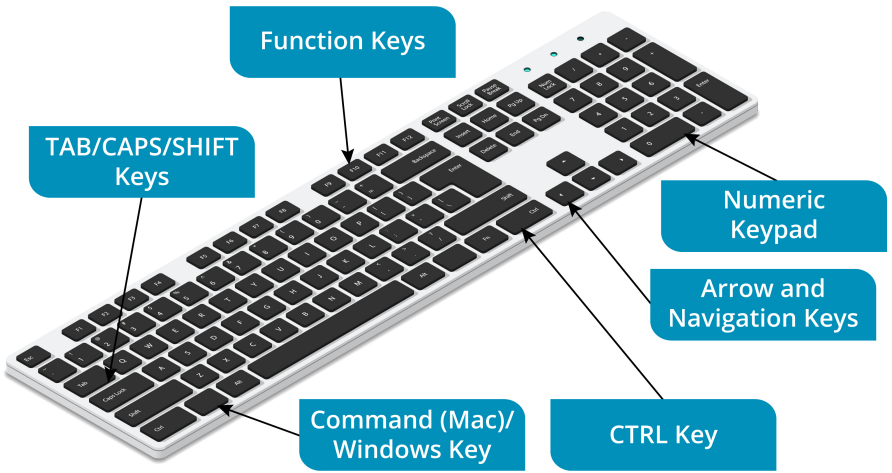
Input Devices

Human Interface Devices: (HIDs) Peripherals that enable the user to enter data and select commands.

- Peripherals that enable users to communicate with a PC.
- Data entry or command issuance.
- Keyboard and pointing devices most common input devices.

Keyboards (Slide 1 of 2)

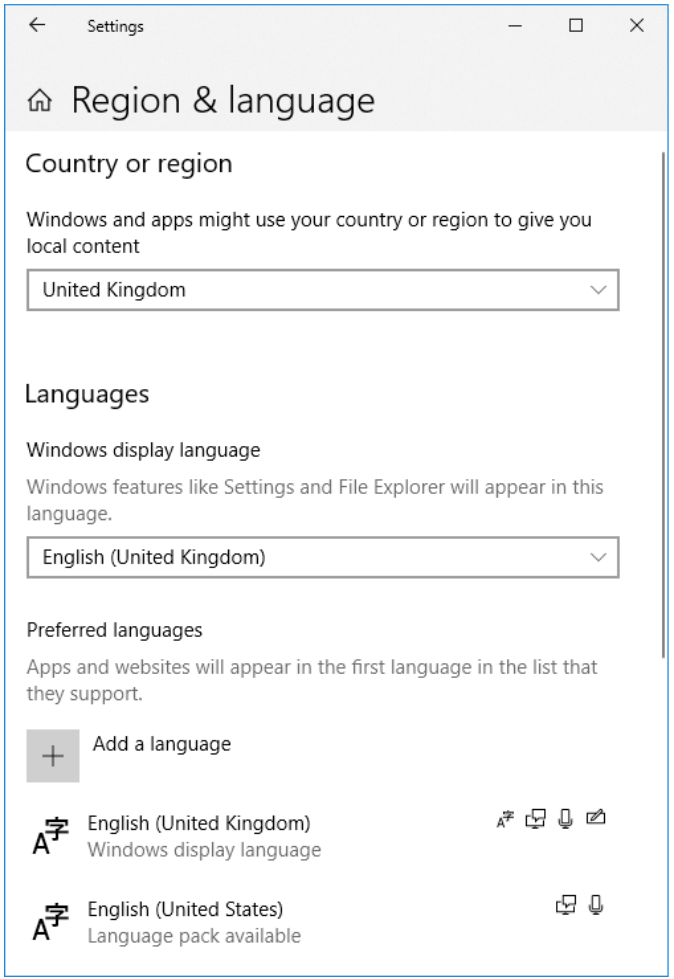
Keyboard: The oldest PC input device and still fundamental to operating a computer. There are many different designs and layouts for different countries. Some keyboards feature special keys.

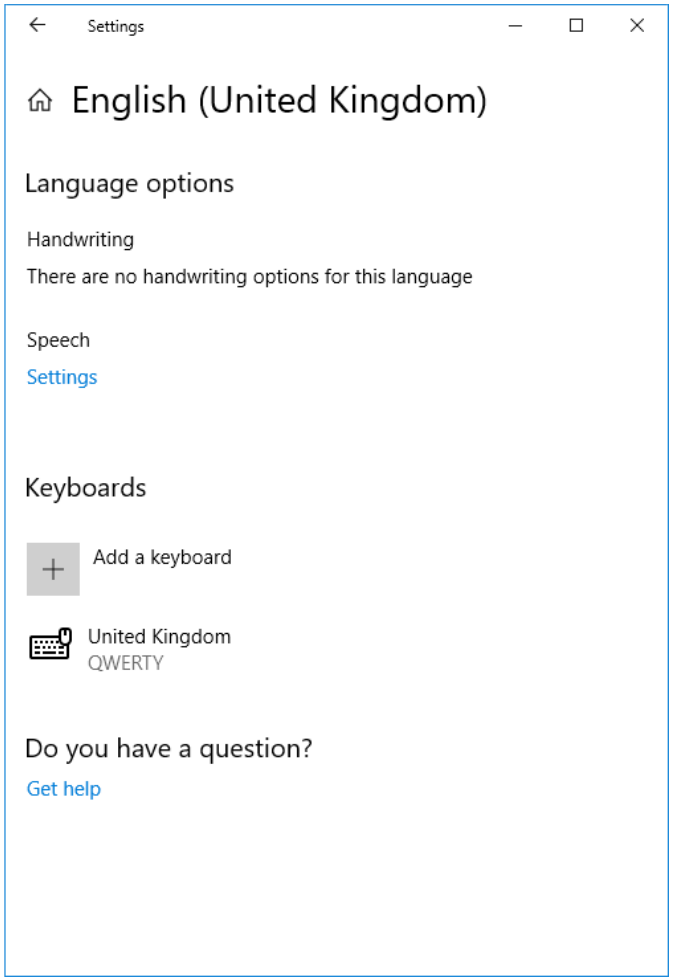


Extended

Ergonomic

Keyboards (Slide 2 of 2). You can change languages

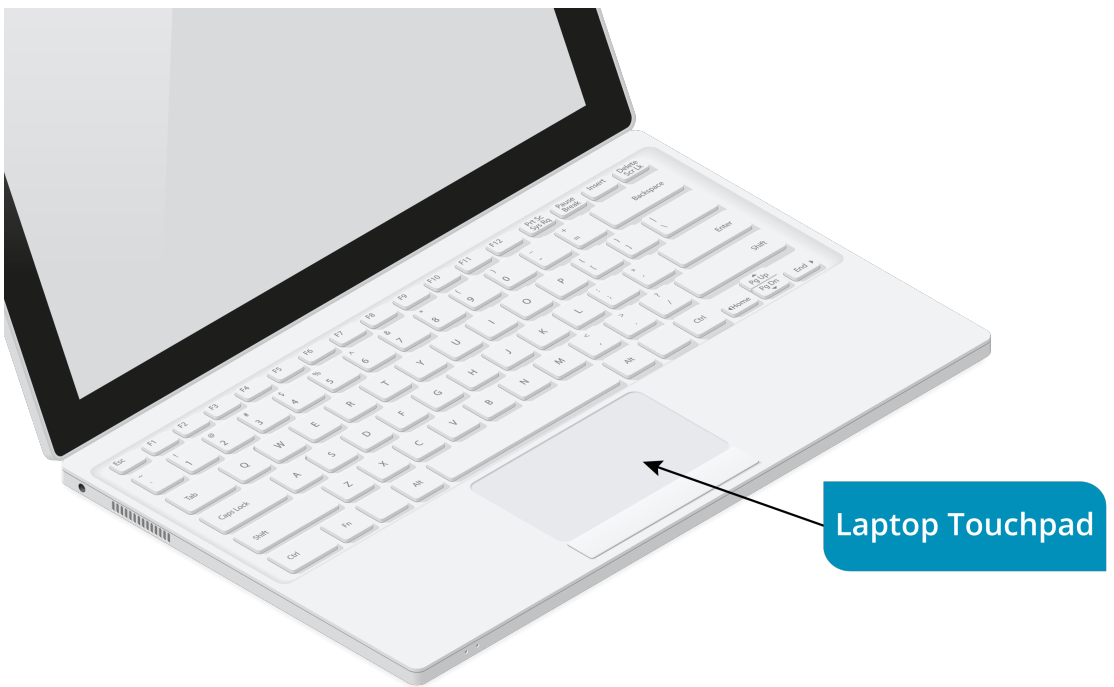




Pointing Devices (Slide 1 of 2)

Pointing device: A peripheral used to move a cursor to select and manipulate objects on the screen.

Mouse



Pointing Devices (Slide 2 of 2)

Game Controller

KVM Switches

KVM switch: (keyboard, video, mouse) A switch supporting one set of input and output devices that control multiple PCs.

- More typically used with servers.
  - 2-port versions allow one keyboard, mouse, and display to be used with 2 PCs.

Security Input Devices (Slide 1 of 3)

- Biometric authentication devices confirm identity via physical characteristics.
  - Retinal patterns
  - Fingerprints
  - Voice print

- Smart card readers feature a slot or sensor to interact with a smart card.
  - Smart cards hold digital certificates.
  - The combination of the certificate and a PIN or password provides security.

Security Input Devices (Slide 2 of 3)

- Magnetic strip/chip readers.
  - Strip holds account information.
  - Chip readers specifically for PoS systems.

- NFC and tap pay devices.
  - Contactless readers use NFC.

Security Input Devices (Slide 3 of 3)

- Signature pads.
  - Used with database of approved signatures.
  - Comparison with stored signature verifies identity.

Installation and Configuration Considerations (Slide 1 of 2)

Plug-and-Play: A protocol framework allowing network devices to autoconfigure services.

System resources: Settings that enable a device to communicate with the CPU and memory without the device conflicting with other devices.

Resource	Description
Memory Ranges/ I/O Addresses	• I/O address map defines each device's memory addresses. • Port addresses range from 0000 to FFFF.
IRQs	• Request for CPU attention. • IRQs range from 0 to 15. • Interrupt controllers allow IRQ sharing by multiple devices.

Installation and Configuration Considerations (Slide 2 of 2)

- Hot swap enables devices to be added or removed without shutting down the PC.
- Drivers might need to be installed or updated (auto or through vendor)
- Connections made by plugging devices into the correct port.
- Configuration after installation.
  - Device Manager
  - Control Panel
  - Windows Settings
  - Vendor software

Guidelines for Installing Peripheral Devices

- Always read the manufacturer's instructions and check that the device is compatible with the PC and operating system.
- Hold the connector, not the cable, when removing a lead.
- Inspect the connector and port for damage (notably broken or bent pins) before attaching a lead.
- Take care to align the connector carefully and do not use excessive force, to avoid damaging the pins.
- Check whether the device requires an external power source.

Activity

Discussing Peripheral Device Installation

30bird labs 7

KVM: https://www.youtube.com/watch?v=CYq9aeDNAFA

Troubleshooting Basics

- The process of problem-solving.
- Focus on causes, symptoms, and consequences.
  - Hard disk drive fault (cause).
  - Fault causes the PC to display a blue screen (symptom).
  - Blue screen prevents user from accomplishing work (consequence).
- Sometimes resolving the consequence is more important than addressing the cause.
- Causes can also be symptoms of larger problems.
  - Especially with recurring issues.

Problem Management

Problem management: A method of identifying, prioritizing, and establishing ownership of incidents.

Incident: Something that is not normal and disrupts regular operations in the computing environment.

1. User contacts Help Desk.
   - Operator or technician is assigned, and trouble ticket is generated.
2. User describes the problem.
   - Operator asks clarifying questions, and categorizes the problem, assesses urgency, and estimates time to resolve.
3. Operator might walk user through some initial troubleshooting steps.
   - Ticket might be escalated to another support person.
4. Troubleshooting continues until the problem is resolved.
   - Operator confirms user satisfaction and records details on trouble ticket and closes it.

The CompTIA A+ Troubleshooting Model (Slide 1 of 2)

1. Identify the problem.
   - Question the user, and identify changes to the computer.
   - Perform backups before implementing any changes.
   - Ask about environmental or infrastructure changes (new equipment? New software?)
   - Review system and app logs.
2. Establish a theory of probable cause.
   - Question the obvious (KISS). “is your machine plugged in” is not just a meme.
   - If necessary, conduct internal or external research based on symptoms.
     - Knowledge base (internal), forums and internet (external)
3. Test the theory to determine causes.
   - Once the theory is confirmed, determine the next steps to solve the problem.
   - If the theory is not confirmed, re-establish a new theory or escalate the issue.

The CompTIA A+ Troubleshooting Model (Slide 2 of 2)

4. Establish a plan of action to resolve the problem and implement the solution.
   - repair, replace, or ignore
5. Verify full system functionality, and if applicable, implement preventive measures.
   - Make sure it doesn't happen again. This can take many forms.
6. Document findings, actions, and outcomes.
   - You don't want to be caught flat footed if this happens again six months down the road to a coworker.

Customer Service and Communication Skills

- Soft skills can be as important as technical skills.
- Question types:
  - Open questions: Encourage the user to explain in their own words.
  - Closed questions: Yes/No, or reading an error message off the screen.
- Develop a troubleshooting mindset.
  - Be calm.
  - Take breaks.
  - Challenge assumptions.
  - Assess costs and impact.
  - Know when to escalate an issue.

Problem Identification (Slide 1 of 2)

- Work methodically to ensure you diagnose the correct problem and select the best resolution.
- Troubleshooting combines problem-solving with decision-making.
- Be prepared before starting the process.
  - Gather tools, documentation, and other necessities.
  - Use clear, concise, and accurate instructions when asking users to perform tasks.
  - Schedule downtime as needed, but be sensitive to the user's needs.
- Back up locally stored data.
  - Consider imaging the drive before changing any configuration parameters.

Problem Identification (Slide 2 of 2)

- Elicit factual information from the user or technician who reports the issue:
  - What are the exact error messages on the screen or coming from the speaker?
  - Has anyone else experienced the same issue?
  - How long has the problem been occurring?
  - What has changed? Did you change things, or did someone else?
  - Has anything been tried to solve the problem?

Sources of Information

- Perform a physical inspection.
- Reproduce the problem.
  - If you can recreate it, that can provide additional clues for fixing.
- Check system and application logs or diagnostic software.
- Check the system documentation, such as installation or maintenance logs.
- Consult any other technicians who might have worked on the system recently or who might be working on a related issue.

Determination of Probable Causes

- Diagnose problems by identifying symptoms.
- Symptoms can lead you to possible causes.
- Question the obvious.
  - Step through what should happen, either yourself or by observing the user, and identify the point at which there is a failure or error.
  - Work up or down layers (for example, power, hardware components, drivers/firmware, software, network, and user actions).
- Categorize and eliminate non-causes.
- Be prepared to backtrack and try different paths.
- Research the issue.
- Re-establish a theory when necessary.

Problem Escalation

- Confer with colleagues and others when you are stuck.
- Escalate when you can’t solve a problem.
  - Senior staff, knowledge experts, SMEs, technical staff, developers, programmers, and administrators within your company.
  - Suppliers and manufacturers—warranty and support contracts and helplines or web contact portals.
  - Other support contractors and consultants, websites, and social media.
- Balance timeliness with possible higher costs.
- Follow organizational policies.

Solution Implementation and Testing

- Three possible solutions for most IT problems:
  - Repair.
  - Replace.
  - Workaround.
- Assess costs and time requirements.
- Be aware of change management policies.
- When implementing solutions:
  - Consider the effect on others.
  - Test after each change, and revert if the change does not solve the problem.

Verification and Documentation

- Tests:
  - Try to use a component.
  - Swap component out for a known good one.
  - Inspect component for proper connection, damage, and indicator lights.
  - Disable or uninstall a component.
  - Check documentation and software diagnostic tools.
  - Update software or device drivers.
- Be sure you are satisfied the problem is solved.
- Be sure the user is satisfied the problem is solved.
- Implement preventive measures.
- Document findings, actions, and outcomes.
  - Helps immensely with future troubleshooting.

Activity

Discussing Troubleshooting Methodology

Reflective Questions

1. Will there be any specialty input devices that you will need to install or configure at your workplace? How might this affect your day-to-day activities as an IT professional?

2. Which part of the CompTIA A+ Troubleshooting Model do you expect to find most challenging, and why?