticate to many services
- Enterprise networks:
  - Email
  - Database
  - Document management system
- Mobile device apps use device sign-in credentials:
  - iPhone with an Apple ID
  - Vendor cloud services

Activity

Discussing Mobile App Support

Supporting and Troubleshooting Mobile Devices

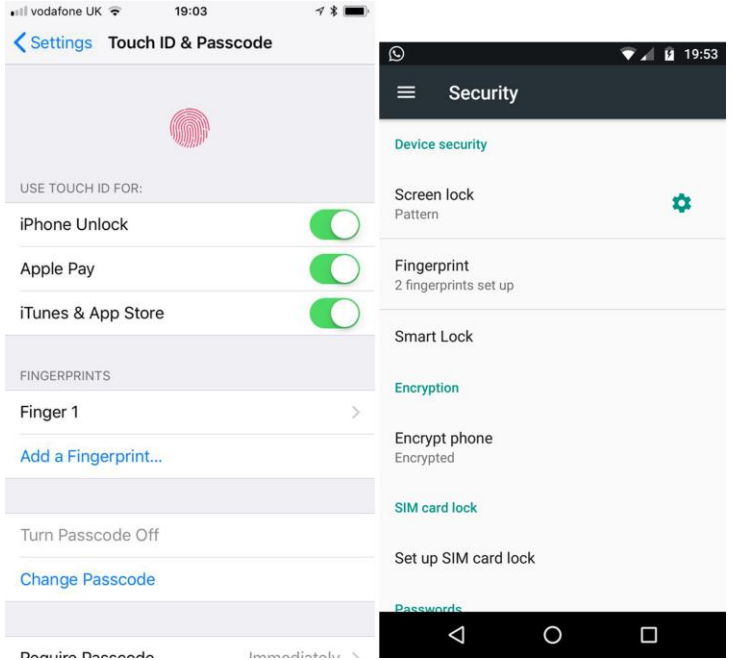
- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Popular Security Controls for Mobile Devices

- Organizations should specify security practices, including:
  - Policies
  - Procedures
  - Training
- Keep mobile devices as secure as the devices that reside inside the physical infrastructure.
- Do not leave mobile devices unattended.

Mobile Device Access Control (Slide 1 of 3)

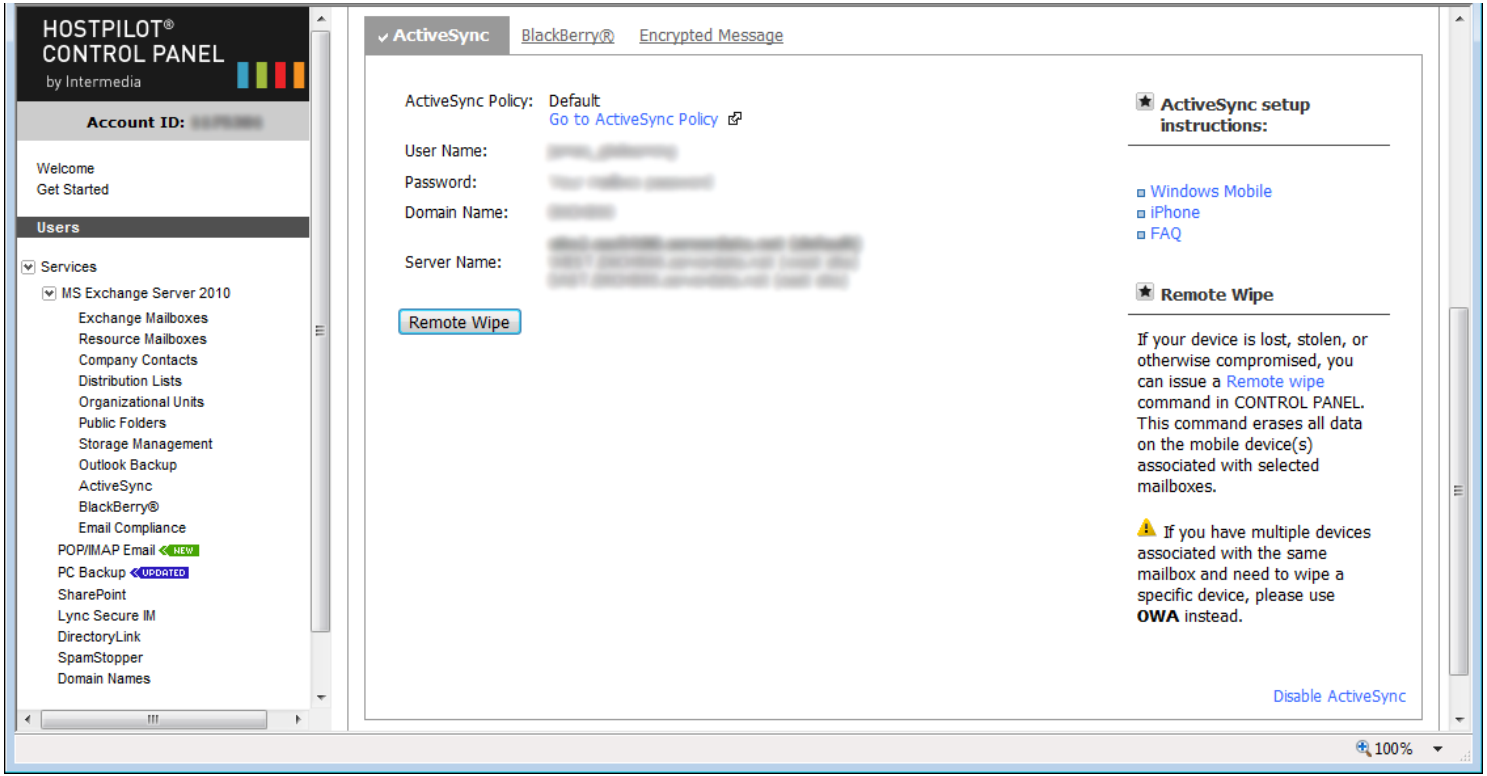
- Screen locks and biometric authentication:
  - Screen locks require a password, passcode, PIN, or gesture to unlock the device.
  - Biometric authentication via fingerprint sensor (Apple Touch ID) or photo (Apple Face ID).



Mobile Device Access Control (Slide 2 of 3)

- Lockout policies:
  - Limits failed logins.
  - Can escalate in duration.
    - For instance, 10 seconds for the first lockout; 30 minutes for the next.
- Remote wiping:
  - Resets a stolen device to factory defaults.
  - All personal data removed.
  - Possibly erase memory cards, too.
  - Preventable, but complicated to bypass.

Mobile Device Access Control (Slide 3 of 3)

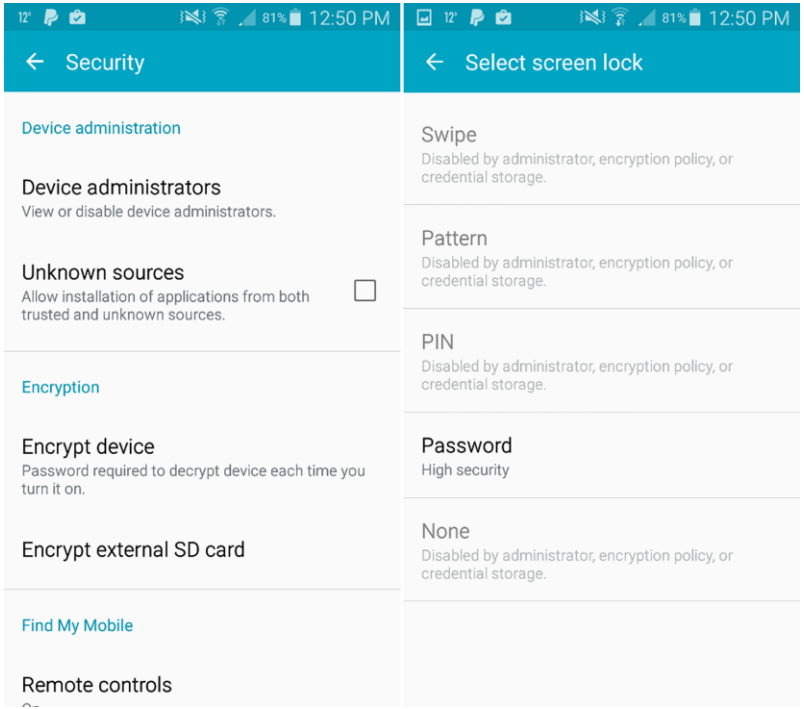


Mobile Device and Data Recovery (slide 1 of 2)

- GPS, geotracking, and locator apps:
  - GPS requires line of sight to satellites.
  - IPS determines position by triangulating distance from access points.
  - Geotracking related to **Location Services**.
  - **Location Services** also supports apps like **Find My Phone**.

Mobile Device and Data Recovery (slide 2 of 2)

- Full device encryption:
  - Prevents bypassing of security controls.
- Remote backup apps:
  - iCloud, Google Sync or Drive, OneDrive



Multifactor Authentication and Authenticator Applications

- Factors:
  - Something you know
  - Something you are
  - Something you have
  - Somewhere you are
- Multifactor authentication requires two different factors.
- Authenticator apps help implement multifactor authentication.
  - 2-step verification: password/PIN (what you know) and a single-use verification code (what you have).

Mobile Device Policies (Slide 1 of 3)

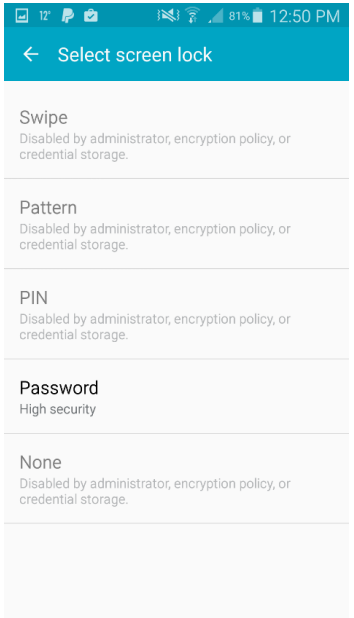
Mobile Device Management (MDM): Software suites designed to manage use of smartphones and tablets within an enterprise.

Bring Your Own Device (BYOD): Security framework and tools to facilitate use of personally owned devices to access corporate networks and data.

- MDM can support multiple OSs.
  - AirWatch
  - Symantec
  - Citrix Endpoint Management
- Some MDM suites are OS-specific.
  - Apple Configurator

Mobile Device Policies (Slide 2 of 3)

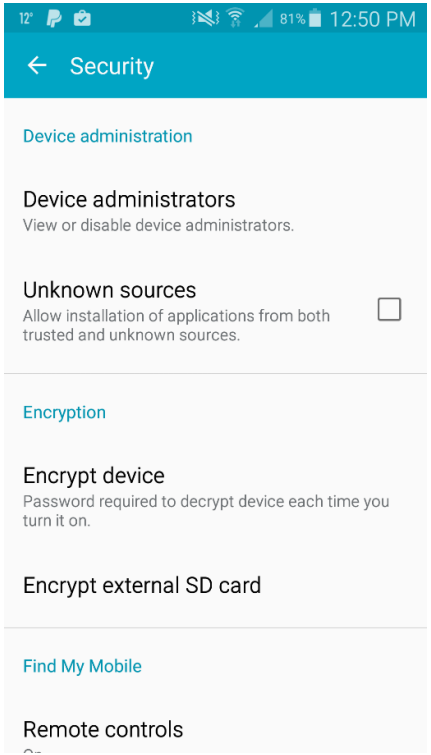
- Profiling security requirements:
  - Onboarding (gaining access to a network).
  - Allow or restrict app, data, or feature usage.
  - Monitor device and antivirus updates.
  - Firewall configuration.
- Trusted and untrusted app sources:
  - Trusted apps are managed by a service provider.
  - Store model is not optimal for deploying custom corporate apps.
  - Enterprise developer programs, private channels, and APKs.



Policy security settings

Mobile Device Policies (Slide 3 of 3)

- Trusted and untrusted app sources:
  - Trusted apps are managed by a service provider.
  - Store model is not optimal for deploying custom corporate apps.
  - Enterprise developer programs, private channels, and APKs.



Access to unknown sources disabled

Mobile Device Security Software

App scanner: A class of security software designed to monitor the permissions allocated to apps and how they are using (or abusing) them.

Firewall app: A firewall implemented as application software running on the host.

- Anti-virus/Anti-malware
- Firewalls
- Patching OS
- Updates

Activity

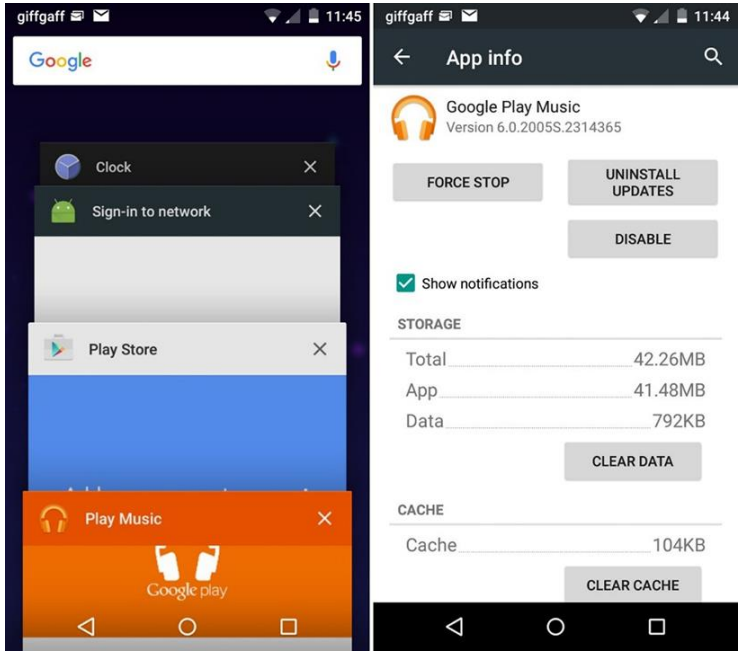
Discussing Mobile Device Security

Supporting and Troubleshooting Mobile Devices

- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Mobile OS Troubleshooting Tools

- Adjust Settings
- Close running apps
  - Force stop
  - Force Quit
- Uninstall and reinstall apps
- Reset the device
  - Soft reset
  - Forced restart
  - Factory default reset



Android Force Stop

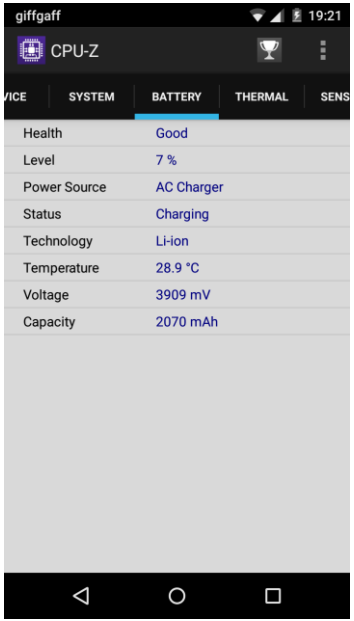
Guidelines for Using Mobile Troubleshooting Tools

- Adjust settings for the core OS and for apps.
- Close running apps that are consuming too much power and draining the battery or those that are unresponsive.
- Uninstall apps that are no longer needed or reinstall apps after replacing a device or after previously uninstalling an app.
- Try a soft reset for devices that are frozen or unresponsive. If that doesn't work, use a forced restart.
- Perform a factory default reset when reissuing the mobile device to another user or preparing it for disposal.

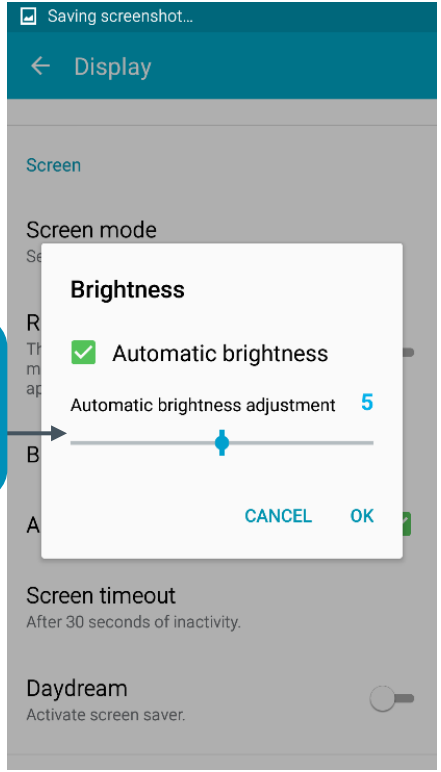
Mobile OS Issue Troubleshooting

- Dim display
- Touchscreen unresponsive or inaccurate
- External monitor issues
- Sound issues
- Overheating

Check for overheating



Check or change display brightness



Guidelines for Troubleshooting Mobile OS Issues (Slide 1 of 2)

- Dim display.
  - Open the **Display** settings and adjust the automatic brightness option or adjust the brightness slider.
  - Check for apps that dim the backlight to conserve power.
- Unresponsive or inaccurate touchscreen.
  - Check for issues with the screen and any screen protectors.
  - Check that there are adequate resources available.
  - Use a re-calibration utility.
- Issues with external monitor.
  - Verify that the cable is good.
  - Verify that a casting dongle is configured correctly between the device and the mobile device.

Guidelines for Troubleshooting Mobile OS Issues (Slide 2 of 2)

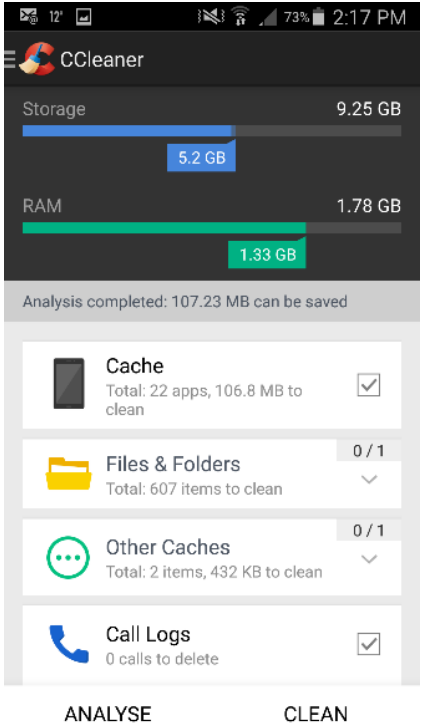
- Sound issues.
  - Verify volume controls are set correctly.
  - Verify silent mode is not enabled.
  - Check volume controls within the app.
  - Verify it is not configured to use external speakers through a cable or Bluetooth.
- Overheating.
  - Determine if the device is being used intensively.
  - Use a battery monitor to view battery status information.
  - Keep the device away from direct sunlight or other heat sources.

Mobile App Issue Troubleshooting (Slide 1 of 3)

- Apps not loading.
- App log errors.
  - Enter developer mode to view log files.

Mobile App Issue Troubleshooting (Slide 2 of 3)

- Slow performance:
  - Resources might be too low.
  - Use an app such as CCleaner.
  - Try soft resets, then factory default reset (as a last resort).
  - Examine recently installed apps.



Mobile App Issue Troubleshooting (Slide 3 of 3)

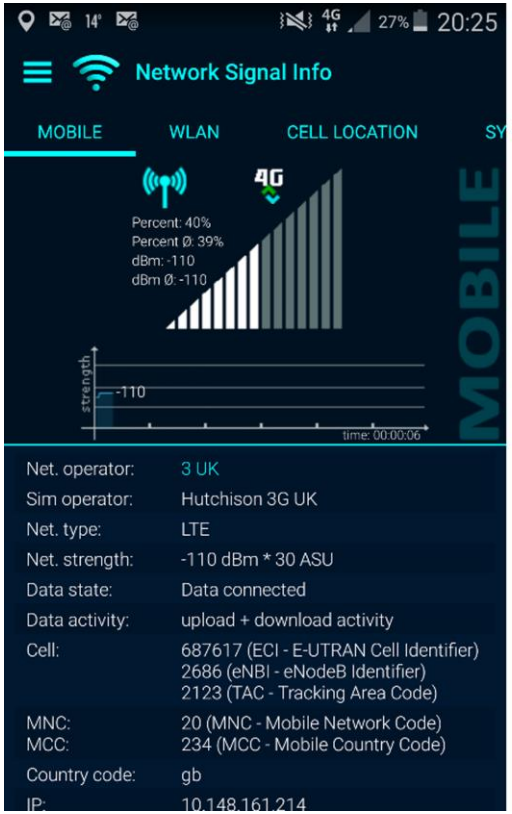
- Battery life:
  - Effectiveness degrades over time.
  - GPU and CPU intensive apps drain a battery quickly.
  - Charge might degrade due to faulty or malicious apps using power-intensive services.
    - GPS, network connections, microphones, and cameras.
  - Uninstall the app, or prevent it from running in the background.

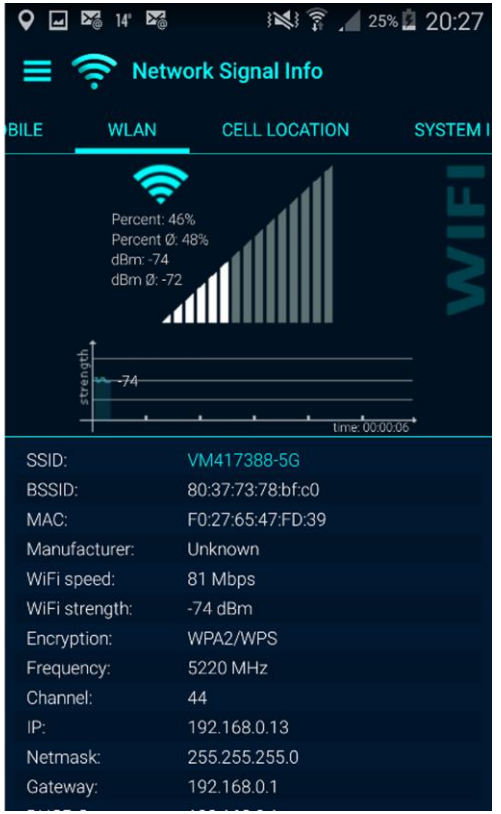
Guidelines for Troubleshooting Mobile App Issues

- If an app is not loading:
  - Verify that it wasn't installed on a memory card that is not in the mobile device.
  - Verify that the app is not corrupted; uninstall and reinstall the app.
- Examine app log files to determine if the issue can be tracked down in the log file.
- Put the device in developer mode to access log files.
- Slow performance:
  - Check for newer apps requiring more resources than are available, reduced battery life, and lack of free storage space.
  - Check that recently installed apps are functioning correctly and are not running in the background.
- Battery life degrades over time. Keep the OS up-to-date to ensure optimum operations and battery life conservation.

Mobile Wireless Issue Troubleshooting

- Issues with any wireless connection type:
  - Wi-Fi
  - Bluetooth
  - Cellular radio
- Determine whether:
  - Configuration error
  - Hardware error
  - Interference problem
    - Wi-Fi analyzers



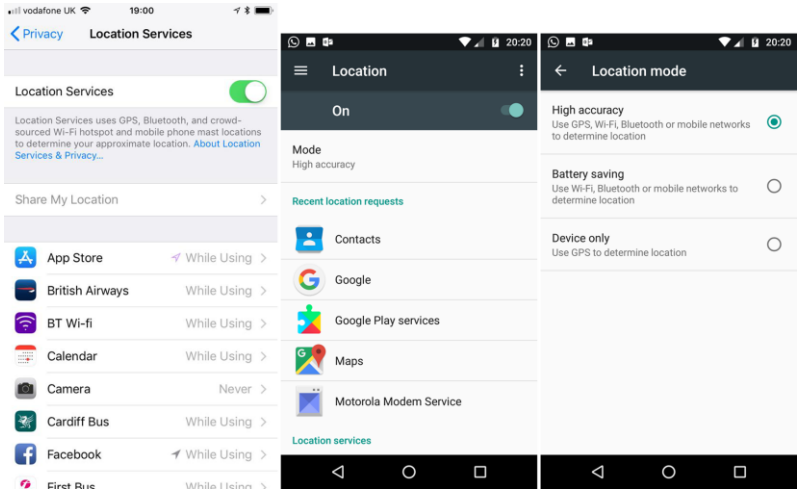


Guidelines for Troubleshooting Mobile Wireless Issues

- Interference issues:
  - Use a Wi-Fi Analyzer app to check for interference and signal strength.
- Configuration issues:
  - Verify that the device is not in airplane mode.
  - Verify that a particular radio service has not been disabled.
  - Use **Settings** to verify that configuration parameters are correctly configured.
  - Verify that the Wi-Fi access point supports the same standard as the mobile device.
- If none of these are the issue, determine if an OS or firmware update is needed.

Mobile Device Security Troubleshooting (Slide 1 of 2)

- Utilization symptoms:
  - Rogue apps running in background can cause power drain and high resource use
  - Sudden data transmission overlimit
  - Unauthorized location tracking
    - Disable location services unless required by apps
  - Install patches and upgrades



Mobile Device Security Troubleshooting (Slide 2 of 2)

- User behavior issues:
  - Careless use
  - Failure to follow security best practices
  - Use of insecure hotspots
  - Unintended Bluetooth pairing
- System lockout:
  - Forgotten password
  - On purpose when the device is reported stolen or lost
- Troubleshooting email problems:
  - Verify credentials and email settings are correctly entered
  - Verify corporate email password change is replicated to mobile devices
  - Use digital certificates to encrypt messages

Guidelines for Troubleshooting Mobile Device Security Issues (Slide 1 of 2)

- If there is a huge power drain or high resource utilization, check for malware or rogue apps.
- Check for unauthorized location tracking.
- Remove geotagging information or metadata from images posted online.
- Ensure users are not engaging in behavior that makes their devices vulnerable to attack.
- If using settings that allow automatic connection to service provider hotspots, verify that the hotspot and device are using trusted, secure connections.

Guidelines for Troubleshooting Mobile Device Security Issues (Slide 2 of 2)

- Ensure unintended Bluetooth pairing is not allowed.
- Ensure users are locking the device when unattended.
- Install apps or enable OS features that allow the phone to be locked and/or wiped if it is lost or stolen.
- Verify that email passwords changed on the enterprise network are replicated to the mobile device.
- When sending and receiving encrypted emails with a digital certificate, use the email client or encryption program's support documentation to install or locate the appropriate certificate.

Activity

Troubleshooting Mobile Device Issues

Reflective Questions

1. In your professional experience, have you supported mobile devices? If not, what kind of experience do you have with them?

2. What type of technical support do you think will be expected of an A+ technician as mobile devices become even more prominent within the workplace?