

12.4 Mobile Devices

As you study this section, answer the following questions:

- What is the difference between a laptop computer and mobile device?
- Which operating systems run on mobile devices?
- What features are commonly included in mobile devices?

Key terms for this section include the following:

Term	Definition
Accelerometer	A tool to detect the physical movements of a tablet by measuring its linear acceleration in one dimension.
Global Positioning System (GPS)	A space-based navigation system that provides location and time information in all weather conditions anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
Gyroscope	A feature that measures the vertical and horizontal orientation of the device.
International Mobile Equipment Identity (IMEI)	A unique number given to each mobile phone. The number is typically found behind the battery.
International mobile subscriber identity (IMSI)	A unique identifier that defines a subscriber in the wireless world, including the country and mobile network to which the subscriber belongs. The IMSI is one of the pieces of information stored on a SIM card.
Software development kit (SDK)	A set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform.
Android Package (APK)	The package file format used by the Android operating system for the distribution and installation of mobile apps and middleware.
Primary Rate Interface (PRI)	A telecommunications interface standard used on an Integrated Services Digital Network (ISDN) to carry multiple Digital Signal 0 (DS0) voice and data transmissions between the network and a user.
Preferred Roaming List (PRL)	A database residing in a wireless device that contains information used during the system selection and acquisition process.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut PC Pro	1.6 Manage mobile devices <ul style="list-style-type: none">• Configure mobile device connectivity

	<ul style="list-style-type: none">• Use common mobile device features
CompTIA A+ 220-1101	<p>1.3 Given a scenario, set up and configure accessories and ports of mobile devices</p> <ul style="list-style-type: none">• Connection methods<ul style="list-style-type: none">◦ Universal Serial Bus (USB)/USB-C/microUSB/miniUSB◦ Lightning◦ Serial interfaces◦ Near-field communication (NFC)◦ Bluetooth◦ Hotspot• Accessories<ul style="list-style-type: none">◦ Touch pens◦ Headsets◦ Speakers◦ Webcam• Docking station• Port replicator• Trackpad/drawing pad
CompTIA A+ 220-1102	<p>1.8 Compare and contrast common operating system types and their purposes.</p> <ul style="list-style-type: none">• Cell phone/tablet operating systems<ul style="list-style-type: none">◦ iPadOS◦ Android◦ iOS

12.4.1 Mobile Device Overview

Click one of the buttons to take you to that part of the video.

Mobile Device Overview 0:00-0:26

In today's world, mobile devices are becoming more of a necessity than a luxury. This is especially true with smartphones, which are the most widely used mobile device. In this lesson, we're going to spend some time looking at the different types of mobile devices you need to be familiar with. We'll also take a look at the common characteristics that all mobile devices share. Let's get started.

Smartphone 0:27-1:13

As we mentioned, the most common mobile device is the smartphone. Smartphones combine the functionality of a cell phone with the features of a desktop computer.

When they were first developed, smartphones were fairly limited in their functionality. But they've since become some of the most powerful and versatile devices out there.

Smartphones access the internet either through Wi-Fi or by using a 3, 4, or 5G cellular connection. They can also serve as a GPS navigation unit, a portable gaming device, or a mobile music player.

Smartphones typically have a screen size upwards of 6 or more inches and a width of 2.5 to 3 inches. With the introduction of expansive screens, you might see a width of 5 or more inches.

Tablet 1:14-1:49

The next mobile device is the tablet. Tablets were some of the first types of handheld mobile devices.

They typically have more computing power than smartphones but are also much larger and more expensive.

A typical tablet screen size is between 7 and 12 inches. Tablets are designed as a type of notebook replacement. While they aren't as powerful as a notebook system, they tend to be more portable, have a longer-lasting battery, and they come with many of the same productivity tools. Most can even connect to a wireless keyboard for easier typing.

Phablet 1:50-2:19

There's another mobile device that's a hybrid of a smartphone and a tablet. This device is called a phablet. Phablets aren't as small as a smartphone and aren't as powerful as a tablet. They're somewhere in between, and they usually have a screen size between 5.2 and 7 inches.

Many phablets use special stylus pens for interaction. This allows more accurate screen tapping for things like writing notes, drawing diagrams, or navigating apps.

Wearable Devices 2:20-2:56

The next category we'll look at are a family of mobile devices that are meant to be worn on the body. As such, they're called wearable technology devices or simply wearables.

These devices range from being as simple as a step-tracking smartwatch to as complex as a virtual reality headset. Most are designed to interface with another device.

For example, a smartwatch by itself has a limited set of functions, but they're also designed to connect to smartphones with Bluetooth. Doing so unlocks additional functionality, like reading texts or answering phone calls through the smartwatch itself.

E-Reader 2:57-3:32

There's one last mobile device we need to look at called an e-reader, which is similar in size to a tablet but lacks the functionality of one.

Their primary purpose is for reading digital books, newspapers, magazines, and other periodicals. Most e-readers use e-ink to display digital content, which is a special technology that creates a high-contrast black-and-white display. Even though they can only display grayscale, these screens are great for e-readers because they consume much less power than LCD, and they don't suffer from visibility problems in bright sunlight.

Mobile Device Power 3:33-4:06

Whether it's a tablet, smartphone, or an e-reader, all mobile devices share some common characteristics. The most common is the power source. As their name implies, mobile devices need to be mobile, so they need to have some sort of mobile power source.

This source is typically a lithium-ion battery, which are rated in milliamp hours. The larger the number, the greater the battery capacity. For example, the average smartphone battery is about 2,000 milliamp hours, whereas a notebook battery is about 6,000.

Mobile Storage 4:07-4:40

Another characteristic is the storage. In order to extend the battery life, mobile devices use some sort of non-volatile flash memory to store information. This type of memory consumes a lot less power than magnetic drives such as those found in desktop and notebook systems. Because there are no moving parts, flash memory is a much more energy-efficient storage medium.

In addition, a lot of mobile devices have expandable storage in the form of microSD cards. This allows these devices to increase their storage to upwards of 1 terabyte or more.

Wireless Features 4:41-4:56

Obviously, mobile devices need to have connectivity to the internet. To do this, they use a variety of wireless connection media.

For example, the typical smartphone uses 802.11, Bluetooth, and cellular wireless technologies together.

Internal Sensors 4:57-5:54

Mobile devices also have internal sensors that collect environmental data. A common example of this is a GPS chip. GPS chips can calculate the device's location, which is helpful for things like navigation apps and location services. Another internal sensor that mobile devices use is called an accelerometer. An accelerometer is a sensor that detects movement on a single plane. In mobile devices, this is typically the horizontal plane. This is the sensor that detects when your smartphone is turned sideways and tells it to change the orientation.

A third sensor to know is called a gyroscope. A gyroscope also detects movement, but it does so a bit differently than an accelerometer. Instead of detecting movement on a single plane, a gyroscope detects both horizontal and vertical movements. If you've ever played a game on your smartphone or tablet that requires you to tilt the device, you've used a gyroscope.

Touchscreen 5:55-6:41

The most common characteristic of a mobile device, though, is the touchscreen. Mobile devices use capacitive touchscreens to receive user input instead of peripherals. The reason is that touchscreens are able to detect multiple contact points.

For example, being able to zoom in on a photo using two fingers is possible only because of the capacitive touchscreen. The one drawback is the fact that these screens require a conductive object, so generally a gloved hand won't work unless it's specially modified.

As we discussed, some mobile devices also use a special stylus. The stylus looks very similar to a pencil or pen but has a special tip that allows you to draw, write, or interact with the device much more accurately than is possible with your finger.

Mobile Operating Systems 6:42-7:23

Another characteristic of mobile devices is the operating system. Unlike notebooks, which use a desktop operating system that contains mobile features, mobile operating systems are designed specifically for mobile devices and with a touchscreen interface in mind. The three most common mobile OSs are Android, iOS, and iPadOS. While there are more than these three, these are the ones you should be most familiar with.

Often times, the decision between purchasing one mobile device over another is largely based on the operating system. The primary reason for this is that each operating system uses its own proprietary app ecosystem, which is another characteristic of mobile devices.

App Ecosystem 7:24-8:41

Software programs that run on mobile devices are called apps. Mobile devices can only use apps that've been written specifically for a particular mobile operating system. This means that an app written for Android won't run on iOS and vice versa.

An app ecosystem is a fancy way of referring to the apps that a particular mobile OS has available to it. For example, iOS and iPadOS use the Apple App Store, Android uses the Google Play Store, and Windows Phone uses the Windows Phone Store. Like most things, each app ecosystem has pros and cons that are largely opinion-based. The main thing to know is that when you purchase a particular mobile device, you're buying into a specific app ecosystem.

One final thing you should be aware of is the fact that most internal mobile hardware components are non-serviceable. This means that if the processor fails, you have to purchase an entirely new device. It's not even possible to replace a faulty battery in some mobile devices. This touches on the fact that mobile devices aren't designed as a complete solution. They're instead designed to be a supplement to other computing devices. So, while they do have a lot of functionality, they have their limitations as well.

Summary 8:42-8:59

Ok, that's all on mobile devices. In this lesson, we looked at the different types of mobile devices you should be familiar with. We also looked at the common characteristics that all mobile devices share, such as power, storage, wireless connections, and touchscreens. And remember, mobile devices use mobile operating systems that each have their own proprietary app ecosystem.

Copyright © 2022 TestOut Corporation All rights reserved.

12.4.2 Mobile Device Facts

This lesson covers mobile devices.

Mobile Devices

The following table describes the most common mobile devices you will encounter.

Device	Description
Tablet	<p>A tablet uses a touch screen interface rather than the touchpad, mouse, and keyboard used by desktop and notebook computers. The touch screen interface is usually capacitive meaning it recognizes fingertip input.</p> <ul style="list-style-type: none">• Capacitive touch screens provide multi-touch or gestures that allow the tablet to recognize simultaneous multiple finger touches.• Many tablets implement a stylus or pen for more precise drawing and control.• Most tablets use the iOS, Android, or iPadOS operating systems.
Smart phone	<p>Smart phones combine the functionality of a cellular phone with the features of a desktop computer.</p> <ul style="list-style-type: none">• Smart phones can access the internet either through a Wi-Fi connection or by using a 2G, 3G, 4G, 5G, and/or LTE cellular connection.• They can also function as a GPS navigation unit, a portable gaming device, and a mobile music player.• Smart phones typically have a screen size between 2.5 inches and 6+ inches.• Most smart phones use the Android or iOS operating system.• Many smart phones can also be used as a mobile WiFi hotspot enabling other devices to access the internet via the phone's WiFi adapter.
Wearable device	<p>Wearable devices are a type of mobile device meant to be worn somewhere on the body. These devices range from a fitness tracker wrist band to virtual reality headsets.</p> <p>Most wearable devices are designed to interface with another device. For example, smart watches are designed to connect to smart phones using Bluetooth. Doing this enables additional functionality, such as reading texts or answering phones calls through the smart watch.</p>
Webcam	<p>Webcams are camera and microphone systems that allow users to communicate through the internet with audio and video. Many laptops have a built-in webcam, but you can purchase one and connect it to the computer through a USB port.</p>
E-reader	<p>E-readers are similar to a tablet; however, they are often used only for reading and do not include many of the apps available on tablets. Their primary purpose is for reading digital books, newspapers, magazines, and other periodicals. Most e-readers use E Ink to display digital content.</p> <p>E Ink is a special technology that creates a high-contrast, black and white display. Even though E Ink screens display only grayscale, they are great for e-readers because they consume much less power than LCD screens and their output can be seen even in direct sunlight.</p>

12.4.3 Mobile Device Connection Methods

Click one of the buttons to take you to that part of the video.

Mobile Connectivity 0:00-0:54

Desktop computers are stationary objects that have external devices connected semi-permanently. Devices like monitors, keyboards, mice, printers, and the like are rarely disconnected. Mobile devices, while they maintain similar ports, connect and disconnect their external components more frequently. In other words, mobile devices are power-packed mini-computers with more interchangeable parts than their full-sized counterparts.

This allows mobile devices to expand their reach with peripherals. Whether with a USB cable or Bluetooth, this expandability is what allows our mobile phones to transmit sound to earbuds or play our favorite tracks on our car stereos. Nowadays, we can even pay our bills with a simple tap to a credit card reader. In this lesson, we'll examine several external devices and their connection methods.

Universal Serial Bus (USB) 0:55-2:47

To start, USB—short for Universal Serial Bus—is a very common connection device that you'll come across. It's versatile and powerful at the same time. Several consumer devices—for example, headphones and cell phones—use USB for their power connection.

USB has several variations. A few of them aren't used as much since they're older and are no longer relevant. That being said, the most common connector for USB is the A connector, which plugs into the computer for data transfer or power adaptation. Then we have the B connector. For years, the B connector was used in end devices for data transfer. To reduce size, USB 2.0 introduced the mini and micro USB connectors. They both look similar, but the mini is slightly larger than the micro.

When USB version 3 was introduced, the data and speed were increased. This brought new B connectors. The standard USB 3.0 connector is stacked and is similar to the classic B connector with another smaller connection on top. The micro USB 3.0 is essentially two connectors in one. It has the same connector as the previously mentioned one but with another smaller connector to its side. These multi-connector configurations allow for faster data throughput.

There's a relatively new connector called USB-C. It's the latest connection type that works for more than just data or charging. We can use it for external monitor and LAN functions as well. It's the fastest and most versatile USB connection so far. Lastly, Apple developed their proprietary lightning connector to connect Apple mobile devices to computers and other external devices. We can use it to charge Apple devices, such as our iPhones, iPads, and iPods.

Serial Interfaces 2:48-3:21

Let's get into serial interfaces, as many devices communicate via serial devices. Routers and switches are often connected with a serial cable that's specifically designed for that purpose. Until recently, both laptops and desktops had these serial interfaces. Today, laptops have done away with them—other than the USB. But desktops often still have a 9-pin serial interface on the back of the system. Devices like modems, printers, and other external components utilize this interface to connect to the computer system.

Wireless Connectivity 3:22-3:24

The next three connection types are all wireless.

NFC 3:25-3:42

Near Field Communication, or NFC, uses inductive coupling to transmit and receive data. The devices must be less than an inch apart to communicate. We often see this in cell phone-to-cell phone communication and contactless credit card transactions.

Bluetooth 3:43-4:14

Bluetooth devices have proliferated the marketplace. Bluetooth is a wireless technology with a 10-meter radius for use with multimedia. There are many manufacturers that utilize Bluetooth technology for their headphones or earbuds. They may also produce Bluetooth speakers to further eliminate the need for wires. Many printers support Bluetooth so they can simply be plugged in without a physical connection to a computer. With a couple of mouse clicks, you can easily print reports, photos, or anything else you need.

Hotspots 4:15-4:44

For most of us, an internet connection is a must. Our phones are constantly connected so that we can send and receive emails, text, and surf the web. Our devices are rarely disconnected, which is why several smartphone manufacturers have enabled USB tethering or hotspot functionality on their phones. With these features, our devices can make our own smartphones their connection point to the internet. You could also purchase a mobile hotspot device that's specifically designed for this purpose.

Summary 4:45-5:08

That's all we have for now on this subject. We discussed mobile device connection methods, including the various types of USB connectors. We also discussed serial interfaces, Near Field Communication, Bluetooth, and hotspots. All-in-one mobile connectivity makes our lives a lot easier. With peripherals and ever-evolving technology, we can expand our reach even further and stay up to speed in our fast-paced modern world.

Copyright © 2022 TestOut Corporation All rights reserved.

12.4.4 Mobile Connection Facts

This lesson covers mobile connections.

Mobile Connections

Most mobile devices share similar design and functionality traits. Most allow for external connectivity via wired and wireless technologies. Many of those traits are described in the following table.

Feature	Description
Universal Serial Bus	<p>Universal Serial Bus (USB) is the most predominant connection type and the most versatile for mobile devices. USB is used to connect most external devices to a PC or tablet. There are different versions of USB:</p> <ul style="list-style-type: none">• USB v2.0—used to connect keyboards, mice, printers, flash drives etc.• USB v3.0—the same as v2.0, but faster. It introduced new type B connectors.• USB-C—a newer technology with different connectivity. It is used for all external devices including displays and Ethernet adapters. <p>USB has three connection types:</p> <ul style="list-style-type: none">• The A connector is generally used to plug into the mobile device.• The B connector is generally used to plug into the external device. It includes:<ul style="list-style-type: none">◦ Standard—older connector used mainly to connect to external hard drives and printers.◦ MiniUSB—smaller version of USB connector used for connections as well as charging external devices.◦ MicroUSB—same as MiniUSB, but smaller.◦ Standard 3.0—dual connection, top and bottom, allowing for higher throughput on capable devices.◦ MicroUSB 3.0—dual connection, side-to-side. It has the same connectivity as Standard 3.0.• The C connector is used for connecting external devices including displays and Ethernet adapters.<ul style="list-style-type: none">◦ It may use type A or C to plug into mobile devices.◦ It uses type C to plug into external devices.
Serial interfaces	<p>Devices that use a serial interface include computers, routers, and switches.</p> <ul style="list-style-type: none">• Serial allows devices to communicate via a stream of binary digits. There may be control signals embedded in the stream to mark the beginning or end of characters or to enable parity.• Many serial connectors are a 9 pin D connector. However, some use a proprietary connector that has a specific use.<ul style="list-style-type: none">◦ While no longer widely used, serial communication was used to connect external serial devices to computers.◦ These devices included printers, modems, scanners, and other serial devices.

Near-field communications	<p>NFC is a newer wireless technology. It is mostly used with credit cards allowing the user to tap the credit card rather than swipe it or insert it into the chip reader.</p> <p>It can also be used to transfer data between mobile devices. NFC's wireless range is less than one inch and uses very little power.</p>
Bluetooth	<p>Bluetooth is a low-power, short-distance wireless technology. It supports a 10-meter radius for connectivity and is usually used for multimedia.</p> <ul style="list-style-type: none">• Often users use Bluetooth with earbuds, headphones, and speakers.• Bluetooth is also used to connect printers wirelessly.• Bluetooth requires devices be paired before they can be used.
Hotspot	<p>Many smartphones can enable a hotspot feature. This feature allows the user to turn the smartphone into a WiFi hotspot.</p> <ul style="list-style-type: none">• The smartphone uses its cellular connection to the internet and provides a WiFi host allowing WiFi enabled devices to connect and use the smartphone's internet connection.• This is useful for any mobile device that does not have direct access to the internet.• Several cellular providers offer devices specifically designed to do this; however, providing a hotspot is their only function. These devices generally sell for a fraction the cost of a mobile phone.

12.4.5 Mobile Device Accessories

Click one of the buttons to take you to that part of the video.

Mobile Device Accessories 0:00-0:26

Most mobile devices are equipped with everything you need to become fully immersed in the mobile experience. But there are some additional items that expand functionality, and they're not always included by default. These accessories give users the ability to hear better, participate in online meetings, and be more efficient. We'll take a look at some of the devices that make the mobile experience better.

Add-Ons 0:27-1:43

Let's start by reviewing a few of the items that many consider must-haves for mobile computing. First, there's headsets. Headsets add a bit of privacy to a conversation. Next, there's touch pens. They provide realistic, fine control for writing. Speakers can be plugged into the speaker output port, or they might be wireless. A webcam can integrate into the mobile device or be plugged into a USB port.

Mobile computers are often a user's primary computer. When you're on the go, you can take the computer along and use its keyboard and display. At home or in the office, you may want the desktop experience with a full-sized keyboard, mouse, and multiple displays. A docking station maintains these permanent connections and provides a dock for the laptop. When it's engaged with a doc, the computer can be used like a desktop. A port replicator provides similar connectivity and generally plugs into one or more USB ports.

Lastly, users may use trackpads rather than a mouse. Many laptops come with a trackpad, so rather than move a mouse around the desktop, the user moves their finger across the pad to move the mouse. Also, a user may use a drawing pad to draw images on the screen.

Headsets 1:44-2:25

Probably the most used accessory is the headset. They come in many forms, such as single ear with microphone, double ear with microphone, and double ear and no microphone. They add a much richer experience for the user, as the sound quality is usually much better than the speakers in the mobile device. Also, the microphone is better quality, so remote users can hear your voice better.

Go into any coffee shop or other public place and you'll often see people with earbuds in their ears. They may be listening to music, having a semi-private conversation, or watching a movie. Bluetooth has eliminated the need for wires, making earbuds easy to use and unobtrusive.

Touch Pens 2:26-2:55

Tablets, mobile phones, laptops with touchscreens, and other mobile devices can benefit from a touch pen. Many believe a stylus and a touch pen are the same, but they're not. Generally, a stylus doesn't contain electronics. Most have a soft rubber tip on the end. A touch pen, or digital pen, is a specific type of pen that usually includes many finer abilities, such as tilt and pressure sensitivity. A touch pen allows users to become more creative with their drawings and writing.

Speakers 2:56-3:10

You might enjoy listening to music while studying or doing your work. Speakers let you listen to your favorite music channel or downloaded music. There are many Bluetooth speakers on the market today that give you the freedom to listen to your music anywhere you happen to be.

Webcam 3:11-3:25

Many laptops come with an embedded webcam in the display bezel. If not, there are several webcams you can purchase that can be clipped on. Webcams are great for attending online meetings, taking still pictures, or recording videos.

Docking Station/Port Replicator 3:26-4:20

Many computer users, especially office workers, might only have a laptop computer. For these workers, it's difficult to utilize the laptop's small display and narrow keyboard. To provide the desktop experience, several manufacturers offer docking stations for laptops. A docking station provides several ports for

connectivity, including HDMI, VGA, USB, and Ethernet ports. With these ports, laptops can utilize full-size keyboards, mice, and displays. In addition, they're generally powered by the same power supply as the laptop.

Similarly, there are many USB-based port replicators that utilize a laptop's USB port to provide the same connectivity as a docking station. Docks are often made for specific models. A port replicator is, generally, more universal and less reliant on a specific manufacturer.

Drawing Pad 4:21-4:42

Some people use their computer for art, and trackpads don't work well for high-quality digital drawings. Instead, they need an external device that provides them more precision. Drawing pads provide that. They're generally powered and come with a pen, and they might include a touch display. There's a wide availability of devices ranging into the thousands of dollars.

Summary 4:43-5:13

In this lesson, we've seen several accessories that many people find useful. Using headsets or earbuds allows for privacy in a crowded room. A drawing pen provides more granular precision when drawing. External speakers produce rich sound for music. A webcam provides the ability to attend remote meetings. A docking station or port replicator provides the desktop experience for office workers. These are just a few of the accessories that users can add to their mobile devices that allow them to become more efficient and have a better mobile experience.

12.4.6 Mobile Device Accessory Facts

This lesson covers mobile device accessories.

Mobile Device Accessories

Mobile phone accessories include hardware or software that is not integral to the operation of a mobile phone as designed by the manufacturer. The following table describes common mobile accessories.

Accessory	Description
Headsets	<p>Mobile headsets allow you to listen to music and answer phone calls. Mobile headsets come in several varieties and options. They include:</p> <ul style="list-style-type: none">• Corded with connections for audio and microphone.• Universal Serial Bus (USB).• Wireless with over-ear and ear buds.
Speakers	<p>Speakers allow you to listen to a mobile device without headphones. You can connect portable speakers to a mobile device using Bluetooth or through the earphone jack.</p>
Gamepads	<p>Gamepads allow you to turn a mobile device into a virtual multi-touch gamepad for PC games through a Wi-Fi or Bluetooth connection.</p>
Docking stations/port replicators	<p>Docking stations and port replicators can provide the desktop experience for laptop computers. Devices (such as keyboard, mouse, and monitor) connect to the docking station; then the laptop connects to the docking station.</p> <p>There are also docking stations/port replicators for other mobile devices such as mobile phones and gaming devices. Standards for each are typically specific to the device docked.</p>
Extra batteries/chargers	<p>Cell phone chargers have gone through an evolution that included cradles, plug-in cords, and (most recently) wireless charging.</p> <ul style="list-style-type: none">• Many devices have micro-USB or USB-C connections.• Apple devices often use Lightning cables.• External batteries can be included in the case (power case). <p>Portable devices go through a constant change, improving as they go.</p>
Protective covers	<p>Protective covers or cases are designed to attach to, support, and hold a mobile device. Protective covers are meant to protect a mobile device from accidental drops, shock, and water. Several cases have convenient straps or handles that make the device easier to hold and use.</p> <p>Protective covers include:</p> <ul style="list-style-type: none">• Pouches and sleeves• Holsters• Shells

	<ul style="list-style-type: none">• Skins• Bumpers• Flip cases and wallets• Screen protection and body films• Leather cases
Credit card readers	A credit card reader allows you to accept credit and debit cards payments through a smart phone or tablet.
Medical accessories	You can use mobile devices with medical technology. Mobile devices use Bluetooth or Wi-Fi technology to communicate with the medical device (e.g., fingertip electrocardiogram (EKG) or continuous glucose monitoring (CGM) for diabetes patients).
Memory/microSD	Some smart phones feature SD card slots, usually for the smaller microSD. You can use SD cards to transfer files from one device to another or to increase the storage capacity of a device.

12.5 Mobile Device Network Connectivity

As you study this section, answer the following questions:

- How do you connect a mobile device to a network?
- How do you synchronize data between a mobile device and desktop PC or laptop computer?

In this section, you will learn to:

- Network mobile devices
- Synchronize mobile devices
- Configure email on mobile devices

The key terms for this section include:

Term	Definition
Bluetooth	A wireless technology standard for exchanging data over short distances from fixed and mobile devices and for building personal area networks (PANs).
Hotspot	A physical location where you can obtain wireless internet access using a wireless local area network (WLAN) with a router connected to an internet service provider (ISP).
Infrared port (IR)	A port on a mobile device that enables devices to exchange data without using cables.
Lightning	A proprietary computer bus and power connector created by Apple Inc. to replace its previous proprietary 30-pin dock connector.
Long-Term Evolution (LTE)	A mobile communications standard used by 5G.
Mobile Virtual Private Network (Mobile VPN)	A VPN that provides mobile devices with secure access to network resources and software applications on their home network. The connection can be wireless or wired.
Near Field Communication Connector (NFC)	A connector that emulates cryptographic smart card functionalities for RFID tags or memory cards.
Tethering	A method that connects one device to another.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut PC Pro	<div>1.6 Manage mobile devices<ul style="list-style-type: none">• Configure mobile device connectivity</div> <div>3.2 Implement mobile device security<ul style="list-style-type: none">• Implement access control and authentication</div>

	<ul style="list-style-type: none">• Implement device encryption
CompTIA A+ 220-1101	<p>1.4 Given a scenario, configure basic mobile-device network connectivity and application support.</p> <ul style="list-style-type: none">• Wireless/cellular data network (enable/disable)<ul style="list-style-type: none">◦ 2G/3G/4G/5G◦ Hotspot◦ Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)◦ Preferred Roaming List (PRL) updates• Location services<ul style="list-style-type: none">◦ Global Positioning System (GPS) services◦ Cellular location services• Mobile device management (MDM)/mobile application management (MAM)<ul style="list-style-type: none">◦ Corporate email configuration◦ Two-factor authentication◦ Corporate application• Mobile device synchronization<ul style="list-style-type: none">◦ Recognizing data caps◦ Microsoft 365◦ ActiveSync◦ Calendar◦ Contacts◦ Commercial mail application <p>2.6 Compare and contrast common network configuration concepts.</p> <ul style="list-style-type: none">• Virtual private network (VPN)
CompTIA A+ 220-1102	<p>1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.</p> <ul style="list-style-type: none">• Metered connections and limitations

12.5.1 Wireless and Cellular Data Connections

Click one of the buttons to take you to that part of the video.

Wireless and Cellular Data Connections 0:00-0:06

In this video, we're going to look at wireless and cellular data connections.

Use Data Connections 0:07-0:38

Today, mobile devices are nearly ubiquitous. It can seem like everyone over twelve years old has a smartphone, and half the people under twelve do, too! But without connectivity, tools like smartphones and tablets are little more than expensive handheld gaming consoles or MP3 players. But when we connect our mobile devices to networks, especially to the internet, we gain all of the same advantages that allowed desktop and laptop computers to participate in the Information Age.

With all that said, let's talk about how we get these devices connected to networks.

Wireless Radios 0:39-2:29

There are several wireless radios in a typical mobile device. A smartphone has a cellular radio for communicating with the mobile phone network towers. This kind of radio is a transceiver. That is, it both transmits and receives.

Another radio found in almost all mobile devices is a Wi-Fi radio transceiver. It allows connection to our wireless LANs and hotspots. Along with finding Wi-Fi on devices, we usually find Bluetooth connectivity on mobile devices these days. While Wi-Fi is directly for connecting to local area networks or wide area networks, Bluetooth is for personal area networks, or PANs.

Lastly, we have the GPS receiver. The Global Positioning System, GPS, is a worldwide network of satellites that help us with navigation. Just a couple of decades ago, we had to buy separate GPS receiver devices, but now we find GPS capabilities built in to most smartphones, many tablets, and a few laptops.

It's also important for all users, not just IT pros, to know how to turn on and off these networking devices. Airplane Mode is a very helpful tool for quickly disabling all of the transmitters. It's so named because the FAA requires us to turn off all transmitters during takeoff and landing for safety reasons. If you've flown recently, you may've heard an announcement from the crew that it was time to turn on Airplane Mode. After reaching 10,000 feet in altitude, they probably said something like, "It's now safe to turn on Wi-Fi." Later in the flight, you once again heard that you had to go back to Airplane Mode for landing.

All phones, tablets, laptops, and other devices have a setting option for Airplane Mode and also for selectively enabling and disabling any of the other radios. You can even disable the GPS receiver by turning off location services, but we'll talk more about all of this shortly.

Cellular Connections by Generation 2:30-4:17

The original mobile phones were analog. While we didn't use the term "first generation" while they were in use, in 1991, we moved to digital mobile phone technology, and the term "second generation," or 2G, was born. 2G is Global System for Mobile Communication-, or simply GSM-based. The 250 kilobits per second speed seems like a snail's pace by today's standards, but it enabled internet access in a way that had never existed before. It also added the SMS and MMS messaging services, leading to the "Why don't they text instead of call?" revolution.

As one might surmise, 3G followed 2G. With every generation, we get improvements, like Universal Mobile Telecommunications System—or UMTS—and speeds up to 7.2 megabits per second. These speeds allowed things like video conferencing and mobile television experiences.

At the time of this video, 4G is the most common deployment for mobile phone connections. We get the term Long Term Evolution—or LTE—with 4G, although it's often only used as a marketing term. With speeds up to 150 megabits per second, things like HDTV and 3D TV became possible. While moving in a car, 4G can still maintain up to 50 megabits per second, so high-bandwidth mobile communications are available while actively moving as well!

The latest and greatest is the much-vaunted 5G. It promises speeds greater than 10 gigabits per second, which means it'll rival land-based practical speeds when connecting to Wi-Fi that's on a DSL or cable line. 5G still has a long way to go as it spreads from the urban centers along major freeways, but it brings great promise to more rural areas that are slower to receive fiber optic internet.

GSM vs. CDMA 4:18-5:26

Before we leave the generations discussion, let's talk briefly about GSM versus CDMA. GSM uses time division multiple access—or TDMA—to share the available space for data on a specific frequency channel. Essentially, each connection is given a short chunk of time to transmit and receive, and then it goes to another connection. With the speed of digital transmissions, these little hops from one to the other are imperceptible to us as we use our phones.

Code division multiple access—or CDMA—is a different technology. All the connections are transmitting and receiving simultaneously, but each one has its own code that allows the system to split them into individual channels. In the USA, Verizon and Sprint are the big names that use CDMA.

Another big difference in the pre-4G LTE days was the SIM card. GSM phones used SIM cards. CDMA phones didn't. Now that we are in the 4G days—and with 5G growing quickly—the differences are less important. To make roaming—especially international roaming—easier, phones are being built with both sets of capabilities.

Hotspot 5:27-7:01

With all of these high-speed connections and technologies available on our mobile devices, we can go a step farther than simply using the data plan on the device itself. We can share these connections with other devices as well through hotspotting. With a hotspot, you can share your mobile device's internet connection through the data plan with your mobile phone provider. Using either a separate hotspot device—often purchased from your mobile service company—or through your phone or tablet, you can set up a mobile wireless access point. It's important to note that if you're using something like a phone or tablet, you'll need to go in to the settings, enable the hotspot, and tell whoever is going to connect what the pre-shared key will be. Typically, you can edit the network name and pre-shared key to your own preference. Remember, just like setting up the wireless access point in a SOHO router, a strong passphrase is the key to security.

Also, always remember that the limits on your hotspot, such as bandwidth, speed, and cost, are determined by your mobile phone service provider and the plan you have with them. If you bust your data plan cap, you may find yourself subject to some surprise charges—unless you already pay for unlimited data. And even if you have unlimited data, that doesn't mean you have the full bandwidth for it all. Most providers give full bandwidth up to a certain point and then throttle the speed after a certain data limit. To save yourself from surprises, you can set certain apps to only use data when connected to Wi-Fi or not to use data when on metered connections. We often find these kinds of settings available on apps that are used for data backups and synchronization, especially for large files like pictures and videos.

PRL Updates 7:02-8:27

One of the greatest benefits of mobile devices is hidden inside the very name mobile. Not only are these devices mobile, but they're moveable, as mentioned earlier. To give a bit more context on that odd sounding statement, let's talk about the Preferred Roaming List—the PRL. When we move a phone, tablet, or other mobile device from place to place, it connects to the nearest tower that works with its cellular connection technology and through the mobile service provider. But what happens when I move the device while it's in use? If I stay within the home area of my phone company, I don't have to worry much about the phone switching from one tower to the next, but I don't always stay in my provider's home area. I like to travel, and sometimes that means being outside that area. My phone—or other mobile device—needs to know how and when to connect to a different provider's network. Some providers partner with each other to keep roaming fees down for their customers. Other providers don't. The PRL lets the phone know what to do outside its home area. Should it connect to non-partner towers and let me incur fees? Should it just wait until I am back in the home or partner service area?

Once upon a time, back in the flip phone days, we had to manually do these updates on our phones. Now, phones do the updates automatically, so those decisions about whether or not to connect to any given tower are answered by the combination of my roaming preferences in the settings and the PRL updates.

Location Services 8:28-9:23

Speaking of roaming, another great feature on nearly all smartphones is location services. There's an old saying, "Not all who wander are lost." Using services, such as GPS, helps us keep from getting lost when we choose to wander! Thanks to smartphones, most of us have GPS location services riding around in our pockets or bags. We no longer need to purchase dedicated GPS devices.

In addition to GPS, we also have cellular location services. Every cell phone tower has a mapped location and service area. The service areas overlap, so a phone's location can be determined by its ability to connect to the towers in the overlapping area. This helps increase the accuracy of GPS, but it also is good for helping to locate a lost or stolen phone if the GPS has been disabled. Just keep in mind that we do need to keep our location services enabled to take advantage of these features, although many of us turn them off to help save battery.

Summary 9:24-9:35

This brings us to the end of this lesson. In this lesson, we discussed the types of wireless connections, the 2G through 5G generations of cell phones, hotspotting, and the two big things to keep in mind when a mobile device is moving around—PRL and location services.

12.5.2 Wireless and Cellular Data Connections Facts

This lesson covers mobile connection types.

Mobile Connection Types

The following table describes mobile connection types.

Connection Type	Description
Generations (G)	<p>Cellular networks used for voice and data include the following types:</p> <ul style="list-style-type: none">• Second generation (2G) networks were the first to offer digital data services. 2G data speeds are slow and mainly used for text messaging, not internet connectivity. 2.5G supports speeds up to 144 Kbps.• EDGE (also called 2.75G) networks are an intermediary between 2G and 3G networks. EDGE is the first cellular technology to be truly internet compatible. EDGE supports speeds of 400–1,000 Kbps.• 3G offers simultaneous voice and data. Minimum speeds for stationary users are quoted at 2 Mbps or higher. The following extensions enhance 3G networks:<ul style="list-style-type: none">◦ Evolved High Speed Packet Access (HSPA+) is also called smart antenna. It uses multiple-input and multiple-output (MIMO). It significantly increases data throughput and link range without additional bandwidth or increased transmit power.◦ Long Term Evolution (LTE) increases downlink/uplink speeds to 100/50 Mbps, while LTE-Advanced increases downlink/uplink speeds to 1Gbps/500Mbps.• 4G is available with minimum speeds around 3–8 Mbps and over 100 Mbps possible. 4G features include:<ul style="list-style-type: none">◦ Uses MIMO.◦ Is not compatible with 3G; 4G requires a complete retrofit on the part of service providers and new equipment for the consumer.◦ Utilizes Worldwide Interoperability for Microwave Access (WiMAX). WiMAX delivers high-speed internet service (up to 1 Gbps for stationary users) to large geographical areas.• 5G can achieve speeds twenty times faster than 4G with peak speeds of 20 Gb per second. 5G features include:<ul style="list-style-type: none">◦ Uses MIMO.◦ Includes lower frequencies than previous generations, down to 600 MHz.◦ Uses LTE for wireless connections.
Hotspot	<p>A hotspot is a physical location where you can obtain wireless internet access using a wireless local area network (WLAN) with a router connected to an internet service provider.</p>
Tethering	<p>Tethering is connecting one device to another to share the internet connection of the phone or tablet with other devices like laptops. You can tether devices over wireless LAN (Wi-Fi), Bluetooth, or by physical connection using a cable, e.g., USB.</p>
Airplane mode	<p>Airplane mode is a setting that suspends the device's radio-frequency signal transmitting functions and disables telephone, Wi-Fi, and Bluetooth. This setting is available on many smart</p>

	phones, portable computers, and other electronic devices.
Virtual private network (VPN)	A mobile VPN provides mobile devices with wired or wireless access to network resources and software applications on their home network.
Bluetooth	Bluetooth is a wireless technology standard that connects multiple devices and avoids problems of synchronization. You can use it to exchange data over short distances from fixed and mobile devices, and for building personal area networks (PANs).
Near-field communication (NFC)	An NFC connection offers low-speed communication to bootstrap two electronic devices in near space of 4 cm or less. NFC can emulate keycards, electronic identity documents, or memory cards.
miniUSB microUSB	<p>A mini-USB connector is a small USB cable connector that is often used by handheld electronic devices like mobile phones, MP3 players, and digital cameras.</p> <ul style="list-style-type: none"> • On mobile phones it is used for both USB data connectivity and charging. • The new connector, called micro-USB, is smaller than the mini-USB connector and allows for even thinner device designs
Lightning	Lightning is a proprietary computer bus and power connector created by Apple. It replaces the previous 30-pin dock connector. You use it to connect Apple mobile devices like iPhones, iPads and iPods to host computers, external monitors, cameras, USB battery chargers, and other peripherals.
Infrared (IR)	An IR port is a port on a mobile device that enables devices to exchange data without using cables.
Metered connections and limitations	<p>A metered internet connection uses a wired or wireless adapter to limit the amount of data a computer can receive per day or month, depending on the plan.</p> <ul style="list-style-type: none"> • When you use both adapters, you can set both to metered or set just one, depending on what you need. • Some metered connections allow you to throttle (slow down and stop) internet usage as you get close to the limit. • Throttling helps prevent you from going over the limit and being charged for extra data usage.
Cellular location services	<p>Cellular Location Services allow apps to track the device's approximate position. They may use GPS, Wi-Fi, cellular, Bluetooth data, QR codes, or RFID technology. You have the option to allow or disallow apps from using location tracking. Keep in mind:</p> <ul style="list-style-type: none"> • Some apps with services such as ridesharing, directions, and delivery depend on this tracking to function. • When you choose to disallow them from tracking you, their services might be very limited. • You can personalize services to your needs by choosing which apps track your location and which don't. • You can also set the permission to allow tracking only while an app is open. Once you close it, the service can't track the device.

	<ul style="list-style-type: none"> Some apps may track location for advertisement, entertainment, or security purposes.
Global Positioning System (GPS)	<p>GPS is a navigation system made of several satellites, a receiver, and algorithms to determine position and/or travel paths using location, velocity, and time data.</p> <ul style="list-style-type: none"> The receiver measures the distance to each satellite by the amount of time it takes to receive a sent signal. After receiving the results from several satellites, it determines the position and displays it electronically. It can also determine the path taken since it started tracking and the path that should be taken depending on the desired destination.
Preferred Roaming List (PRL)	<p>PRL is a database in Code Division Multiple Access (CDMA) wireless devices. The information is used during the system selection and acquisition process.</p> <ul style="list-style-type: none"> In the case of cellphones, it's built and provided by the carrier to connect the phone to the tower. It dictates which radio bands, sub-bands, and service provider IDs the phone will search for. Then, it connect to the right tower. Without a correct and valid PRL, the phone can't roam outside the home network and may not be able to connect at all inside the network. The database is made of an acquisition table listing the radio frequencies to search for in certain areas. It has a system table to tell the phone which towers allow connection and the best order. It doesn't mean the phone will always connect to the strongest tower available. When you're in an area with weak, but steady signal from your carrier, the PRL will connect you to your carrier signal instead of connecting to a stronger signal on a different carrier.
Global System for Mobiles (GSM) vs (CDMA)	<p>CDMA and GSM are older radio systems also known as 2G and 3G.</p> <ul style="list-style-type: none"> These networks are slowly fading away and being replaced by 4G and 5G. Most cell phones are already on 4G and 5G. Some older model phones may still use 2G and 3G, but may experience poor call quality as more and more providers formally shutdown these older networks. <p>Both CDMA and GSM have multiple access standards that allow multiple calls to go through a single tower.</p> <ul style="list-style-type: none"> Some noticeable differences between these two systems is that GSM devices come with a SIM card slot, but CDMA devices do not. This means CDMA phones are a handset-based standard, with a phone number linked to a particular device. To upgrade to another phone, a person must contact the network carrier, de-activate the old device and activate the new one. GSM devices have the phone number linked to the SIM card. To change devices, you take out the SIM card from the old device and place it into the new device.

12.5.3 Networking Mobile Devices

Click one of the buttons to take you to that part of the video.

Networking Mobile Devices 0:00-0:11

In this demonstration, we're going to practice working with network settings on an iPad.

Let's begin by configuring an 802.11 Wi-Fi wireless connection.

802.11 Wireless Connection 0:08-1:09

To connect this iPad to an 802.11 wireless network, I need to come down here, to Settings, and then I need to select Wi-Fi.

You'll notice that I'm already connected to a network named NotYourWireless. You can tell that by the little blue checkmark that's located next to the network name. Now, if I need to connect to a different network, I have two different options for doing so.

First of all, if the network is broadcasting its network name, then it will appear under Choose a Network. As you can see here, I have another network called Tampico. If I wanted to connect to it, all I would have to do is tap on it and then provide the appropriate passphrase. But please be aware that there are a lot of wireless networks that, for security reasons, do not broadcast their SSID. If that's the case, you will not see that network listed under Choose a Network.

The wireless network is still there, and you can still connect to it. You just can't see it under Choose a Network. If this is the case, then you'll have to use another option to manually connect to that wireless network.

Wireless Network Connection 1:10-2:30

So, let's take a look at using the first option, where we connect to a wireless network that's broadcasting its SSID.

To do this, I simply tap on the network that I want to connect to. In this case, that's the Tampico network. I have to enter the passphrase to connect. And then I tap Join. Now you can see that I'm connected to the Tampico wireless network instead of the other one, and you can tell that because there's a little blue checkmark next to Tampico now.

If you want to see the IP network configuration parameters that were assigned to the device when it connected to the wireless network, I just have to tap the little blue information icon. When you do, you can see how this connection is configured.

First of all, you can see that I'm connected automatically using DHCP and that I received an IP address from DHCP 192.168.1.106. My subnet mask is 255.255.255.0. My default gateway router is 192.168.1.1.

I tap on Configure DNS, and you can see my DNS settings.

Now, you're not stuck with using DHCP.

If I wanted to, I could come over here and select Automatic. Using a static option, I would then manually assign my IP addressing parameters.

But in this case, I really don't want to. I just want to go ahead and use DHCP. So we'll go back, and we'll leave it set that way.

Forget This Network Option 2:31-3:24

Before we leave this screen, there is one other option that I want you to pay attention to. That's the Forget This Network option at the very top of the screen.

The key thing to remember with most mobile devices is that when you connect to a wireless network, the device will automatically remember that network and try to connect to it automatically the next time that network comes into range, and there may be times when you don't want that to happen. If this is the case, then you can tap Forget This Network at the top of the screen. When you do, the passphrase that you use to connect to that wireless network will be deleted. Of course, to connect to it again, you'll have to manually specify the appropriate passphrase again.

In the case of my networks, they're broadcasting its SSID. So even if I were to tap Forget This Network, they'll still appear in the list of available networks under Choose a Network on the previous screen. But the passphrase would be gone, so I'd have to enter that passphrase again to reconnect.

Network Not Broadcasting SSID 3:25-4:58

So, let's suppose you need to connect to a wireless network that's not broadcasting its SSID, which, as I said before, is pretty common. In that case, you need to tap Other down here under Choose a Network. The first thing you're prompted to specify is the name of the network you want to connect to. In this case, let's connect back to the first wireless network that we were using before, which was named NotYourWireless.

As you saw earlier, the NotYourWireless network really is broadcasting. But let's say, for demonstration purposes, that it was a functioning wireless network that was not broadcasting. The administrator turned off SSID broadcast for security reasons.

In this situation, I would enter the name of the network in the name field. Then I would need to specify what type of security that network is using. Currently, it's set to None. I'm going to tap None so I can see a list of security options. I happen to know that this particular wireless network uses WPA2 personal, so I'll tap WPA2, and then we'll tap Other Network to go back. And now you can see that WPA2 is selected for the security mechanism.

The last thing I need to do is type the WPA2 passphrase that's used to connect to that network.

At this point, we're connected to the NotYourWireless network as before. If we want to see what IP address has been assigned to this device via DHCP again, we tap on the little blue information icon, and we now have new IP address information, which is different from previously because this is a different wireless system.

At this point, we've configured this iPad to connect to an 802.11 Wi-Fi network.

Summary 4:59-5:02

That's it for this demonstration. In this demo, we talked about how to configure mobile device wireless network settings.

12.5.4 MDM and Synchronization

Click one of the buttons to take you to that part of the video.

MDM and Synchronization 0:00-0:09

In this video, we're going to look at mobile device management and then also look at mobile device synchronization.

Mobile Device Management 0:10-0:41

When we talk about mobile device management, or MDM, we're talking about corporate networks that have mobile devices allowed on them and how we manage those devices. It's not just a managerial concept, but the name for an actual technology. We have MDM software from many vendors, including from those who manufacture the phones and from the phone service providers themselves. MDM solutions help us manage our networks by giving us the ability to control phones and tablets remotely in the same way we control desktops, laptops, and servers remotely.

MDM and MAM 0:42-1:02

Mobile device management and mobile application management are closely related concepts, so maybe a Venn diagram will help. Mobile device management is the overall concept. Mobile application management is a subset of mobile device management. That is, we manage the applications on the devices through our MDM systems.

Corporate Email Configuration 1:03-1:38

There are many similarities between corporate email configuration and personal email configuration, but there are also some important differences. Like personal email, you'll need to know the user ID and password. Unlike personal email, though, you might also need to know information like the mail servers' IP addresses, the incoming mail protocol—either IMAP or POP—and the security settings for things like email encryption. Some corporate email servers even go so far as to differentiate between email address and user ID, so make sure you look out for that little detail! It doesn't happen often, but it'll throw you for a loop when it does.

2FA 1:39-2:53

Speaking of email security settings, what about other security settings, such as how we access the device and data? As a best practice for cybersecurity, you should enable two-factor authentication on all the company's mobile devices. You'll do this through your MDM system.

Let's review the authentication factors and what we mean by two-factor authentication. The first basic authentication factors are something you know—these are things like usernames, passwords, and PINs—and something you have—which are things like physical tokens and smart cards. Keep in mind that a something-you-have token can include an app on your phone. Just because it generates a number that resembles a PIN doesn't make it something you know. You didn't know it until the app gave it to you, so it's something you have.

The other authentication factors are something you do, which includes pattern recognition, like sophisticated software that can track the way you make keystrokes. Then there's something you are, which is biometrics. The most popular are fingerprints and facial recognition. Lastly, there's somewhere you are, like geotagging or geofencing based on location services—but it's not limited to just GPS-like things. You can use a network IP address to define somewhere you are.

Corporate Applications 2:54-4:09

Earlier, I mentioned that mobile application management was a subset of mobile device management, so let's talk a little about corporate applications. All application management can be done through the MDM system, but there can be a bit of contention when it comes to phones owned by employees versus those owned by the company. Company-owned phones are relatively easy to manage by virtue of the fact that the company owns them. The company gets to do what it feels like with what it owns, right?

But when it comes to a Bring Your Own Device, or BYOD, type of situation—which is where the employee owns the phone that's being allowed on the corporate network—things get more complex. We have to ask questions about ownership rights and data jurisdictions, and the answers to those questions aren't always simple and clear, so we address it with the use of things like corporate apps on our personal devices that segregate a portion of the phone's storage to be used exclusively by the app. The employee can use the corporate app to access things like email, office software, and data on a company

server, but keep it entirely separate from their personal apps and data on the same device. The company then has 100% control over everything governed by the company app, while the rest of the device is free for the owner to use.

Mobile Device Synchronization 4:10-6:19

Now that we have our email set up, we've secured our devices with two-factor authentication, and we're managing the applications and settings remotely through MDM, how do we manage to update our data without worrying about duplicates? After all, mobile devices aren't always connected to a reliable network 100% of the time. Using mobile device synchronization, we can make sure that all data is up to date on a mobile device, a workstation, or server.

Tethered synchronization is one of the oldest methods. You simply connect the appropriate data cable from the mobile device to a computer. Using software that comes with the computer's operating system or third-party software, anything that's been updated on the mobile device is updated on the computer, and vice versa.

More commonly these days, we use untethered wireless methods to synchronize data to or through the cloud. Whether through Wi-Fi connections or through our phone service provider's networks, our mobile devices often automatically synchronize with our accounts. If you want to watch this happen live, open the Apple Calendar on your iPhone or Google Calendar on your Android and then open up the calendar in a web browser on a computer. Create a new appointment on the phone. Within a few seconds, you should see that appointment show up on the calendar in your browser. As some jokingly say, it happens "automagically"!

Before we move on to the types of data that we sync, I want to tell you—or possibly warn you—about another type of syncing. Modern automobiles are often Bluetooth-enabled and use the car's audio system to act as a speakerphone system for your mobile phone. When you pair your phone to a car, there's usually an option to sync the contacts list. That way, you can use the car's audio system for voice commands, like "Call Mom" or "Navigate to work." By doing so, you're making a copy of your contact list that stays in the car until you clear it. This can be problematic with rental cars, as someone else will rent the same car later and could get a copy of your entire contact list. It's not just buyer beware, but renter beware! It is also something to keep in mind with your own car, as you might just sell it or trade it in in the future.

Sync Software 6:20-7:31

Before we move on to the types of data that tend to get synchronized, let's talk briefly about a couple of popular syncing platforms. First, I'd like to mention Microsoft 365, formerly known as Office 365. When a corporate user is logged in to Microsoft 365, changes made in the cloud through a browser-based app and changes made on a local device—mobile or otherwise—through a downloaded and installed app will synchronize. You can work in an Edge browser, the Word app on your phone or tablet, or the full-function Word program on your computer and they will all synchronize the data to Microsoft 365.

Microsoft also offers ActiveSync, which primarily synchronizes Outlook information, such as email, contacts, calendar events, and so forth. It includes many capabilities, but it no longer supports remote synchronization. According to the Microsoft website, "Remote PC Sync (via WiFi or LAN) has been removed due to Enterprise customer feedback around security issues." It still works well as a Mobile Device Management service to set password policies, locking, and remote wiping, as well as to control which types of mobile devices can synchronize with your organization.

Synced Data Types 7:32-7:59

When we sync our mobile devices, there are a variety of data types that synchronize with the system. We can expect our applications, email, pictures, music, videos, bookmarks, documents, location, social media data, E-books, and even our passwords to sync with our various systems. You should keep all this in mind when deciding exactly which types of data to sync, as you and your company may have specific privacy concerns about one or more of these categories.

Special Concern 8:00-8:15

Remember, we're especially concerned about data privacy when it comes to email, calendars, and contacts. Personally identifiable information, personal health information, and maybe even financial information could be gleaned from these, as well as corporate data that could be valuable to a competitor.

Summary 8:16-8:34

That's it for this video. In this video, we looked at the difference between MDM and MAM in managing our applications and data. We discussed corporate email configuration, including two-factor authentication. We then discussed corporate applications and mobile device synchronization. And we finished up by discussing software synchronization and being careful with any private data.

12.5.5 Synchronize Mobile Devices

Click one of the buttons to take you to that part of the video.

Synchronize Mobile Devices 0:00-1:20

In this demonstration, we're going to talk about how you can synchronize data between a PC system and a mobile device. For this demo, I've connected an iPad to this Windows 10 system. When I did this, the iTunes app, which allows me to synchronize data between the iPad and the desktop, automatically opened.

We're going to focus on how to synchronize data using an Apple device. If you're using a device from a different manufacturer say, an Android device, or maybe a Microsoft Surface tablet--then the steps you follow will be different.

There are multiple ways we can connect this iPad to this PC system. One option is to plug the mobile device directly into the system with a USB cable. That's what I've done in this instance. There are other ways to connect the two devices together.

Another option is to come down here, under Summary, and turn on Sync this iPad over Wi-Fi. Using this option, I can get rid of the USB cable and just synchronize the iPad to the PC using a wireless connection.

There is a third option, and that's to synchronize data from this iPad and this computer system to the same iCloud account. Using this option, the data from the iPad and the data from this computer system are both copied up to a cloud server on the internet. Then we can share data back and forth between them. We'll talk about how to do that later on in this demo.

Sync Though Direct Connection with USB 1:21-3:49

For now, let's talk about synchronizing data using a direct connection via USB.

Now, notice, down here, one of the synchronization options we have is to back up the iPad. When you do this, the data on the iPad is copied over to the PC to protect it and you have two different options. One is to back it up to the computer itself, and that's selected by default. The other option is to back it up to your iCloud account. We'll talk more about how that works later on in this demo.

With this option, the data is copied over the USB cable to the PC. And then, the data is copied up through an internet connection to a cloud server hosted by Apple. I also have an option to manually back up the data. I can just click the Back Up Now button, and then the data on the iPad will be copied over to the PC.

The way this works is I go to my iTunes store, and I purchase various items that I want to put on my iPad.

Once they're on the PC, I have to get them over to the iPad. To do this, I can come over to my settings and specify what it is I want synchronized.

For example, if I want to synchronize music files that I've downloaded, I click on Music and then click the Sync music option. Then the music files that I've purchased and downloaded to the PC will be copied over here to the iPad. Now, notice, we have the option to synchronize all the music in my music library, or I can just say I only want certain songs copied over to the iPad.

I will point out, before we go any further, if you come back to Summary and scroll down, there's an option here called Manually manage music and video. This option is not selected by default. If it's turned off, then everything is going to be synchronized automatically as soon as the iPad is connected to the PC system, and there may times when you really don't want that to happen. You want to filter what actually goes onto the iPad. If you want to do that, which is what I usually do, turn this option on right here so that you can manually manage the video and music files that end up getting synchronized over here, to the iPad.

You can also synchronize your movies. Come over here and mark this option to sync movies. You can specify which movies you want synchronized. You can synchronize TV shows. You can even synchronize photos.

If we come over to Info, you can also see that you can synchronize bookmarks. If you go to Other, my bookmarks are being synced automatically.

Now, any time you make changes in the configuration, you need to come down here and hit Apply. Also, make sure you sync before disconnecting.

Sync Through the Cloud 3:50-5:02

So, that's one option for synchronizing data the PC and the iPad. The other option is to use the cloud. Instead of directly connecting the iPad to the PC, we can instead configure both the PC and the iPad to use the same iCloud account, and that allows us to share data between the iPad and the PC system. Let's take a look at how that works.

To use iCloud to sync data, you have to configure both the computer system itself as well as the iPad to use the same iCloud account and put in my user account information.

To do this, I'm going to tap on settings. And then, under Settings, I need to make sure I have my user account selected, and I want to go over to the right and tap iCloud.

So, I need to then set up this iPad to use the same iCloud account as I use for my PC system, and I've already done that. And then I need to come down here and specify what information I want to be synchronized. For example, I could tell it to synchronize photos. I can synchronize my email. I can synchronize my contacts, calendars, and reminders, my Safari browser information, notes, and so on. By doing this, all of this information will be copied up to my iCloud account, and then I can access that same information using the iCloud client on my desktop PC system.

Summary 5:03-5:06

That's it for this demonstration. In this demo, we talked about how to synchronize data between a PC system and a mobile device.

12.5.6 Configure MDM Solution

Click one of the buttons to take you to that part of the video.

Configure an MDM Solution 0:03-0:28

In this demonstration, we're going to look at mobile device management, or MDM, and mobile application management, or MAM. Before we begin, be aware that there are many tools available to provide management services for mobile devices. Although they won't have the exact same settings, it's all the same general idea. For this demonstration, I'll be using Microsoft's Intune product.

Why MDM and MAM 0:29-1:39

Let's first talk about some broad mobile device management generalities. In most cases, the point of MDM and MAM is to ensure that work-related content that's viewed on a phone, tablet, or laptop is secure from unauthorized access. This means that there needs to be rules to define which precautions to take. These are usually things like enforcing the need for a password, pin, or biometric—a fingerprint or face scan, for example—be used to unlock a device. Another rule might require that access to certain tools be guarded by multi-factor authentication. There are many other possibilities.

In addition to having a rule or policy like this, there must be a method on each device for those settings to be enforced. Sometimes, it's built into a device's operating system. Other times, a specific application has to be installed. You'll have to tweak things depending on the platform—iOS, Android, Windows, Mac, Linux, etc.—but that comes with the territory.

Let's look at a couple of examples of how device management is handled in Intune. Again, remember that this is a look at a single tool.

Configure MDM Policies on Intune 1:40-3:27

Okay, I've logged in to Intune. On the left is a **Devices** option. I now see links for the various possible platforms that I might need to manage. I have Windows, iOS/iPadOS, macOS, and Android. I'll click on **Android**. Currently, I have no devices configured. Before I can do that, I have to create a policy to define what I want to allow on Android devices that connect to my network.

Clicking on **Compliance policies**, I can see that I currently have only one defined. I'll click the **Create Policy** button, select the platform, and click **Create**. I'll give it a name and click **Next**. Under Compliance settings, I have several categories to work with. For example, under Device Health, I can configure that Google Play Services must be configured on a device before it can have access to my corporate tools. I can also prevent rooted devices from connecting. Under System Security, I can mandate that the data storage on the device be encrypted. I can also block USB debugging to prevent physical developer-level access to the system through USB.

On the Actions for noncompliance section, I can specify how to notify a user when their device is out of compliance. I can give them a number of days before they're locked out, with warnings.

Under Assignments, I can take a group of users and apply the policies that I've created for them. I can have multiple policies, for example, for the sales department or for the executives. This allows flexibility when people access sensitive corporate data from their mobile devices.

The previous pieces we've discussed have been about mobile device management.

Configure MAM on Intune 3:23-4:30

Now, let's look at mobile application management. Intune has an Apps component as well. I'll click on that. Notice that there's a list of platforms, much like in the Devices section. Clicking on **Android**, a list of applications is shown that'll be pushed down to the managed devices. In this case, the Adobe Acrobat Reader app is allowed to be installed. To add an application, I click on **Add** and then select the type of app—whether it's found on the online app store or a web link—and include it on the devices. The last one—the web link—allows for corporate apps to be downloaded and installed, should that be necessary.

Again, the point of all this is to ensure security for corporate tools and data. One last point to consider is that most of the utilities that perform device and application management provide a way to wipe a device if necessary. This means that if a device were lost, you could scrub all corporate data from it remotely, preventing information from falling into the wrong hands.

Summary 4:31-4:38

And that's it for this demonstration. We talked about mobile device management and mobile application management, and we gave you some examples of how these tools can be used to secure corporate data.

12.5.7 MDM and Synchronization Facts

Data synchronization has become a fundamental requirement. Data synchronization ensures that the data on all devices is up to date.

This lesson covers the following topics:

- Data synchronization
- Synchronization software
- Mutual authentication
- Data to synchronize

Data Synchronization

Data synchronization is the process that maintains data consistency between the source and target. Key points are:

- You can synchronize data between a cloud account, PC system, or even a car.
- Data synchronization can continually update devices.
- You can transfer data based on a scheduled time transfer or triggering event when documents change or a device comes online.
- Microsoft automatically syncs a mobile device with the corresponding Exchange mailbox using ActiveSync. You may already have access to a lot of synchronized information.

Cloud-based file synchronization allows apps on a mobile device to send data to the cloud. A few cloud-based file synchronization providers include Dropbox, Microsoft OneDrive, and Google Drive. You can also synchronize mobile devices by connecting to a laptop or desktop computer via USB, Wi-Fi, or Bluetooth. You can configure both a PC and a mobile device to use the same iCloud account.

Synchronization Software

You should be aware of software requirements needed to install the synchronization app on the PC or mobile device. Some software requires a specific operating system and cannot run on any other operating system. For example, Android apps run on only Android devices. Apple apps run on only devices with iOS.

Also be aware of hardware synchronization requirements. For desktop synchronization, Windows requires the PC to have 4 GB or more of RAM and at least one USB 2.0 port, with 300 MB of free space on the hard drive. Desktop synchronization software for macOS requires 10.5 or greater on a USB port. Some cloud-based applications have higher requirements.

Be aware of any defaults, limitations, or data caps for the environment. These will determine what is synchronized. Examples include:

- A maximum range of 30 days backwards for synchronizing.

- A maximum number of files per folder.
- A default to include documents smaller than 500 KB but drop any attachments larger than 500 KB.

Mutual Authentication

Mutual authentication (also called two-way authentication) is used for services like purchasing music and saving content to the cloud. Mutual authentication schemes ensure data security when transmitting data. Not to be confused with two-factor authentication, mutual authentication is a process where two entities authenticate each other at the same time with two types of credentials such as usernames/ passwords, and public key certificates.

- The client authenticates the server and vice-versa.
- Online services use mutual authentication or single sign-on to allow you to connect to servers to sync data.

For example, iTunes requires you to authenticate to its servers using an Apple ID. At the same time, Apple verifies that the iTunes app on your computer or device is the same app and computer used to access your iTunes account.

Data to Synchronize

These are the types of data you can synchronize:

- Contacts
- Programs
- Email
- Pictures
- Music
- Videos
- Calendar
- Bookmarks
- Documents
- Location data
- Social media data
- eBooks
- Passwords

12.5.8 Configure Email on Mobile Devices

Click one of the buttons to take you to that part of the video.

Configure Email on Mobile Devices 0:00-0:27

In this demonstration, we are going to practice setting up email on a mobile device. We are going to do this on an iPad. If you are using an Android device, or a Microsoft Surface tablet, then the steps are obviously going to be a little different.

For this iPad, I need to come down here to Settings. Under Settings, I need to tap on Accounts & Passwords. Notice over on the right, we have an option under Accounts & Passwords to add a new account.

Add an Email Account 0:28-1:15

I'll tap on that option. Now, I have to decide which type of email account I want to add. This depends on which service provider I'm using for my email. Notice, I can set up an iCloud, Exchange, Google, Yahoo, AOL, or Outlook account. If I'm using one of these service providers for my email, then I will tap the appropriate option here.

It is also possible that you are not using one of these email service providers and are instead using another email service provider that provides you POP3 or IMAP, plus SMTP access to their mail server. If that's the case, then you don't want to use the top six options in this screen. Instead, you want to tap on Other at the bottom.

Here you can add your email account. To do that, you would manually setup the IP addresses of your POP3 or IMAP servers, as well, as the IP address of your SMTP server.

Add a Well-known Service Account 1:16-2:34

We aren't going to do that in this demo. We have a Google account that we want to connect. So I am going to tap Google. Then, I enter in the email address that I want to connect to. Next, I have to enter the password that I set up for that account. Once I enter my password, I tap Next. Now I need to specify what I want synchronized between my Google account and the local mobile device.

Notice that my email messages, my contacts, my calendar items, and my notes can all set to be synchronized. If for some reason I didn't want one of these to synchronize, I would just tap the appropriate button over here. For example, on my notes, I can turn it off or on. Once I get it set the way I want, I tap Save. Now the account has been added.

So let's go ahead and try it. If I want to access my email from my Gmail account, I tap Mail, and wait a minute for it to pull down any messages. There are currently none in my inbox. However, now I can use this to read and send messages.

The key thing to remember is that if you are using an account on one of these very well-known email service providers, you need to use the appropriate option under Accounts & Passwords. But if you are using a different email provider that requires you to enter in IP addresses for the POP3, IMAP, or SMTP servers, then you need to use the Other option as we talked about.

Summary 2:35-2:37

That's it for this demonstration. In this demo we talked about how to configure email on a mobile device.

Copyright © 2022 TestOut Corporation All rights reserved.

12.5.9 Mobile Email Configuration Facts

This lesson covers the following topics:

- Mobile device email service providers
- Mobile device email configuration

Mobile Device Email Service Providers

You can configure email accounts on a mobile device using email service providers. Well-known email providers include:

- Exchange
- Google/Inbox
- iCloud
- Outlook.com
- Yahoo

Mobile Device Email Configuration

You can also add an email account and setup the IP addresses of the POP3, IMAP, or SMTP servers.

- To configure these email accounts, you may need to modify the port settings.
- To encrypt the email, configure the SSL and S/MIME settings. Both SSL and S/MIME securely sign and encrypt email to prove that the email actually came from the person claiming to be the sender.

12.6 Mobile Device Security

As you study this section, answer the following questions:

- What is biometric authentication?
- What is multifactor authentication?
- What is the set number of failed login attempts allowed on a mobile device?
- If you lose a mobile device, how can you find it?
- Which type of device encryption does not encrypt deleted files?

In this section, you will learn to:

- Secure mobile devices
- Configure iPad access control and authentication

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut PC Pro	<div>3.2 Implement mobile device security</div> <ul style="list-style-type: none">• Implement access control and authentication• Implement device encryption• Implement device location
CompTIA A+ 220-1101	<div>1.1 Given a scenario, install and configure laptop hardware and components.</div> <ul style="list-style-type: none">• Physical privacy and security components<ul style="list-style-type: none">◦ Biometrics◦ Near-field scanner features
CompTIA A+ 220-1102	<div>2.1 Summarize various security measures and their purposes.</div> <ul style="list-style-type: none">• Mobile device management (MDM) <div>2.7 Explain common methods for securing mobile and embedded devices.</div> <ul style="list-style-type: none">• Screen locks<ul style="list-style-type: none">◦ Facial recognition◦ PIN codes◦ Fingerprint◦ Pattern◦ Swipe• Remote wipes• Locator applications• OS updates• Device encryption• Remote backup applications• Failed login attempts restrictions• Antivirus/anti-malware

- | | |
|--|--|
| | <ul style="list-style-type: none">• Firewalls• Policies and procedures<ul style="list-style-type: none">◦ BYOD vs. corporate owned◦ Profile security requirements• Internet of Things (IoT) |
|--|--|

12.6.1 Mobile Device Security

Click one of the buttons to take you to that part of the video.

Mobile Device Security 0:00-0:29

Mobile devices are used for everything from making phone calls to managing bank accounts and everything in between. As such, they pose a unique security threat. A single smartphone sometimes contains more personal information than a desktop computer. And all that information is in a device that can be lost essentially anywhere.

In this lesson, we're going to take a look at the various aspects of a mobile device security and the different ways mobile devices can be protected.

Lock Screen Authentication 0:30-1:04

Let's start by looking at the different authentication methods that mobile devices use. By default, most mobile devices are configured to use a swipe lock screen. This means that anyone can unlock the device with a simple swipe of the screen. There's no authentication at all. For obvious reasons, this isn't very secure.

To secure access to a mobile device such as a tablet or a smartphone, it's important that you configure the device's lock screen to use some sort of authentication. And, there are actually several different types of lock screen authentication methods, each with varying degrees of security strength. Let's take a look at a few of them.

Biometric 1:05-1:52

Some mobile devices support biometric authentication on lock screens. The two most common ones are fingerprint and facial recognition. With fingerprint recognition, the index finger of the user is scanned and used to unlock the device.

With facial recognition, the device's camera is used to scan the user's face and unlock the device. It may seem pretty cool that mobile devices have this technology, and it really is. However, the technology is somewhat lacking and can be fooled relatively easily. For example, a simple photo of the device's owner can be used to trick facial recognition. By printing a picture of the owner's fingerprint using a simple laser printer, fingerprint recognition can be fooled. Because of this, biometric authentication probably shouldn't be used for mobile devices that contain highly sensitive information.

PIN 1:53-2:25

Probably the most common lock screen authentication method is using a PIN. It's very similar to the authentication method used by debit cards. The user needs to enter the correct four numbers in order to unlock the mobile device.

Using a PIN for authentication is actually relatively secure. There are 10,000 possible combinations using a four-digit PIN. A PIN can be memorized very easily, reducing the need to write it down somewhere. But a PIN does have some drawbacks. For example, a PIN can be shouldersurfed somewhat easily. A person doesn't even need to see the exact numbers being pressed, simply the location of the press.

Pattern Unlock 2:26-2:49

Another method of screen authentication is specific to the mobile devices that use the Android OS and is called pattern unlock. With this authentication method, the user creates a line pattern on a nine-point grid which looks something this. To unlock the device, the user has to provide the exact same pattern. Pattern unlock is actually harder to shoulder surf than PIN authentication. However, it's much easier to guess.

Passcode 2:50-3:16

The last method we'll look at is the passcode authentication, and it's potentially the most secure authentication method. Passcode authentication uses a user-defined password to unlock the device. The password can be a mix of letters, numbers, and symbols.

Now, I say it has the potential to be the most secure because, let's face it, some people don't put a lot of thought into their passwords. So, if the passcode is 1-2-3-4 or the word "password," the device won't be very secure.

Failed Login Attempts 3:17-4:05

We have these lock screen authentication methods, all of which prevent someone from accessing the mobile device. But, what if someone really wants to get the information contained on the device? What's to stop them from entering all 10,000 possible PIN combinations until the right one is found?

Luckily, most mobile devices are configured by default to allow only a set number of failed login attempts, which is usually 10. If more than 10 failed logins are attempted, the mobile device automatically wipes the entire contents of the device and resets it to the factory defaults.

It's important to make sure that this feature is enabled on all mobile devices. This is one of the best lines of defense you can provide to a mobile device. Even if the passcode or PIN aren't very secure, it will be pretty hard to guess the right one with only 10 attempts at your disposal.

Device Encryption 4:06-5:02

Another line of defense that can be implemented and is used by default on most new devices is encryption. Encryption prevents someone from accessing the stored information in any capacity. This means even if someone gets ahold of a device and were somehow able to copy the content of the device, they wouldn't be able to view any of the information. It would be encrypted.

There are two types of encryption methods used by mobile devices. The first is partial device encryption. With this method, only the sections of the device's storage that contain files are encrypted. This type of encryption is fast, but it doesn't encrypt deleted files, which can be recovered using software.

The second method is full device encryption. This method encrypts every sector of the device's storage, regardless of whether it is data or not. This protects the entirety of the device, including deleted files.

If a mobile device doesn't encrypt contents by default, it's important to make sure that full device encryption is enabled and configured.

Security Features for a Lost Device 5:03-5:10

There are two more security features used by mobile devices that you should be aware of, and they are both used in situations where the device has been lost.

Remote Wipe 5:11-5:36

The first is called remote wipe. Remote wipe is used to remotely format a mobile device. It's a feature that's built into a lot of mobile devices, especially smartphones. But, it's also possible to use third-party software, such as Windows Intune, to achieve this functionality. Remote wipe requires some sort of connection to the device. This means that in order to send a remote wipe command, the device needs to be powered on and have cellular or Wi-Fi connection.

Device Locator 5:37-6:44

The second feature is a device location service. A lot of smartphones, and even some tablets, have a device location feature to locate a lost or stolen device. This feature is usually a proprietary service specific to the device manufacturer. However, there are also third-party apps that offer location services.

If the service has been set up on a device, the owner can use a website or software application to identify the approximate location of the device on a map. The service can even do some pretty cool things, such as tell the device to take a picture with both the front and back cameras, then send the pictures to you. This can further help you identify the device's exact location.

The find my device feature does have some limitations. Because this feature uses GPS, the device needs to have a GPS signal. If the signal can't be found, the device can't be located. The device also needs to be powered on. This means that if the battery dies or if the person who stole it turns the device off, then it cannot be located. And if the SIM card is taken out or the device is wiped, either from remote wipe or from too many failed login attempts, then the device location services won't work.

Summary 6:45-7:01

So, those are some ways that you can secure a mobile device. To review, in this lesson, we looked at the different ways you can secure the information on a mobile device. We looked at the different lock screen authentication methods, the failed login attempt features, and the two types of device encryption. And we finished by looking at the remote wipe and device locator services.

12.6.2 Mobile Device Security Facts

This lesson covers mobile device security.


Mobile Device Security

Mobile devices are used for making phone calls, managing bank accounts, and everything in between. As such, they pose a unique security threat. A single smartphone sometimes contains more personal information than a desktop computer. All that information is on a device that can be easily lost or stolen.

The following table lists methods for securing a mobile device:

Security Method	Description
Screen locks	<p>To secure access to a mobile device, configure the device's lock screen to use some sort of authentication. Lock screen authentication methods include:</p> <ul style="list-style-type: none">• Swipe lock. Most mobile devices are configured to use a swipe lock screen. This means that anyone can unlock the device with a simple swipe of the screen (there's no authentication at all). For obvious reasons, this is not very secure.• Biometric locks. The two most common biometric locks are fingerprint and facial recognition. With fingerprint recognition, the user's finger is scanned and used to unlock the device. With facial recognition, the device's camera is used to scan the user's face and unlock the device.• PIN. A PIN allows a user to enter the correct four or six numbers to unlock the mobile device.• Pattern unlock. Pattern unlock allows the user to create a line pattern on a nine-point grid to unlock a mobile device.• Passcode. Passcode authentication requires a user-defined password to unlock the device. The password can be a mix of letters, numbers, and symbols.
Near-field scanner features	<p>Data can be transferred from device-to-device using a very low power and short distance connection. The distance between devices is generally less than an inch. It is often used with credit card machines as tap and go.</p>
Biometric authentication	<p>Biometric authentication is a type of authentication that relies on the unique physical characteristics of individuals to verify identity. Some mobile devices support biometric authentication on lock screens.</p> <p>The two most common ones are fingerprint and facial recognition.</p>
Multifactor authentication	<p>Multifactor authentication is a type of authentication that requires multiple authentication credentials to verify the user's identity for a login or other transaction.</p> <p>For example, you might require a user to enter a username, password, pin, and fingerprint before authenticating to a computer system.</p>

Failed login attempts	<p>Most mobile devices are configured by default to allow only a set number of failed login attempts (usually ten). If more than ten failed logins are attempted, the mobile device will automatically wipe the entire contents of the device and reset it to the factory defaults.</p> <p>It's important to make sure that this feature is enabled on all mobile devices. This is one of the best lines of defense you can provide to a mobile device. Even if the passcode or PIN isn't very secure, it will be difficult for someone to guess the right one in only ten attempts.</p>
Device encryption	<p>Encryption is another line of defense you can implement. It is set by default on most new devices. Encryption makes the stored information unreadable without decryption. This means even if someone was able to copy the contents of the device, the encrypted data wouldn't be usable.</p> <p>There are two types of encryption methods used by mobile devices:</p> <ul style="list-style-type: none">• Partial device encryption. With this method, only the sections of the device's storage that contain files are encrypted. This type of encryption is fast, but it doesn't encrypt deleted files, which can be recovered using special software.• Full device encryption. This method encrypts every sector of the device's storage, whether it has data or not. This protects the entire device, including deleted files. If a mobile device doesn't encrypt contents by default, it's important to make sure that full device encryption is enabled and configured.
Remote wipe	<p>Remote wipe remotely formats a mobile device. It's a feature that's built into a lot of mobile devices, especially smart phones. Third-party software (such as Windows Intune and other mobile device management (MDM) software) is also available.</p> <p>Remote wipe requires a connection to the device. This means that in order to send a remote wipe command, the device needs to be powered on and have a cellular or Wi-Fi connection.</p>
Device locator	<p>Many smart phones and tablets have a device location feature to locate a lost or stolen device. This feature is usually a proprietary service specific to the device manufacturer; however, there are also third-party apps that offer location services.</p> <p>If the service has been set up on a device, the owner can use a website or software application to identify the approximate location of the device on a map. The service can also tell the device to take a picture with both the front and back cameras, then send the pictures to you. This can further help identify the device's exact location.</p>
Remote backup applications	<p>Remote backup applications allow you to recover important business data and personal files (e.g., pictures and texts) from a lost, stolen, or broken phone. Most cellular providers offer some type of cloud backup service. In addition, each mobile OS offers its own proprietary backup service:</p> <ul style="list-style-type: none">• iOS devices have two backup tools:<ul style="list-style-type: none">◦ The desktop application iTunes can backup and restore iOS devices. iTunes requires mobile devices to be connected to the desktop computer via a USB cable.◦ The iCloud service can backup and synchronize files and settings across all Apple devices (i.e., mobile and desktop devices).<ul style="list-style-type: none">■ iCloud is a cloud-based backup service and requires an Apple ID, which must be logged into and configured on each Apple device.■ The iCloud service synchronizes and backs up files on Apple devices over the internet.

	<ul style="list-style-type: none"> Android devices use the Google sync service to sync and backup mail, contacts, calendar, and files across all android devices. Google sync is a cloud-based service and requires a Google account. Windows Mobile devices have two backup tools: <ul style="list-style-type: none"> OneDrive is Microsoft's cloud-based backup service and requires a Microsoft account. Windows Mobile devices can also be backed up using a desktop computer with the Windows OS installed. <div>  <p>There are several third-party backup solutions that provide similar and enhanced features</p> </div>
Authenticator applications	<p>An authenticator application is a specialized app called an authenticator. You pre-set the app to work with the service and provide a constantly rotating set of codes for two-factor authentication. The codes in authenticator apps sync across accounts and provide an extra layer of security.</p> <p>For example, implementing two-factor authentication on a Gmail account requires a username, password and one of the generated codes from the authenticator app to log in to the Gmail account. It may take a little longer to log in, but it provides an added layer of security.</p>
OS updates and patches	<p>Operating system updates often fix security vulnerabilities. Because hackers are constantly trying to find new ways to exploit technologies, keeping a device's operating system up to date is very important.</p> <p>The way a device receives an update depends on the type of mobile device, the manufacturer, and (if it's a smart phone) the cellular carrier.</p>
Trusted vs. untrusted apps	<p>Applications for mobile devices can be placed into two categories: trusted and untrusted.</p> <ul style="list-style-type: none"> Trusted apps are those that have been reviewed and approved by the device's app service. <ul style="list-style-type: none"> When approved, the app is signed with a certificate that identifies it as a trusted app. For the most part, this means the app is safe to install and does not contain malicious code. Untrusted apps are those that have not been verified and approved by the app service. <ul style="list-style-type: none"> While it's possible that an untrusted app is safe, it's very risky to install one. By default, most devices won't install untrusted apps. <p>Software for mobile devices should be restricted to trusted app stores such as Google Play, the Microsoft Store, or Apple App Store.</p>
Antivirus and anti-malware	<p>It is a good idea to install an anti-malware app on mobile devices, especially devices that are used by an organization or connect to a company network. This will protect the device from malicious email attachments, downloads, or applications. It will also help prevent the spread of viruses onto a network.</p>
Firewalls	<p>A firewall inspects network traffic and allows or blocks traffic based on a set of rules. It can be a powerful tool to help protect a device.</p>

Unauthorized Access	<p>Because smart phones connect to so many networks, it is possible for an unauthorized person to access data, location, camera, microphone, and mobile device account information. Implementing basic security practices (e.g., locking the phone with a strong password) can help protect against unauthorized access. There are several things you can do to mitigate this risk:</p> <ul style="list-style-type: none">• Data. Mobile phones are computers that contain financial, personal, or sensitive information. Be aware that:<ul style="list-style-type: none">◦ A phone's portability makes it vulnerable to being easily lost or stolen. Be sure to use a lock screen with strong authentication.◦ Hackers can access data on a phone using the same methods they use for desktop and laptop computers. Anti-malware and training in detecting social engineering can help protect against hackers.◦ Many social media applications allow third-party app developers to collect and sell information about users. Review privacy practices of social media applications and restrict collection and sale of information.• Account. Share mobile device account information only with authorized vendors and people who share the mobile device plan.<ul style="list-style-type: none">◦ Carefully select who to share a mobile phone plan with.◦ If you suspect a plan provider's employee has accessed an account without authorization, contact the provider and explain the concerns as soon as possible.• Location. A cell phone's GPS tracking feature makes a user vulnerable to unauthorized location tracking.<ul style="list-style-type: none">◦ To mitigate this risk, turn the GPS location feature off when you aren't using GPS navigation.◦ Also carefully select the apps that you allow to track location. Many apps that request location tracking don't need it to perform the function they provide.• Camera and microphone. Be aware that:<ul style="list-style-type: none">◦ Many apps that request access to a camera and microphone don't need those features to function. Grant access only when necessary for the app's function.◦ If a phone's camera and microphone are hacked, all visual and auditory data the phone collects is accessible to the hacker.
Prevent unintended connections	<p>Some mobile devices are configured to automatically connect to open Wi-Fi networks or accept other types of wireless connections (e.g., Bluetooth). This presents a serious security threat. For example, if a mobile device were to connect to an AP owned by a malicious individual, any information sent by the device can be captured and used.</p> <ul style="list-style-type: none">• To prevent against unintended Wi-Fi connections:<ul style="list-style-type: none">◦ Configure Wi-Fi settings to always ask for permission to connect to unknown wireless networks.◦ If Wi-Fi is not being used, consider turning off the Wi-Fi adapter.◦ If a mobile device has already connected to an unknown wireless network, remove the network from the saved networks list in order to prevent future connections.• To prevent against unintended Bluetooth pairing:<ul style="list-style-type: none">◦ Turn off Bluetooth unless it is actively being used. This not only prevents Bluetooth pairing and discovery, it also increases the device's battery life.◦ Delete (unpair) a device that has been accidentally paired to a mobile device. Navigate to Bluetooth settings to see what devices are paired and unpair unwanted devices.

Policies and procedures	<p>Policies and procedures to secure your mobile devices.</p> <ul style="list-style-type: none">• BYOD vs. corporate owned. Some organizations implement security policies that forbid users from connecting personal mobile devices to the organizational network (wired or wireless). Some organizations allow mobile devices; they may even provide users with mobile devices.<ul style="list-style-type: none">◦ There is a risk that company data on a device could be compromised if a device is lost, stolen, or hacked.◦ As a safeguard, many organizations require remote wipe to be enabled on the device so that if it is lost, stolen, or hacked, a command can be sent remotely to the device to remove all data on it.• Profile security requirements. Utilize an Acceptable Use Policy to specify how users:<ul style="list-style-type: none">◦ Connect personally owned mobile devices to the organization's wireless network. The policy may also specify rules for internet sites that can be accessed using those devices.◦ Use company-owned computers for personal use, such as shopping for personal items on ecommerce websites.
Internet of Things (IoT)	<p>The Internet of Things defines a body of devices that utilize the internet or other communication networks to exchange data with other devices and systems. It is an integration of technology and communications to provide monitoring, connectivity, and configuration. Examples include wearable technology and home automation.</p>
Device management	<p>In addition to policies, mobile devices can be secured by using special mobile device management tools that allow for remote management of multiple mobile devices. Using an MDM tool, an IT administrator can:</p> <ul style="list-style-type: none">• Test configuration settings before deploying them.• Create and enforce mobile device security policies.• Remotely wipe mobile devices.• Push OS updates to devices. <p>The specific MDM you use depends on the mobile device's operating system.</p> <ul style="list-style-type: none">• iOS devices use the Apple Configurator tool.• Windows Mobile devices use the Microsoft Intune tool, a cloud-based mobile management app.• Android devices can be managed using a variety of free, subscription or fee-based third-party MDM tools, including the Microsoft Intune tool.

12.6.3 Secure Mobile Devices

Click one of the buttons to take you to that part of the video.

Secure Mobile Devices 0:00-0:14

In this demonstration, we're going to discuss mobile device security. Specifically, we're going to look at a few things you can do to increase the overall security of an iPad running the iOS operating system.

Passcode Locks 0:15-1:09

Let's begin with passcode locks. I'm going to go to Settings, then to Touch ID & Passcodes.

Now, I need to enter my current passcode.

You can use passcodes on your iPad to protect the information stored on the device. If you set a passcode, then every time you either power on the device or wake it up, you will be prompted to enter the passcode before you can run any apps or access any of the information on the device.

That's a really good idea in case you forget this device in a taxicab, hotel, train station, or airport. You don't want just anyone to pick up the device and have full access to whatever's on it.

So, let's look at how you do this. Notice that, right now, passcodes are currently turned on. Let's go ahead and tap Turn Passcode Off, and then we're prompted to confirm that. I'll tap Cancel.

Right below that, I can change the passcode. And when I tap it, the iPad wants to know what my current passcode is before it allows me to change to a new one.

So, that is how you work with passcodes.

Auto Lock 1:10-1:53

In addition, we can also specify how long this device can be idle before we're going to require the passcode to be re-entered. So, first, we need to go to Display & Brightness. And then to Auto-Lock right here. Notice that currently, Auto-Lock is set to Never. That means that this iPad can sit idle forever and the user will not be required to re-enter the passcode.

Let's change that. I'm going to tap on Never. And let's set the auto-lock for 15 minutes. Now, if this iPad sits idle for 15 minutes, meaning I'm not tapping anything, then the screen is automatically going to lock.

So, to this point, we've enabled a passcode, and we've set our screen to automatically lock after 15 minutes. So far, we've increased the security a little bit on this device.

Erase Data 1:54-3:00

But there are more things we can do. I'll tap Touch ID & Password again. I'll enter in my passcode.

Now scroll to the bottom of this screen. There's an option called Erase Data. If I turn Erase Data on, then all the data on this iPad will be erased if the user tries to enter an incorrect password 10 times in a row. After 10 consecutive failed passcode attempts, all the data on this iPad is going to get erased.

Let's turn that option on. And it warns us, "Hey, if you turn this option on, then everything on this iPad is going to be erased after 10 failed passcode attempts." We're going to go ahead and say, "Nope." I'm borrowing this iPad, so the owner might not like that.

This is a powerful option, and you need to carefully decide whether you want it on. If you have it turned on and someone enters the wrong passcode 10 times in a row, you'll have to restore all the data on this iPad from backup, either from iTunes on a PC using a USB cable or pulling it down from iCloud.

Basically, what we're assuming is that if somebody enters the wrong passcode 10 times in a row, it isn't their iPad. So, at this point, we've really increased the overall security of this device.

Locate a Lost Device 3:01-5:09

Another aspect of mobile device security involves being able to track down a lost device because, well, mobile devices do get lost. They get lost all the time. People leave them on airplanes. They get left in hotels, taxicabs, elevators, and train stations. If this happens, you not only want to protect the data on the device, you also probably want to figure out where that device is.

Many mobile devices provide functionality that you can use to locate the lost device. The iOS operating system running on this iPad provides a function called Find My iPad, and it's tied to the iCloud backup function. If we enable this function and then we lose this iPad, we can sign into iCloud from any web browser on a PC or a laptop system and then use the Find My iPad option to view the device's approximate location on a map.

I tapped iCloud a second ago. Now scroll down a little bit. Notice down here that the Find My iPad option is already turned on. This gives us a lot of options.

For example, you could have a message displayed on the iPad that tells whoever finds it how to get in touch with you. You could even use iCloud.com to go in and remotely change the passcode lock assigned to this device. And if you're really concerned about not losing the data on a lost device, then you can use iCloud.com to perform a remote wipe.

Essentially, what we're doing with a remote wipe is assuming that the iPad is lost, that the person who found it has no intention of returning it, and that they may want to get at the information that's stored on it. In this case, you can use iCloud.com to send a remote wipe command to the iPad, which will then restore the iPad to its original factory settings. Any personal information on it, as well as any proprietary sensitive information belonging to your organization, gets wiped out.

If you have this option turned on, it's not a bad idea to come over here, under Backup, and turn on iCloud Backup as well. The idea here is that if you ever do end up performing a remote wipe, or if you end up losing the iPad altogether and never get it back, then you can restore all the data from your old iPad onto a new iPad. Go ahead and tap Cancel for now.

Summary 5:10-5:34

That's it for this demonstration. In this demo, we talked about some things you can do to increase the overall security of a mobile device, in this case, an iPad. We began this demonstration by talking about how to set passcode locks. We talked about how to set the auto-lock feature of the iPad. We talked about wiping the data off the iPad if somebody enters the wrong passcode more than 10 times in a row. Then we ended this demonstration by talking about how to locate a lost device using the Find My iPad option and iCloud.

12.7 Laptop and Mobile Device Troubleshooting

As you study this section, answer the following questions:

- Which tools can you use to troubleshoot mobile devices?
- What are the common causes of touchscreen issues?
- What should you do if a mobile device's battery is swollen?
- What can cause a mobile device to perform poorly?
- What is the difference between a cell tower analyzer and a wireless network (Wi-Fi) analyzer?

In this section, you will learn to:

- Maintain mobile devices

The key terms for this section include:

Term	Definition
App scanner	A troubleshooting tool that identifies issues in installed apps.
Wi-Fi analyzer	A troubleshooting tool for Wi-Fi connectivity issues that: identifies the number of broadcasting access points (APs); displays the signal strength and channel of each wireless network; and obtains wireless network information such as the network type, data activity, and service provider.
Cell tower analyzer	A troubleshooting tool for cellular network connectivity issues that: reports signal strength; interference; number of cell towers in the area; the location of each cell tower; and mobile network information such as the network type, data activity, and service provider.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA 220-1101	<p>5.5 Given a scenario, troubleshoot common issues with mobile devices</p> <ul style="list-style-type: none">• Common symptoms<ul style="list-style-type: none">◦ Poor battery health◦ Swollen battery◦ Broken screen◦ Improper charging◦ Poor/no connectivity◦ Liquid damage◦ Overheating◦ Digitizer issues◦ Physically damaged ports◦ Malware◦ Cursor drift/touch calibration

12.7.1 Common Laptop Issues

Click one of the buttons to take you to that part of the video.

Common Notebook Issues 0:00-0:32

In this lesson, we're going to review several common notebook computer issues that you could be required to troubleshoot as a PC technician. There are many issues that are specific to notebook systems, so obviously, there's more than we could ever go over at once. But knowing some general things to look for is a good start. We'll talk about batteries and power sources, broken screens, malware, and touchpad issues today. Now, you might call a notebook a laptop. The terms are mostly interchangeable, so we'll use both in this demo. Let's get started.

Power Issues 0:33-1:57

Considering that notebooks use batteries for power and adapters for charging, notebook power issues are quite different from those facing desktop systems. Most new notebooks use a Lithium-Ion battery, which have a few known issues, such as overheating and swelling. Some of these batteries have even caught fire in the past. While these issues have mostly been fixed, it's still important to be vigilant. If your battery appears swollen or feels hot, shut off the machine and unplug it immediately.

Additionally, as batteries age, they become less reliable and may not fully charge. Another issue might be the AC adapter itself. Over time, they do get damaged and wear out. The internal wiring or internal electronic parts may wear and brake, causing the adapter to fail.

Another issue relating to the AC adapter is the adapter's plug and the notebook's power port. While not common, it's possible to damage the power plug. Furthermore, the solder joint can fracture or break on the power port's motherboard connection. This generally isn't something you can repair. It might be best to purchase a new motherboard or have it fixed by a trained technician.

Should you decide to replace the AC adapter, it's almost always best to replace it with one from the same manufacturer. But there are several third-party manufacturers that make replacement adapters. If you go this route, make sure that you get one that's compatible with your specific notebook model. If you decide to attempt a motherboard repair, train yourself in small component and heat-sensitive soldering first. But again, most repairs should only be attempted by training technicians.

Display Issues 1:58-4:38

Next, let's talk about display issues that are common with notebook systems. The first issue is where no output is visible on the display. There are several possible causes for this. The system might be configured to use an external monitor on a video port, usually VGA or HDMI. Check the settings found in the system configuration or in the display settings.

A blank display could also be caused by a disconnected video ribbon cable. If this is the case, you need to disassemble the notebook and reconnect the cable. Be sure to verify that both ends are properly secured. Finally, a blank output could be caused by a failed display panel. Display panels tend to fail over time, especially LCD display panels. If this happens, disassemble the system, remove the display panel from the bezel, and replace it with a new one.

You could also experience dimness or flickering. This is a common occurrence with LCD screens, and there are several things to look at. First, check the brightness setting. The brightness setting is usually controlled by pressing a function key combination. It's not uncommon for a user to accidentally hit the

wrong keystroke combination and dim their display. Check the system documentation to discover the key combination that affects brightness.

If your system uses an LCD display, it's also possible that the inverter has failed. The inverter is a small electronic component used to power the LCD backlight. If the inverter fails or is failing, the backlight may flicker or go off—similar to a fluorescent bulb. If either of these conditions occur, you'll need to replace the parts.

Most notebooks have a port on the side or rear of the case for connection to an external monitor. More often than not, the issues aren't hardware related, but it's not impossible—external ports can break. First, make sure that you have the correct cable. The cable must match the connection to your notebook and the monitor. There are a few different connection types. HDMI, DisplayPort, and DVI are all digital cable types that should work on either side of a connection. In other words, if the notebook has an HDMI connection and the monitor has a DVI or DisplayPort connection, the external monitor shouldn't have an issue as long as you have the right port.

VGA, on the other hand, is analog and won't work with a digital signal. So, if you only have a VGA connection on the notebook, you'll have to use a monitor with an analog VGA connector. You'll also have to ensure that the notebook's output and the monitor's input are set to the correct port. This is especially important with monitors since they often have two or more connection ports.

Beyond finding the right cable, check some of the more obvious solutions. For example, is the external monitor powered on? Is the notebook display configured correctly? Are the cable connections secure? Okay, let's move on.

Connectivity Issues 4:39-5:42

In the past, notebooks didn't have any way to connect in to an external network. In the early 90s, laptops started coming equipped with PCMCIA cards, which finally gave them this ability. In the late 90s, laptops started coming equipped with Ethernet ports. Then, in the mid-2000s, Wi-Fi began to find its way into the mainstream. When first introduced, the communication speed was about 1 or 2 megabytes per second. Today, many laptops come with the latest technology, where speeds are close to 1 gigabyte or more per second. That's really fast considering where we started out.

Remember that there are several factors that affect how well your notebook communicates wirelessly. The signal can degrade depending on how far away you are. When a signal has to go through solid objects, it can weaken as well. Too many devices and channel crowding also affect performance. All of these are reasons to be observant when you place your antennae.

Simply moving an antenna closer can go a long way. Dense and immovable objects—trees, for example—are much more difficult to mitigate. These issues not only affect Wi-Fi, but many of the same issues affect other wireless technologies, such as Bluetooth.

Additional Issues 5:43-7:29

We've reviewed some of the major issues that affect how a notebook computer performs. While not an exhaustive list, there are a few other issues to go over quickly.

Considering a notebook's portable nature, simple wear and tear can affect the machine. A notebook is easily damaged by liquids. If something spills on the keyboard or desk, the liquid could seep into the electrical components and cause a short. Heat is another factor at play. It's import to keep in mind how small a notebook computer is and how important the airflow is. If the input or exhaust fan opening gets blocked, the machine could overheat very quickly. And the constant plugging in and removing of components—things like USB devices, external monitors, and Ethernet cables—can damage external ports. Don't ever yank or tug the cords, even if you're in a hurry.

Besides physical issues, there are additional software and internal hardware issues. If the touchpad isn't working correctly, there are a few things to consider. Some laptops come with a physical switch that turns the touchpad off. It may be as simple as turning it back. Cursor drift and ghosting could be caused by corrupted drivers or other connectivity issues. It's possible to have a conflict between the touchpad and another pointing device, such as an external mouse. Simply removing the mouse or updating drivers will probably fix this. Lastly, a touchpad can lose its calibration. Consult the system documentation to learn how to recalibrate your touchpad.

Lastly, we have malware. Malware is the generic term for software that's meant to harm a system. You've probably seen it in the form of viruses, adware, and ransomware. Your system should have good malware and real-time scanners. Hopefully, the scanners will catch an infection before it's allowed to take hold. Proper scanner software and virus definition file updates will help keep your system current. Furthermore, avoiding sketchy websites altogether greatly reduces the chance of infection.

Summary 7:30-7:48

That's it for this demo on notebook system troubleshooting. These issues can be a daunting task. But with a bit of knowledge, you can fix a lot of things with simple techniques and the process of elimination. Often, a simple update or replacement parts is all that's needed. When in doubt, and especially if the machine needs to be taken apart, it's probably best to leave it to a trained technician. Just remember that a little care goes a long way.

Copyright © 2022 TestOut Corporation All rights reserved.

12.7.2 Laptop Maintenance Facts

Mobile device integration into the workspace requires that you have the knowledge and skills to perform maintenance on them and provide users with preventative maintenance tips. This lesson provides important concepts for working with mobile devices.

This lesson covers the following topics:

- Mobile device assembly
- External components care
- Cooling
- Transporting mobile devices

Mobile Device Assembly

When assembling and disassembling mobile devices keep in mind:

- Most laptop manufacturers provide service manuals on their websites. You can use the service manuals to learn disassembly/reassembly procedures for the laptop makes and models you work with.
- The components used in laptop systems are much smaller than those used in desktop system. You should carefully organize and label each part as you remove it from the system to ensure that it doesn't get lost and that it gets reinstalled in the correct location.
- Liquid spills are especially damaging to a portable device. Liquid can easily run beneath the keyboard and onto internal components. Keep food and drink away from devices.

External Components Care

It's important to take care of the external parts of devices. Keep the following tips in mind.

- If individual keys on a keyboard stick, you might be able to remove the sticking keys and clean underneath them. If that does not work, you need to replace the keyboard.
- You should clean the display with a lint-free cloth and isopropyl alcohol. Spray the alcohol on the cloth, not directly on the screen, to avoid getting it on other components.

Cooling

Cooling is a major concern for portable devices. Follow these recommendations:

- Keep all air vents clear and unobstructed. Vents are typically located on the back of the unit.
- Do not place a laptop on a surface where air can't circulate beneath it evenly. This will with help heat dissipation.

- Consider purchasing special laptop cooling bases that provide fans for the bottom of the unit. A cooling base is the best way to keep a laptop properly ventilated.
- Set laptops on top of a hard, solid surface, such as a desk or countertop. Do this when a laptop cooling base is not available.
- Avoid soft surfaces, such as a couch or your lap. These surfaces can obstruct even air flow.
- Adjust processor throttling (if supported) and configure Power Options to reduce power consumption. Lower power consumption not only saves battery life, it lowers heat output.

Transporting Mobile Devices

Transporting a mobile device without careful attention can cause damage to or loss of the device. To avoid unnecessary repair or replacement, follow these guidelines:

- When moving from outside to inside, allow the computer to warm up before using it. This will help prevent water vapor condensation when it warms up quickly.
- You should avoid leaving portable devices in cars where the temperature can reach extremes or where direct sunlight is magnified.
- Although they are built to withstand being moved, protect portable devices in properly padded cases; use proper packaging materials when shipping them.
- When installed, both PCMCIA and ExpressCard cards extend past the outer edge of the laptop. Remove the cards from the slots before putting them in a case to protect them from damage.

12.7.3 Battery Recalibration Facts

Battery power meters in laptops commonly report the incorrect amount of charge remaining in the battery. Typically, the power meter reports less available power than the battery has. This becomes a problem because Windows Power Schemes use the power meter to automatically turn off the laptop when the battery level reaches a certain level (such as 5% remaining). The system may shut down even when there is sufficient battery power remaining.

This lesson covers the following topics:

- Calibrate the battery
- Calibration tips

Calibrate the Battery

Calibration synchronizes the power meter to the charge capacity of the battery. Many laptops come with a software tool for calibrating the battery; some include a function in the BIOS. If the laptop does not include a calibration tool, you can calibrate the battery by following these steps:

1. Charge the battery to 100%. Because you might not be able to trust the power meter shown in Windows, allow sufficient charging time.
2. In Windows, change the Power Scheme settings so the system is not shut down automatically when the battery level reaches a low level.
3. Unplug the laptop and run it only on battery power.
4. When the battery level drops below 3%, turn the laptop off.
5. Connect the laptop to a power source and fully charge the battery.
6. Restart the computer and restore the previous Power Scheme settings.

Calibration Tips

Be aware of the following when working with laptop batteries.

- Some manufacturers recommend calibrating the battery when you first use it and every 3 months thereafter.
- Extreme high or low temperatures shorten the battery life.
- To provide more working time when running on battery power, turn down the display brightness, avoid watching DVDs, avoid playing CDs, turn off wireless networking when not in use, use Power Scheme settings to power off unused devices, and adjust processor power settings (if available).
- If the battery will go unused for longer than 2 weeks (for example, if you are not using the laptop or are running it only on AC power) remove the battery and store it separately.
- Storing a battery longer than 3 months without use might affect its ability to hold a charge.
- Depending on how you use them, most batteries will last between 1-3 years. Under normal conditions, the battery will gradually lose capacity over time. If the battery life is still low after

calibration, the only solution is to replace the battery.

12.7.4 Laptop Troubleshooting Facts

Due to the integrated nature of laptops, troubleshooting laptop components is significantly harder than troubleshooting desktop components. Most laptop manufacturers provide service manuals on their websites. You can use these service manuals to learn specific troubleshooting procedures for a particular make and model.

This lesson covers troubleshooting guidelines.

Troubleshooting Guidelines

The following table provides troubleshooting guidelines to follow when working with laptop computers.

Component	Troubleshooting Tips
Power	<p>Laptops can run on AC power from the power adapter or battery power. When troubleshooting power, verify that:</p> <ul style="list-style-type: none">• The cord from the AC outlet to the power adapter is correctly connected to both the wall and the adapter. Move it around to see if you can make a secure connection.• The LED light on the power adapter is lit. If it isn't lit, the point of failure is between the outlet and the adapter.• The battery is sufficiently charged. If the battery reads fully charged in Windows, disconnect the laptop from its power source. If the battery lasts only a short amount of time, replace the battery.• If the computer runs for only a short time even while plugged in, it could be that the power adapter is bad. If the adapter is not working, the computer will run off of the battery until the battery is drained. Try using a different adapter or verify the power coming from the adapter.• If the battery seems to be losing the ability to hold a charge, or if the power drops shortly after starting to use the laptop, try recalibrating the battery.• If the device starts to show signs of distortion, bulging, or wobbling, the battery may be swollen. Possible causes are the battery is too old, or was exposed to too much heat and humidity. You must replace a swollen battery.
Video	<p>If the laptop has no display at all:</p> <ul style="list-style-type: none">• You can press Function (Fn) and the appropriate display key to switch the display output to the laptop monitor.• If the built-in monitor isn't working, connect an external monitor to the laptop. Use the Fn keys to direct output to the external monitor.• If you don't get a display on either monitor, you likely have a problem with the video card. Repairing the video card typically means replacing the motherboard.• If the display renders on the external monitor but doesn't render on the laptop, there is likely a problem with the LCD display. If this is the case, you should verify:<ul style="list-style-type: none">◦ The LCD cutoff switch is working. Sometimes the switch can get stuck in the off position, preventing the output from going to the LCD.◦ There aren't cracks in the bezel around the LCD. Bezel cracks can be an indicator that the LCD has been damaged.

	<ul style="list-style-type: none"> ◦ The power bundles that go from the laptop to the LCD are not damaged or cracked. Remove the bezel around the LCD to inspect the power bundles. <p>Additional problems with laptop displays include:</p> <ul style="list-style-type: none"> • Dead Spots—areas on the screen (sometimes entire rows or columns of pixels) that no longer work. This means that the LCD assembly is no longer functioning and you need to replace it. Be aware that it is often cheaper to purchase a new laptop computer than to replace the display. • Bad backlight—may cause a display to become dim. It is important to note that dimming the backlight is a power saving method used by laptop computers. Always verify that the screen isn't dimmed before replacing the backlight. • Flickering Screen—can be caused by a faulty backlight or inverter. Replacement parts can be purchased from the laptop's manufacturer. <p>If you know that the LCD needs to be replaced but you don't have the resources to buy a new LCD or a new laptop, consider converting the laptop into a desktop system by connecting it to an external monitor permanently. If the video card is bad, try using a remote solution (such as Remote Desktop) to connect to the laptop from an external system.</p>
Applications	<p>If you cannot load an app from the Microsoft Store, use the Windows Store Apps Troubleshooter to search for and correct problems. Third-party apps have varying levels of support. You may have to contact the developer to troubleshoot issues.</p> <p>If you are unable to decrypt an email, you probably don't have the correct private key. You must import it from another computer.</p> <p>If the GPS is not functioning:</p> <ul style="list-style-type: none"> • Begin troubleshooting by running the Hardware and Device Troubleshooter program. • Update Bluetooth drivers if you have trouble pairing a GPS-dependent Bluetooth device. • Install the drivers in Compatibility mode for the correct Windows version if the pairing device uses Window 7 or older. • Use known good devices to check for damaged hardware and replace components as necessary.
Laptop Components	<p>The most common portable components used with laptop systems are keyboards, mice, digitizer pads, and antennae. The following list suggests troubleshooting methods to use when working with these components:</p> <ul style="list-style-type: none"> • You can test a bad keyboard by plugging an external keyboard to the laptop. If it works, the laptop keyboard is malfunctioning and needs to be replaced. • Most laptop systems have features that cause keyboard keys to perform alternate functions (such as NUM LOCK emulating 10-key functionality). Before troubleshooting other problems, make sure that special features that can cause keys to perform alternate tasks are not enabled. • Some power saving modes don't support indicator light function. Also, the NUM LOCK indicator lights may not correspond to the NUM LOCK's function state. <ul style="list-style-type: none"> ◦ You can press the F LOCK key with the NUM LOCK key to see if it responds. ◦ If it doesn't respond, the computer probably isn't properly maintaining the NUM LOCK state and may have damaged components. • Mouse malfunction on a laptop is usually caused by the installation of an incorrect driver. Good indicators that the incorrect driver has been installed are:

- The laptop mouse's sensitivity isn't consistent.
 - The mouse doesn't recognize a double tap.
- A digitizer pad in laptop and PDA systems receives input. Input is written onto the pad with a stylus pen. Those motions are translated into data that is processed by the system. If the pad becomes scratched, the laptop or PDA cannot receive input correctly.
 - This is most easily resolved by buying a cleaning product named Screen Clean. It removes the top layer of plastic from the digitizer pad, thus removing existing scratches and giving the pad a fresh surface.
 - You will need to replace the digitizer pad or buy a new system if the scratch is too deep.
- Digitizer pads can have an issue called pointer drift (also known as ghost cursor).
 - Drift occurs when a pad's pressure sensors need to be realigned.
 - Recalibrating the digitizer pad can fix this issue.
 - It is best to recalibrate before it progresses to the point that you can't access the recalibration utility.
- Though laptop antennae are supposed to be omni-directional, they sometimes need to be re-oriented to get the best reception.
 - This can usually be done by moving the laptop until the reception improves.
 - If redirecting the antennae doesn't work and wireless reception is consistently poor, the antennae may need to be replaced.
- Many laptops include a switch that turns the wireless network card on and off. When troubleshooting wireless network connectivity, make sure the switch is turned on.
- If the speakers are not producing sound, try the following in this order:
 - Verify the volume is turned all the way up and the speakers or headphones are connected correctly.
 - Make sure the sound card works properly and is running with updated drivers.
 - Run the Windows Audio Troubleshooter program.
 - Consider that the hardware components are damaged and need to be replaced.
- If the external components are not connecting to the device and you've checked that they are working on a known good device, the laptop may have malfunctioning ports.
 - If it's a software issue, reinstalling the driver should fix the problem.
 - If the problem persists, it's likely hardware-related and one or more ports have been physically damaged. In this case the most probable solution is to replace the motherboard.

As long as the laptop runs, you can substitute an external device connected to a PS/2, USB, PCMCIA, or ExpressCard slot for most failed components. This will allow you to continue using the computer.

12.7.5 Mobile Device Troubleshooting

Click one of the buttons to take you to that part of the video.

Mobile Device Troubleshooting 0:00-0:38

In this lesson, we're going to take a look at the various problems that are specific to mobile devices and the steps you can take to troubleshoot these common issues. Before we begin, it's important to note that there are a lot of differences between mobile devices. This is especially true with Androids. The exact same Android OS version can look entirely different depending on the smartphone manufacturer. Even though there are differences, the troubleshooting techniques we'll talk about in this lesson can be used regardless of the mobile OS or phone manufacturer. When in doubt, refer to the device manufacturer's documentation on how to fix a particular issue.

Display Issues 0:39-1:36

Let's start with a mobile device's display. Because of their mobile nature, mobile devices are prone to being dropped. The damage caused from dropping a device can range from a minor scratch to a completely broken display and screen. If a mobile device is having display issues, the first thing you should find out is whether or not the display was dropped recently. Do this even if there's no physical damage. Sometimes, even a fall that results in no external damage can still cause internal damage. If the display does have cracks or physical damage, chances are that the entire screen has failed and needs to be replaced.

Before replacing the screen, make sure the device is on and fully charged. Another thing to check is the display brightness. Most mobile devices have an auto-brightness setting that changes the screen's luminance depending on the ambient light. It's possible that auto-brightness was accidentally disabled, and the screen is at the lowest brightness setting. To rule this out, look at the screen in an area with very little light.

Touchscreen Issues 1:37-2:49

Another issue related to the screen has to do with the touchscreen functionality. If the touchscreen isn't being responsive or the touch accuracy is off, there are a couple of things you can look at. First, remember that mobile devices use capacitive touchscreens. This means that a conductive material, such as a finger, needs to contact the screen for a tap to be recognized. As such, wearing gloves or using nonconductive utensils can cause the touchscreen to not function. Conductive touchscreens can also be affected by even the smallest amount of liquid. A tiny drop of water can cause the touchscreen to behave erratically or not work at all. Make sure the screen is clear of any moisture.

A cracked or damaged screen can also cause touchscreen problems. If this is the case, the screen should most likely be replaced. This is especially true if the screen is made of glass. Not only will the touchscreen not work, but it's very easy for the cracked edges to cut a finger. If there's no physical damage, but the screen seems to respond inaccurately, it's possible that it needs to be calibrated. To do this, enter the device's configuration settings and follow the calibration steps. These usually involve tapping specified areas on the screen multiple times.

Replace Display 2:50-3:11

If you tried cleaning the screen and calibrating the touchscreen, but it still doesn't work, there's a chance that the screen and digitizer need to be replaced. Earlier, we talked about a device being dropped. If a device was dropped, especially if you see cracks on the screen or case, there's a strong possibility that a qualified technician might need to replace the screen and digitizer.

Battery Issues 3:12-4:28

Another area of concern for mobile devices is the battery. Not only can the battery cause several problems, but it can also point to other non-battery related issues. For example, let's say that a mobile device's battery is being drained a lot faster than normal. One initial reaction is to replace the battery with a new one. But what if the problem wasn't the battery, but it was instead due to an installed app consuming too many resources? In this situation, a new battery wouldn't fix this issue. Because of this, it's important to be able to identify whether a battery is faulty or not.

A swollen battery is probably the easiest way to identify a bad battery. If the battery is bulging at all, it needs to be replaced immediately. If not, the battery could explode and even cause a fire. If there are no physical abnormalities, try to identify how old the battery is. Most smartphone batteries have only a lifespan of about a year. After that, the amount of charge they can hold is drastically reduced. If the battery is new and has no physical abnormalities, the battery drain could be a result of too many running apps. Many mobile devices have a battery usage history that can be used to identify which apps are consuming the most battery power. You can then uninstall or disable the culprit if necessary.

Overheating 4:29-4:53

One of the early signs of a battery going bad is overheating, but the battery isn't the only cause of this. Heat problems can come from running too many apps at the same time or from apps using too many resources. The physical environment can also cause overheating, such as using the GPS on a phone for navigation while you have it sitting on your car's dashboard in the sun, especially if you're charging the device at the same time.

Inability to Charge 4:54-6:12

Another indicator of a bad battery is when the device won't charge properly. But once again, charging problems can be caused by issues unrelated to the battery. Failure to charge could be a bad charger, so try using a different one. Charging from a USB port on a computer will work more slowly than using the charger that came with the device, as will using a charger that wasn't recommended by the manufacturer. The problem might be the cable that goes from the charger to the device, so trying a different cable can be helpful.

The second most expensive problem comes when the actual data and charging port is damaged. Modern Apple mobile devices use a Lightning port, and most Android devices these days use USB-C or micro-USB. In any case, it's very easy for someone to accidentally break the port by sitting on a phone while it's plugged in, or when a device falls off of something while plugged in, or by moving the device around while it's plugged in. The small, fragile components inside phones and tablets can't take much strain, so even the slightest movement can break that port, which will have to be repaired by a trained technician.

The most expensive problem is when the charging system on the device's motherboard is broken. At this point, the device usually needs to be replaced. Very rarely will you find it cheaper to try to actually fix or replace that board!

Liquid Damage 6:13-7:26

Batteries, as well as all other components in a mobile device, will be damaged when wet. In fact, manufacturers put moisture detectors inside devices to see if customers violate the warranty by allowing them to get wet. Liquid damage is a frequent problem with the smallest of our devices—our phones—because we use them in environments where they may be dropped into water or may get wet from splashing or rain.

If a device gets wet, you might be able to save it. First and foremost, DO NOT turn it off or on. Leave it in exactly the power state it was in when it got wet. Hold it upright with the charging port down so any water can drip out the bottom, and wipe the outside dry with a cloth. Prop it up where it'll get plenty of air circulation and allow it to air dry for at least 24 hours or more, depending on the humidity. If it's on, you may be tempted to answer calls or text messages, but don't! Leave it alone, even if the battery dies. Your best hope to save it is patience.

Some people like to put the device in a bag of desiccant or rice to absorb moisture. We can't recommend the use of rice, as it could get inside the ports, but using desiccant packs might be helpful if you live in a high-humidity environment where air-drying isn't very effective.

Performance Issues 7:27-8:24

Performance issues are another problem that can occur with mobile devices. If the device seems to be running slow, there are a couple of things you should look for. First, identify the system resources and usage. Check how much memory running applications are consuming and disable any unnecessary apps. One indication of high resource usage is the mobile device being warm or hot to the touch, which indicates the device is doing a lot of processing.

Second, check to see if the device is attempting to run applications that were intended for newer devices. Even though an app can be installed on an older device, it doesn't mean that device will be able to run it properly. Just like desktop computer applications, mobile device apps have recommended hardware specifications.

Third, check the device's storage usage. If the mobile device storage is more than 80% full, performance can be reduced considerably. If this is the case, uninstalling unnecessary and unused apps can help speed up performance.

Malware 8:25-9:29

Performance issues can also be caused by malware. In the early days of smartphones, malware wasn't a problem because the devices were new to the market and few people had them. Nowadays, smartphones have replaced traditional computing devices, like desktops and laptops, for many people. Malicious actors now write code targeting our new favorite computers—the ones we hold in our hands. Gone are the days of security through obscurity!

While malware on iOS devices like iPhones and iPads is less common than malware on Android devices, it still exists. It's very important that you get, install, and maintain anti-malware apps for all your mobile systems. Frequently, newer devices come with security software provided by either the manufacturer or by the mobile phone service provider. Still, you should always double check. Don't just assume that the phone company gave you the software if you bought the phone from them. There are also many free and paid options available for smartphone and tablet security software, so remember to protect your mobile devices the same way you protect your computers.

Connection Issues 9:30-10:54

Connection issues are another area where mobile devices can have problems. Not only do most mobile devices connect to a cellular carrier server, but they also use Wi-Fi, Bluetooth, and GPS technology for communication. When troubleshooting connection issues, make sure the device isn't in Airplane Mode. In this mode, cellular service is disabled, and other wireless connections are also typically disabled.

Make sure that the wireless technology in question is properly enabled. GPS, Wi-Fi, and Bluetooth can all be turned off on mobile devices to conserve battery power or to protect the device from unwanted connections. Ensure that the device has a solid connection. For cellular problems, check the connection level—1X, 3G, 4G, and so on. The number of bars indicates the signal strength.

For Wi-Fi, make sure that the device is connected to the access point. If the signal seems to be intermittent, try installing and using a Wi-Fi analyzer app to identify the signal strength and interfering signals. For GPS to function properly, the device needs a line-of-sight connection to satellites in orbit. If there are obstructions such as large buildings, the connection won't work properly. Most Bluetooth devices need to be paired with each other by entering Discovery Mode and using a special code. If pairing hasn't been configured, devices won't be able to communicate with each other.

Frozen Device 10:55-11:39

Occasionally, you'll run into a problem that requires the device to be restarted, such as a frozen app or the device itself being locked up. If this is the case, there are two ways to reboot a mobile device. The first and preferred method is to do a soft reset. With a soft reset, you hold the power button on the device. Depending on the device, the device will reset or a power options dialog will appear, giving you the option to shut down or restart.

The second method is a hard reset, which should be used only if a soft reset doesn't work. With a hard reset, the device's battery is typically removed and then reinserted. If the device's battery can't be removed, a hard reset is performed by holding a combination of buttons on the device until it powers off.

Summary 11:40-11:59

That's it for this lesson. These are just some of the issues you may encounter when working with mobile devices. Remember, mobile devices vary by both manufacturer and operating system. The configuration and troubleshooting steps for one device might be completely different for another. But by understanding the basics that we've talked about in this lesson, you should be able to troubleshoot any mobile device you encounter.

12.7.6 Maintain Mobile Devices

Click one of the buttons to take you to that part of the video.

Maintain Mobile Devices 0:00-0:22

In this demonstration, we're going to talk about some things you can do to maintain a mobile device. Specifically, we're going to look at how you can maintain an iPad device that's running iOS.

If you're working with a mobile device running a different operating system, maybe an Android device or a Windows tablet, the tasks will be different on those devices, but the general concepts will be the same.

Delete Apps 0:23-1:39

So let's begin by talking about removing unnecessary apps from the device. Understand that all the apps you install on the system consume space and they also drain battery power. To optimize the device, you really should remove apps that you don't need.

I understand that there are apps that are installed by default with the operating system. For the most part, you cannot get rid of them or they're extremely difficult to remove. We're not going to deal with those here. We're simply going to deal with the apps that you download and install from the appropriate app store.

Here's what happens. When you get a new mobile device and go to the app store, such as iTunes, Google Play, or the Windows Store, for the first time, you see all the apps that are available. It's like a kid in a candy store. It's like, "I'm going to download everything and install it!" But, you end up using only one out of ten of those apps that you put on your device.

So let's take a look at how you do that on an iPad. Let's go down here. You see I have the Weather Channel app. I find the weather forecast depressing and therefore, this app has to go.

If I want to uninstall it from this iPad, I tap and hold it on the device until it starts wiggling. When it starts wiggling, you see that there's an X up in the top left corner. To uninstall the app, I tap the X. Then I am prompted as to whether or not I want to remove the app. I say, "Please delete it." And the app is now uninstalled.

Install Updates 1:40-2:24

Let's now move on to the next topic, managing updates. It's very important to keep your operating system up to date on the mobile device. If there are security flaws found, as much as Apple, Google, and Microsoft would like you to believe that there are no security flaws in their mobile device operating systems, there are, and these updates should take care of them as they're found.

On this iOS system, we go to Settings. Then, here on the General tab, notice there's an option called Software Update. I'll tap it. It tells us that iOS 12.0.1 is available, and I should download and install it. To do that I would select the Download and Install link, down here on the bottom right.

Now I'm not actually going to do it for the sake of this demonstration because it would take a very long time to complete. Just understand that's where you would go.

Install Anti-Malware 2:25-3:26

The next thing we need to talk about is anti-malware. Back in the old days when mobile devices were first introduced, all the vendors, including Apple, Google, and Microsoft, kind of insisted that these devices didn't need anti-virus software at all because the apps that go on them are tightly controlled.

You know that you can get apps only from the app store for your particular operating system, such as iTunes, Google Play or the Windows Store, unless you jailbroke your device. But as long as you did not jailbreak your device, then you could get apps only from the app store.

The idea would be that app vendors such as Apple, Google, or Microsoft would take a look at apps as they were submitted by app developers and check them for malware before they put them in the app store. Therefore there was no need for anti-malware software.

Well guess what? There is a need for anti-malware software on these devices, because there have been many security exploits over the years that have been implemented against them. What you need to do is go to the app store for your device and operating system and select one of the reputable anti-malware software apps that is available and install it on your system.

Reboot the Device 3:27-4:22

The next thing we need to talk about is how to reboot the device itself. The problem is that a lot of users just assume that when the device goes into suspend mode that it's powered off. But it's not. The device is still on and the operating system is still running. That's why it drains battery power even though the screen is off.

If you find that your device is running slowly, let's suppose this iPad is running slow or if I try to launch an app, it crashes every time I do, sometimes rebooting the device will fix a lot of problems. In fact, my experiences has been that it fixes a ton of problems.

The way you do this on an iPad is to hold down the suspend button. When you do, you'll see this icon displayed that says slide to power off. If I do, it'll then ask me if I really do want to power down the system. If I say yes, the device shuts off. Then, I click the suspend button again to power it back on. I don't want to do that on this one because we're recording demos but that's how you would reboot the device.

Backup Mobile Device 4:23-5:29

The last thing I want to talk about is how to back up the data on the device. You have two options for doing this. One option is to connect this device to a PC system using a USB cable and then use the appropriate utility to back up the device. Because were dealing with an iPad, we can use iTunes to back up the device.

Another option is to back up the device to the cloud. That's quickly becoming preferred option. If we put the backup of the device in the cloud, I can access that data wherever I have an internet connection. I can even synchronize that information with a standard computer system that's running the iCloud client software.

On this iPad device, I tap Settings and then I tap my User Account up in the upper left pane. Next I tap on iCloud Backup over to the right. Let's tap it to open it.

When turned on, iCloud Backup will automatically backup the data on our device including our accounts, documents and so on.

It also points out that this will work only if three conditions are met. The iPad has to be connected to power, the screen has to be locked, and the iPad has to be connected via Wi-Fi to the network.

I'm going to turn this off and tap OK.

Summary 5:30-5:45

That's it for this demonstration. In this demo, we talked about how to maintain a mobile device. First we talked about how to delete apps that you don't need. We talked about implementing anti-malware on the device. We talked about installing operating system and app updates. And then, we ended this demonstration by talking about how to back up the device.

12.7.7 Mobile Device Troubleshooting Facts


Mobile devices present a unique challenge for troubleshooting. Their mobile nature makes them prone to a variety of problems that can manifest in various ways.

This lesson covers the following topics:

- Troubleshooting tools
- Common mobile issues

Troubleshooting Tools


You can use the following tools to help troubleshoot mobile devices.

Tool	Description
App scanner	<p>An app scanner is a tool that can identify problems with installed apps.</p> <ul style="list-style-type: none">• When installed, the app scans all installed apps on the mobile device and uses a definitions list to identify any issues.• You can configure an app scanner to automatically scan the mobile device on a specified schedule. <div> Because app scanners use a definitions list to identify problems, it is important to always keep the list up to date.</div>
Wi-Fi analyzer	<p>Wi-Fi analyzers are special apps you can use to troubleshoot Wi-Fi connectivity issues. Most Wi-Fi analyzer apps provide the following functionality:</p> <ul style="list-style-type: none">• Identify the number of wireless access points (WAPs) that are broadcasting.• Display the signal strength and channel of each wireless network.• Obtain wireless network information (e.g., signal band, SSID, security mode, etc.).
Cell tower analyzer	<p>You can use a cell tower analyzer to troubleshoot cellular network connectivity by displaying the following information:</p> <ul style="list-style-type: none">• Signal strength/interference.• Number of cell towers in the area.• The location of each cell tower.• Mobile network information (e.g., network type, data activity, service provider, etc.).

Common Mobile Issues

The following table describes the most common mobile issues and the actions you can take to identify and fix the problem.

Issue	Description
No display	<p>A mobile device's display can stop working for a several reasons. If you are troubleshooting a mobile device with a display issue, take the following actions.</p> <ul style="list-style-type: none"> • Verify the device is fully charged and powered on. It is possible that the device is powered off or the battery is drained. • Check the device's brightness level. If the brightness level is too low, it may appear as though the display is off. Look at the screen in a dark room to make sure this isn't the case. • Find out if the device was dropped. When a mobile device is dropped, it is possible for the screen to be damaged, even if there is no visible physical damage. • Look for physical damage. If the screen is cracked or the device has physical damage, the display is most likely broken and needs to be replaced. • If the device is displaying but won't cast to an external device (e.g., a television), make sure both devices: <ul style="list-style-type: none"> ◦ Are using updated software versions ◦ Have permission to connect to other devices ◦ Are paired correctly ◦ Use online forums to search the symptoms and find solutions for the specific devices. Or contact the device's manufacturer for support.
Non-responsive touchscreen	<p>Mobile devices use capacitive touchscreens that require a conductive material touching the screen to work. If the touchscreen is not functioning or is inaccurate, you should:</p> <ul style="list-style-type: none"> • Look for liquid on the screen. Because water is conductive, any type of moisture on the screen will result in erratic touchscreen behavior. • Check for cracks or physical damage. A cracked screen can disrupt the current flow across the screen and cause specific sections of the touchscreen to fail. • Make sure the screen is calibrated. You can calibrate it using the device's built-in calibration app.
Unauthorized access	<p>Mobile devices are vulnerable to many of the same attacks that target desktop systems. One such attack is unauthorized access, where an attacker gains access to a specific feature or functionality of the mobile device.</p> <ul style="list-style-type: none"> • Unauthorized account access occurs when an attacker obtains the login credentials for a cloud backup service or the device itself. This can result in leaked personal files and data. To protect against this: <ul style="list-style-type: none"> ◦ Use some authentication on the mobile device. ◦ Use complex passwords. ◦ Set up two-factor authentication with all accounts that contain sensitive information. • Unauthorized root access is typically the result of a virus or malicious program installed on the mobile device. With root access, the malicious program can make low-level system changes to the mobile device, including modifying root certificates. To protect against unintended root access: <ul style="list-style-type: none"> ◦ Install a anti-malware app on the mobile device. ◦ Keep it up to date. • Unauthorized location tracking occurs when the GPS on the device is being used to track the user's location without permission. To protect against this: <ul style="list-style-type: none"> ◦ Review the device's security settings.

	<ul style="list-style-type: none">◦ Identify the installed apps that have access to location services.◦ Modify the permissions to deny location tracking access for those app's that you don't want to track the user.• Unauthorized camera/microphone activation is the use of the device's camera or microphone without the user's permission. This can be caused by a malicious program, a malicious individual, or an installed application that has been granted permission to use these services.• Most mobile devices have an LED or icon that indicates if the camera is being used. If a camera is being used without permission:<ul style="list-style-type: none">◦ Review the device's security settings and app permission settings.◦ Install an anti-malware app and run a scan on the device to remove any malicious apps. <div> If you become locked out of your phone, you can always get back in by performing a factory reset, but note that this will remove all data from your device.</div>
Weak or no signal	<p>Most connectivity issues are a result of a weak signal or some sort of interference.</p> <ul style="list-style-type: none">• If the device is having problems connecting to a wireless network:<ul style="list-style-type: none">◦ Verify the wireless adapter is turned on.◦ Verify that the wireless configuration settings are correct.◦ Use a Wi-Fi analyzer to identify the network's signal strength as well as interference sources (e.g., other network signals).◦ Verify that the data limit data limit hasn't been exceeded and data access is being denied by the provider.• If the device is having problems with cellular service:<ul style="list-style-type: none">◦ Make sure the mobile device has a SIM card installed.◦ Use a cell tower analyzer to identify network coverage, signal strength, and network type (i.e., 1x, 3G, 4G).◦ Verify that the data limit data limit hasn't been exceeded and data access is being denied by the provider.
Slow performance	<p>If the device seems to be running slow, actions to identify the problem include:</p> <ul style="list-style-type: none">• Identify system resources and usage. Many mobile devices have a system monitor you can use to identify the apps using system resources (i.e., memory, processor, etc.).• Make sure the apps being used are compatible with the mobile device. Older mobile devices have slower processors and might not be able to run all the latest mobile apps available to it.• Check the amount of free storage on the mobile device. If a mobile device's storage is more than 80% full, performance can be reduced considerably.• Turn off an overheating phone and place it in a cool place out of direct sunlight. Overheating can damage hardware, but cooling the device can correct issues. Avoid overheating by keeping the phone out of direct sunlight and extremely hot places, such as a car parked in direct sunlight.• Troubleshoot speakers not performing correctly, by checking the sound settings.<ul style="list-style-type: none">◦ Make sure nothing is set to Mute, Vibrate, Do not Disturb, or Silent.◦ Make sure the phone isn't connected to another device with Bluetooth.

- If speakers still aren't working, plug headphones into the device. If you can hear sound through the headphones but not through the device's speakers, you may have a hardware issue.
 - Turn the phone off and back on again.
 - Contact phone's manufacturer or the cell service provider for support if the you can't resolve the issue.
- If the GPS isn't functioning:
 - Verify the phone is receiving a clear signal. You need a clear signal for the GPS to work and to troubleshoot any GPS problems.
 - Verify the location permissions are enabled for the app you are trying to use.
 - Refresh location services by turning the **Location** function on and off or putting the phone in Airplane mode for a few moments.
 - If these solutions don't work, you may have to reset all the location and network data, or restore the device's factory settings.
- Review security and performance logs on a phone. This can help you troubleshoot performance issues.
 - Review materials from the device manufacturer to learn how review logs on the phone.
 - Be aware that you may have to connect the phone to a computer with a USB.