Device Configuration and Management

Student Edition

Presented By

LearnKey®

Device Configuration and Management Project Workbook

First Edition

LearnKey creates signature multimedia courseware. LearnKey provides expert instruction for popular computer software, technical certifications, and application development with dynamic video-based courseware and effective learning management systems. For a complete list of courses, visit https://www.learnkey.com.

www.learnkey.com

LK LearnKey

Table of Contents

Introduction

Device Configuration and Management

Best Practices Using LearnKey's Online Training

LearnKey offers video-based training solutions that are flexible enough to accommodate private students and educational facilities and organizations.

Our course content is presented by top experts in their respective fields and provides clear and comprehensive information. The full line of LearnKey products has been extensively reviewed to meet superior quality standards. Our course content has also been endorsed by organizations such as Certiport, CompTIA®, Cisco, and Microsoft. However, it is the testimonials given by countless satisfied customers that truly set us apart as leaders in the information training world.

LearnKey experts are highly qualified professionals who offer years of job and project experience in their subjects. Each expert has been certified at the highest level available for their field of expertise. This expertise provides the student with the knowledge necessary to obtain top-level certifications in their chosen field.

Our accomplished instructors have a rich understanding of the content they present. Effective teaching encompasses presenting the basic principles of a subject and understanding and appreciating organization, real-world application, and links to other related disciplines. Each instructor represents the collective wisdom of their field and within our industry.

Our Instructional Technology

Each course is independently created based on the manufacturer's standard objectives for which the course was developed.

We ensure that the subject matter is up-to-date and relevant. We examine the needs of each student and create training that is both interesting and effective. LearnKey training provides auditory, visual, and kinesthetic learning materials to fit diverse learning styles.

Course Training Model

The course training model allows students to undergo basic training, building upon primary knowledge and concepts to more advanced application and implementation. In this method, students will use the following toolset:

Pre-assessment: The pre-assessment is used to determine the student's prior knowledge of the subject matter. It will also identify a student's strengths and weaknesses, allowing them to focus on the specific subject matter they need to improve the most. Students should not necessarily expect a passing score on the pre-assessment as it is a test of prior knowledge.

Video training sessions: Each training course is divided into sessions or domains and lessons with topics and subtopics. LearnKey recommends incorporating all available external resources into your training, such as student workbooks, glossaries, course support files, and additional customized instructional material. These resources are located in the folder icon at the top of the page.

Exercise labs: Labs are interactive activities that simulate situations presented in the training videos. Step-by-step instructions and live demonstrations are provided.

Post-assessment: The post-assessment is used to determine the student's knowledge gained from interacting with the training. In taking the post-assessment, students should not consult the training or any other materials. A passing score is 80 percent or higher. If the individual does not pass the post-assessment the first time, LearnKey recommends incorporating external resources, such as the workbook and additional customized instructional material.

Workbook: The workbook has various activities, such as fill-in-the-blank worksheets, short answer questions, practice exam questions, and group and individual projects that allow the student to study and apply concepts presented in the training videos.

Using This Workbook

This project workbook contains practice projects and exercises to reinforce the knowledge you have gained through the video portion of the **Device Configuration and Management** course. The purpose of this workbook is twofold. First, get you further prepared to pass the Device Configuration and Management exam, and second, to teach you job-ready skills and increase your employability in the area of Windows devices.

The projects within this workbook follow the order of the video portion of this course. To save your answers in this workbook, you must first download a copy to your computer. You will not be able to save your answers in the web version. You can complete the workbook exercises as you go through each section of the course, complete several at the end of each domain, or complete them after viewing the entire course. The key is to go through these projects to strengthen your knowledge in this subject.

Each project is based upon a specific video (or videos) in the course and specific test objectives. The materials you will need for this course include:

- LearnKey's **Device Configuration and Management** courseware.
- A device running a Windows 10 or Windows 11 operating system.
- The course project files. All applicable project files are located in the support area where you downloaded this workbook.

For Teachers

LearnKey is proud to provide extra support to instructors upon request. For your benefit as an instructor, we also provide an instructor support .zip file containing answer keys, completed versions of the workbook project files, and other teacher resources. This .zip file is available within your learning platform's admin portal.

Notes

- Extra teacher notes, when applicable, are in the Project Details box within each exercise.
- Exam objectives are aligned with the course objectives listed in each project, and project file names correspond with these numbers.
- The Finished folder in each domain has reference versions of each project. These can help you grade projects.
- Short answers may vary but should be similar to those provided in this workbook.
- Teachers may consider asking students to add their initials, student ID, or other personal identifiers at the end of each saved project.
- Refer to your course representatives for further support.

We value your feedback about our courses. If you have any questions, comments, or concerns, please let us know by visiting https://about.learnkey.com.

LearnKey

Skills Assessment

Instructions: Rate your skills on the following tasks from 1-5 (1 being needs improvement, 5 being excellent).

Skills	1	2	3	4	5
Install Windows using the default settings.	☐	☐	☐	☐	☐
Configure user account options.	☐	☐	☐	☐	☐
Configure desktop settings.	☐	☐	☐	☐	☐
Manage accessibility settings.	☐	☐	☐	☐	☐
Manage updates.	☐	☐	☐	☐	☐
Manage applications and Windows features.	☐	☐	☐	☐	☐
Compare and contrast capabilities of peripheral connection types.	☐	☐	☐	☐	☐
Describe cloud services.	☐	☐	☐	☐	☐
Describe and configure file sharing and permissions.	☐	☐	☐	☐	☐
Manage backup and restore.	☐	☐	☐	☐	☐
Describe data access and retention policies.	☐	☐	☐	☐	☐
Describe network firewall settings.	☐	☐	☐	☐	☐
Describe user authentication.	☐	☐	☐	☐	☐
Given an attack type, describe mitigation methods.	☐	☐	☐	☐	☐
Manage User Account Control (UAC) settings.	☐	☐	☐	☐	☐
Manage mobile device security.	☐	☐	☐	☐	☐
Perform troubleshooting tasks.	☐	☐	☐	☐	☐
Troubleshoot operating system and application issues.	☐	☐	☐	☐	☐
Troubleshoot device issues.	☐	☐	☐	☐	☐
Troubleshoot device connections to networks and domains.	☐	☐	☐	☐	☐

Skills	1	2	3	4	5
Troubleshoot peripheral device connections.	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

Device Configuration and Management Video Times

Domain 1	Video Time
Install Windows	00:05:35
Configure User Account Options	00:02:33
Configure Desktop Settings	00:10:12
Manage Accessibility Settings	00:04:51
Manage Updates	00:03:06
Total Time	**00:26:17**

Domain 2	Video Time
Manage Applications and Windows Features	00:04:18
Capabilities of Peripheral Connections	00:03:47
Total Time	**00:08:05**

Domain 3	Video Time
Describe Cloud Services	00:03:43
File Sharing and Permissions	00:07:59
Manage Backup and Restore	00:02:41
Data Access and Retention Policies	00:01:59
Total Time	**00:16:22**

Domain 4	Video Time
Describe Network Firewall Settings	00:02:51
Describe User Authentication	00:03:08
Attack Mitigation Methods	00:06:26
UAC Settings	00:05:09
Manage Mobile Device Security	00:03:25
Total Time	**00:20:59**

Domain 5	Video Time
Perform Troubleshooting Tasks	00:06:47
Troubleshoot Operating System and Application Issues	00:08:05
Troubleshoot Device Issues	00:03:16
Troubleshoot Device Connections to Networks and Domains	00:02:48
Troubleshoot Peripheral Device Connections	00:04:08
Total Time	**00:25:04**

Domain 1
Lesson 1

Device Configuration and Management

Fill-in-the-Blanks

Instructions: While watching Domain 1 Lesson 1, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. An upgrade install overwrites the current _____with a newer version. [Time Zone Options and Upgrade vs. Custom Install]
2. A local account uses a username and _____ to sign in to Windows, whereas a Microsoft account uses an email address. [Microsoft Account vs. Custom Install]
3. The first account created when installing an operating system is automatically a(n) _____account and has the highest level of access. [Account Types]
4. The main display is automatically labeled display _____ in display settings. [Display and Time Zone Settings]
5. On Windows 11 devices, the Start menu and taskbar are _____ at the bottom of the screen. [Start Menu]
6. It is wise to _____ your account anytime you walk away from your computer, especially if you work in a public place. [Power Settings]
7. Pinning an app to the taskbar creates a _____ for the app. [Taskbar Settings and App Shortcuts]
8. The _____ feature hides the window to the taskbar, while the _____ feature fills the application to the screen. [Windows Management]

Install Windows

An operating system allows users to communicate with their computer or device. It is responsible for helping the computer store files, run software, and connect to the internet. An operating system must be installed on a new computer, and the Windows operating system can be installed as an upgrade or a custom installation. Users can change settings such as language or accept the default settings. Users can sign in using a Microsoft account or a local account and set a PIN to allow for secure access.

Purpose

Upon completing this project, you will better understand the difference between an upgrade and a custom installation and what options are available during a Windows installation.

Steps for Completion

1. What is the difference between an upgrade and a custom installation?

   _____
   _____
   _____
   _____

2. Is a product key always required during a Windows installation? Why or why not?

   _____

3. What options does a Windows installer ask to confirm before beginning the installation process?

   _____

4. A Microsoft account allows one to use _____ verification to add an extra layer of protection when signing in.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
- **Topic**: Install Windows
  - **Subtopic**: Time Zone Options and Upgrade vs. Custom Install; Microsoft Account vs. Custom Install

Objectives covered
1 Windows Installation and Configuration
- **1.1** Install Windows using the default settings
  - **1.1.1** Time zone options
  - **1.1.2** Microsoft vs. Local Account
  - **1.1.3** Upgrade vs. Custom install

User Accounts

Users must create an account when setting up Windows for the first time. An administrator account can add user accounts to a device using users' Microsoft accounts or creating local accounts. An administrator account assigns permissions to local users and can create additional administrator accounts.

Purpose

Upon completing this project, you will better understand the distinctions between cloud and local accounts and the purpose of administrator accounts.

Steps for Completion

1. Determine whether the following statements are True or False:
   a. _____ The first account created is automatically the administrator.
   b. _____ Local accounts require an internet connection.
   c. _____ Only one administrator account can exist on a single device.
   d. _____ Security questions should be unique and challenging.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Configure User Account Options
Subtopic: Account Types

Objectives covered
1 Windows Installation and Configuration
1.2 Configure user account options
1.2.1 User account (cloud or local)
1.2.2 Local user and administrative account types

Display Settings

There are several customization options available under Display settings. For example, the brightness of the screen can be raised or lowered. When using multiple displays, the displays can be arranged in Display settings to match the arrangement of the monitors. Displays can be extended, duplicated, or shown only on one monitor.

Purpose

Upon completing this project, you will better understand the display options available and the differences between them.

Steps for Completion

A. Extend these displays	D. Display resolution
B. Night light	E. Duplicate the display
C. Scaling	

1. Match each display setting name to its effect.
   a. _____ Reduces blue light and emits warmer colors
   b. _____ Changes how many pixels are displayed horizontally and vertically
   c. _____ Creates a panoramic display with multiple monitors
   d. _____ Changes the size of items on the screen
   e. _____ Shows the same display on two or more monitors
2. Time zones can be set to a specific time zone or set _____.
3. If using a Windows device, change your scaling to 150%.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: Configure Desktop Settings
Subtopic: Display and Time Zone Settings

Objectives covered
1 Windows Installation and Configuration
1.3 Configure desktop settings
1.3.2 Display settings
1.3.4 Time zone settings

Start Menu

The Start menu offers quick access to applications, power settings, and account options. It differs slightly between Windows 10 and Windows 11 in appearance and placement, and power options include Sleep, Shutdown, and Restart. Users can sign out or lock their computer from the Start menu.

Purpose

Upon completing this project, you will better understand using the Start menu and available power options.

Steps for Completion

1. What are two differences between the Start menu on Windows 10 and Windows 11?

   _____
   _____
   _____
   _____
   _____

2. On the Windows 10 Start menu, the Documents and Pictures options open _____.
3. The power option used to fix an application error or clear the RAM cache is _____.
4. In _____ mode, applications stay open and ready to use.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Configure Desktop Settings
Subtopic: Start Menu; Power Settings

Objectives covered
1 Windows Installation and Configuration
1.3 Configure desktop settings
1.3.1 Start menu
1.3.6 Power settings

LearnKey

Taskbar Settings and App Management

The taskbar shows applications currently open and application shortcuts that users have pinned. The taskbar can be hidden or always visible, and its location on a display can be changed. Application windows can be minimized, maximized, or closed. Windows 11 offers Snap Layouts, which provides additional options for managing windows.

Purpose

Upon completing this project, you will better understand how to change taskbar settings and manage application windows.

Steps for Completion

1. Users can reveal a hidden taskbar by _____ over it.
2. The default location of the taskbar is at the _____ of the screen.
3. Users can find Taskbar options within their device Settings, under _____.
4. Explain what each app window management option does.
   a. Close: _____
   b. Minimize: _____
   c. Maximize: _____
   d. Snap Layouts: _____
5. If you are using Windows 11, open three or four windows and organize them using Snap Layouts. If you are using Windows 10, open two applications and arrange them on either side of your screen.

Project Details

Project file
N/A

Estimated completion time
5-10 minutes

Video reference
Domain 1
Topic: Configure Desktop Settings
Subtopic: Taskbar Settings and App Shortcuts; Windows Management

Objectives covered
1 Windows Installation and Configuration
1.3 Configure desktop settings
1.3.3 Application shortcuts
1.3.5 Taskbar settings
1.3.7 Windows management

Domain 1
Lesson 2

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 1 Lesson 2, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. The _____ setting results in a change in brightness around mouse pointer touchpoints. [Display Settings and Mouse Settings]
2. Someone who is _____ might use color filters to help distinguish between colors. [Color Filters and High-Contrast Settings]
3. In the Ease of Access audio settings, users can set notifications to _____the active window or the entire screen. [Audio Settings and Closed Captions]
4. Speech recognition is software that can convert spoken words into _____. [Speech Recognition and Magnifier]
5. Sticky Keys allows users to keep _____ such as the Shift key active until they select another key to deactivate it. [Sticky Keys and On-Screen Keyboard]
6. The Narrator reads any text and _____ on the screen out loud. [Narrator]
7. The longest users can pause Windows Updates for is _____ days, after which they should run updates as soon as possible. [Windows Updates and Update History]
8. Optional updates do not include _____ fixes. [Patches, Optional, and Driver Updates]

Visual Accessibility

Accessibility settings for Windows are under the Ease of Access menu. There are display options available under the Vision settings, such as changing text size. There are also options to change mouse pointer properties such as size and color. Color filters and high contrast settings can make the display easier for users with vision impairments or colorblindness to see display elements better.

Purpose

Upon completing this project, you will better understand the visual accessibility options available for Windows.

Steps for Completion

1. Selecting _____ in Mouse Pointer settings allows users to set the mouse pointer to any color.
2. If you are using a Windows device, change the color and size of your mouse pointer.
3. The Ease of Access Display settings allow users to make just the text bigger or make _____ on the main display bigger.
4. Color filters can invert colors or change them to grayscale to make them more _____.
5. High contrast changes background colors and _____ colors to make on-screen elements more visible.
6. If you are using a Windows device, turn on and off one of the high contrast settings.

Project Details

Project file
N/A

Estimated completion time
5-10 minutes

Video reference
Domain 1
Topic: Manage Accessibility Settings
Subtopic: Display Settings and Mouse Settings; Color Filters and High-Contrast Settings

Objectives covered
1 Windows Installation and Configuration
1.4 Manage accessibility settings
1.4.1 Display settings
1.4.2 Mouse settings
1.4.3 Color filters
1.4.4 High contrast settings

Audio Accessibility

There are audio and closed caption settings under the Hearing section of Ease of Access. Under Audio, there are options for device volume and to change how notifications are shown. Under Closed Captions, there are options to change the color, size, and transparency of the caption text and caption background.

Purpose

Upon completing this project, you will better understand the audio accessibility options available in Windows.

Steps for Completion

1. If you are using a Windows device, watch a short video of your choice with closed captioning turned on.
2. What are two options available under the Audio settings in Ease of Access?

   _____

   _____

3. How does having a variety of closed captioning options improve accessibility?

   _____

   _____

   _____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Manage Accessibility Settings
Subtopic: Audio Settings and Closed Captions

Objectives covered
1 Windows Installation and Configuration
1.4 Manage accessibility settings
1.4.5 Audio settings
1.4.6 Closed captions

Interface Accessibility

Ease of Access offers several accessibility options based on interacting with the system and display. Options such as speech recognition and an on-screen keyboard allow users to input information without using a physical keyboard. The Magnifier and Narrator offer more tools for users with vision impairments. Sticky Keys can prevent repetitive strain injuries by eliminating key presses.

Purpose

Upon completing this project, you will better understand the accessibility features available for a Windows system interface.

Steps for Completion

A. Speech Recognition	D. Sticky Keys
B. Magnifier	E. On-Screen Keyboard
C. Narrator	

1. Match each accessibility feature with its description.
   a. _____ Reads text on screen out loud along with any notifications.
   b. _____ Converts spoken words into text.
   c. _____ Zooms in on parts of a display.
   d. _____ Allows users to input text using a mouse.
   e. _____ Allows users to keep modifier keys like Shift active.
2. If you are using a Windows device, practice using the On-Screen Keyboard.
3. Practice using Sticky Keys.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 1
Topic: Manage Accessibility Settings
Subtopic: Speech Recognition and Magnifier; Sticky Keys and On-Screen Keyboard; Narrator

Objectives co7ered
1 Windows Installation and Configuration
1.4 Manage accessibility settings
1.4.7 Speech Recognition
1.4.8 Magnifier
1.4.9 Narrator
1.4.10 Sticky Keys
1.4.11 On-Screen Keyboard

Manage Updates

Windows Updates often fix newly discovered flaws in the operating system or other Microsoft products. Patches fix specific vulnerabilities in operating systems or software programs, while general updates include many different features. Optional updates are bug fixes or patches that do not need to be implemented immediately. Driver updates help devices communicate more efficiently and are usually automatically installed. A history of updates to a device can be viewed under Settings and may be useful when troubleshooting a problem. Users can pause updates but only for a limited amount of time.

Purpose

Upon completing this project, you will better understand the different types of Windows updates.

Steps for Completion

1. Why is it important to regularly check for updates?

   _____
   _____
   _____

2. What is the difference between a driver update and a patch?

   _____
   _____
   _____

3. Determine whether the following statements are True or False:
   a. _____ Windows Updates can be paused indefinitely.
   b. _____ Optional updates do not include security fixes.
   c. _____ View update history only shows updates from the last month.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 1
Topic: Manage Updates
Subtopic: Windows Updates and Update History; Patches, Optional, and Driver Updates

Objectives covered
1 Windows Installation and Configuration
1.5 Manage updates
1.5.1 Windows update settings
1.5.2 Software updates and patches
1.5.3 Optional updates
1.5.4 Device driver updates
1.5.5 Update history

Domain 2
Lesson 1

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 2 Lesson 1, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. Administrative users have permission to install and uninstall all _____. [Optional Windows Features and App Removal]
2. The Microsoft Store allows users to install applications and _____ games and music. [Microsoft Store Purpose and Modify App Installs]
3. By default, most applications installed on a Windows computer will automatically be installed to drive _____. [Microsoft Store Purpose and Modify App Installs]
4. Users can enable parental controls in Windows by adding a(n) _____ account. [User Account Requirements]
5. An HDMI cable transmits _____ audio and video from another source like a TV or laptop. [HDMI and Mini-HDMI]
6. DisplayPort connectors transmit high-definition video and audio and are more commonly found on PCs than _____. [DisplayPort]
7. A VGA is (a)n _____ video graphics array connection and is used to link computers and laptops to additional monitors. [VGA]
8. USB cables can connect _____ and devices to a computer or transfer power. [USB]
9. USB-C is used to transmit data and power between a computer and a(n) _____. [USB-C and Converting Between Connection Types]

Manage Applications

Users can install and uninstall applications on their devices. Administrators have permissions to uninstall any application, though they should use caution when uninstalling optional features that came with the Windows operating system. Administrators can also install any application, while other users can only install the application types for which they have permissions. Users can enable parental controls by adding a child account, which allows them to set further limitations on how and when a child can use that device.

The Microsoft Store allows users to install both free and paid applications, and they can also purchase music and games. Applications are installed to drive C by default, but users can change where new content is saved if needed.

Purpose

Upon completing this project, you will better understand the options for managing applications and other Windows features.

Steps for Completion

1. Search for an app in the Microsoft Store. If you have the permissions to do so, install a free app on your device.
2. What are two apps that can be found in Optional features?

   _____
   _____
   _____
   _____

3. Determine whether the following statements are True or False:
   a. _____ All non-administrator accounts are managed with parental controls.
   b. _____ Standard accounts cannot install apps from the Microsoft Store.
   c. _____ Drive C is where Windows is stored on a computer.
   d. _____ Optional features can be uninstalled, but doing so may result in issues for the device.
4. What are four ways to use parental controls?

   _____
   _____
   _____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 2
- **Topic**: Manage Applications and Windows Features
  - **Subtopic**: Optional Windows Features and App Removal; Microsoft Store Purpose and Modify App Installs; User Account Requirements

Objectives covered
2 Application and Peripheral Management
- **2.1** Mange applications and Windows Features
  - **2.1.1** Identify user account requirements and permissions for application installation
  - **2.1.2** Modify application installations
  - **2.1.3** Remove desktop applications
  - **2.1.4** Locate and identify optional Windows features
  - **2.1.5** Describe the purpose of the Microsoft Store

Peripheral Connectors

Peripherals are hardware input or output devices such as a keyboard, mouse, camera, microphone, or printer. These devices are commonly connected to a computer using a port connection and a cable. Some of the port types available include HDMI, DisplayPort, VGA, and USB. Converters can be used in cases where devices have port types that do not match.

Purpose

Upon completing this project, you will better understand the purpose of different types of peripheral connections.

Steps for Completion

1. Label each connector type with its name:

a.  _____

b.  _____

c.  _____

d.  _____

2. What is each type of peripheral connector used for?

a. HDMI: _____

b. DisplayPort: _____

c. VGA: _____

d. USB: _____

e. USB-C: _____

Project Details

Project file
N/A

Estimated completion time
5-10 minutes

Video reference
Domain 2
Topic: Capabilities of Peripheral Connections
Subtopic: HDMI and Mini-HDMI; DisplayPort; VGA; USB; USB-C and Converting Between Connection Types

Objectives covered
2 Application and Peripheral Management
2.2 Capabilities of peripheral connections
2.2.1 HDMI
2.2.2 DisplayPort
2.2.3 VGA
2.2.4 Mini-HDMI
2.2.5 USB
2.2.6 USB-C
2.2.7 Converting between connection types

Domain 3
Lesson 1

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 3 Lesson 1, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. Cloud services allow users to store data and programs on _____ servers rather than on a computer's hard drive. [Cloud Storage]
2. A user can use a virtual machine to run a(n) _____ in an app window on their desktop. [Local and Hosted Virtual Machines]
3. Giving a user Read permissions allows them to view a file, while Read/Write allows them to view and _____ a file. [File Sharing Permissions]
4. Explicit permissions are the _____ permissions set when an object or file is created. [Effective Permissions and Share Types]
5. One can use _____ folders to share files with others using a shared network or PC. [Effective Permissions and Share Types]
6. A mapped drive is a(n) _____ to a physical location on a different computer that users can access through a shared network. [Map Drives]
7. When a file is moved or copied between file systems, it inherits permissions from the _____ folder. [Ownership of Files Between File Systems]
8. Backing up files creates a(n) _____ of important files so that a user can restore them if a device breaks or files are lost. [File Backup Types and Restore Operations]
9. A(n) _____ Use Policy is a document stating any constraints and practices that users must follow when using a corporate network. [Types of Retention and Data Access Policies]
10. A remote wipe is a security feature that allows users to _____ data remotely from a mobile device. [Types of Retention and Data Access Policies]

Cloud Services

Cloud services allow users to store data and programs on remote servers rather than on a computer hard drive. They can then access the data from any device with internet access and a web browser. Cloud storage allows individuals to save files and share them easily with others, and users can determine permissions for the documents they share.

A virtual machine allows individuals to run an operating system in an app window on their desktop and emulates a separate computer. It can be used to test and run different operating systems and software.

Purpose

Upon completing this project, you will better understand the different cloud services available to Windows users.

Steps for Completion

1. What is the purpose of each Microsoft cloud service?
   a. SharePoint: _____
   b. Microsoft Teams: _____
   c. Azure: _____
   d. OneDrive: _____
2. What are two ways a user might use a virtual machine?

   _____

   _____
3. The Sync Center allows users to create and open _____ files, which will automatically sync to the cloud the next time the device connects to the internet.
4. Giving users Editing permissions will allow them to edit and share the document while _____ mode will only allow them to make comments and suggestions.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 3
Topic: Describe Cloud Services
Subtopic: Cloud Storage; Local and Hosted Virtual Machines

Objectives covered
3 Data Access and Management
3.1 Describe cloud services
3.1.1 Cloud storage and collaboration concepts
3.1.2 Common cloud storage providers
3.1.3 File sharing capabilities and permissions
3.1.4 Capabilities of local and hosted virtual machines
3.1.5 Offline file synchronization

File Sharing Permissions

Windows allows users to share files with others in their network. Users can set a basic permission level of Read or Read/Write when sharing files. Advanced permission settings also allow users to individualize permissions for different people and groups.

A file's effective permissions are composed of explicit permissions, the default permissions set when that file was created, and inherited permissions that the file receives due to it being either a parent or a child object. Documents in a public folder can be shared with other users, and local users can always access a device's shared folders, while users on a shared network will only be able to do so if public folder sharing is turned on.

Purpose

Upon completing this project, you will better understand how to share files and set permissions from Windows File Explorer.

Steps for Completion

1. Open the Control Panel and turn on Public folder sharing.
2. Take a screenshot of the Advanced Sharing settings page and save it to your Domain 3 student folder as **321-Complete**.
3. File _____ allows a user to grant control to any other user and decide who can access the folder or file.
4. What is the difference between the Change permission and the Full Control permission?

   _____

   _____
5. A file will receive _____ permissions from the drive on which it was created.
6. Public folders are stored in the _____ folder on Drive C in File Explorer.

Project Details

Project file
N/A

Estimated completion time
5-10 minutes

Video reference
Domain 3
Topic: File Sharing and Permissions
Subtopic: File Sharing Permissions; Effective Permissions and Share Types

Objectives covered
3 Data Access and Management
3.2 Describe and configure file sharing and permissions
3.2.1 File and share permissions
3.2.2 Effective permissions
3.2.3 Basic and advanced permissions
3.2.4 Public, basic, and advanced shares

File Ownership and Map Drives

Mapping a drive creates a shortcut to a physical location on a different computer, which users can access over a shared network. A mapped drive allows multiple people to view and edit the same files.

When a file is moved or copied between file systems, it inherits permissions from the destination folder. The most restrictive permission takes precedence over any other permissions that have been set.

Purpose

Upon completing this project, you will better understand how to use a mapped drive and the effects of moving objects between file systems.

Steps for Completion

1. Before a mapped drive can be used or created, a user must turn on _____.
2. How would moving a file from the C drive to a mapped drive affect the file's permissions?

   _____

   _____
3. Open your Domain 3 Student folder and view the Advanced Security Settings for the document named **322.docx**.
4. Take a screenshot of the Advanced Security Settings window.
5. Save the screenshot as **322-Complete**.

Project Details

Project file
322.docx

Estimated completion time
5-10 minutes

Video reference
Domain 3
Topic: File Sharing and Permissions
Subtopic: Map Drives; Ownership of Files Between File Systems

Objectives covered
3 Data Access and Management
3.2 Describe and configure file sharing and permissions
3.2.5 Map drives
3.2.6 Identify the effect on permission of copying or moving data between file systems
3.2.7 Describe taking ownership of files or folders

Manage Backups

Backing up files creates a copy of files that a user can restore if their device breaks or the files are lost. Different types of backups are available depending upon a user's needs, and one can back up files to an external hard drive, a flash drive, or a network location.

Purpose

Upon completing this project, you will better understand the different backup types available and how to use backup and restore to protect important files.

Steps for Completion

A.	Full backup
B.	Mirror backup
C.	Differential backup
D.	Incremental backup

1. Match each type of backup with its description.
   a. _____ Automatically creates copies of data as it changes on a hard drive.
   b. _____ Only backs up data that has changed since the most recent backup.
   c. _____ Makes one or more copies of selected data on a hard drive.
   d. _____ Only backs up data that has changed or been created since the initial full backup.
2. Why is it important to regularly back up important files?

   _____

   _____

   _____
3. If you have a flash drive or external hard drive available, create a backup of your Domain 3 Student folder.

Project Details

Project file
N/A

Estimated completion time
5-10 minutes

Video reference
Domain 3
Topic: Manage Backup and Restore
Subtopic: File Backup Types and Restore Operations

Objectives covered
3 Data Access and Management
3.3 Manage backup and restore
3.3.1 Describe backup types
3.3.2 Perform full backup and restore operations
3.3.3 Restore previous versions

Data Policies

Data access and retention policies help users and organizations safely retain, remove, and protect their own data. Data owners have both possession of and responsibility for their data and determine others' access to that data. Documents such as memorandums of understanding and Acceptable Use Policies can help create and define these policies.

Purpose

Upon completing this project, you will better understand the terms used in data ownership and some of the tools available for protecting data.

Steps for Completion

1. Determine whether the following statements are True or False:
   a. _____ A memorandum of understanding is legally binding.
   b. _____ An Acceptable Use Policy should include specific rules regarding user access to a corporate network.
   c. _____ Data owners determine who can modify, sell, or remove that data.
   d. _____ A remote wipe sends data to an employee's device.
2. What is a data retention policy?

_____
_____
_____
_____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 3
Topic: Data Access and Retention Policies
Subtopic: Types of Retention and Data Access Policies

Objectives covered
3 Data Access and Management
3.4 Describe data access and retention policies
3.4.1 Memorandums of understanding
3.4.2 Acceptable Use Policies (AUPs)
3.4.3 Ownership of and access to data and history
3.4.4 Use of remote wipe

Domain 4
Lesson 1

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 4 Lesson 1, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. A firewall is a gatekeeper between a(n) _____ and the outside world. [Firewall Settings and Network Types]
2. Depending on the level of security one wants for a network, one can block all incoming connections, including those in the list of allowed _____. [Firewall Settings and Network Types]
3. One of the most common forms of user authentication is a username and _____. [Types of Authentication]
4. _____ authentication helps to provide additional security to an account by requiring two or more credentials to be entered when signing in. [Types of Authentication]
5. Bring-your-own-device (BYOD) mobile devices are most common among _____ businesses that ask their employees to supply their devices to work from or make phone calls. [Passwords for BYOD and Corporate Devices]
6. Whether the company utilizes bring-your-own-device (BYOD) or corporate-managed devices, it must create a strong _____ policy to protect devices against unauthorized users gaining access to technology or data. [Passwords for BYOD and Corporate Devices]
7. A virus must be attached to a(n) _____ to spread. [Mitigating Attacks]
8. _____ software is best used to protect against common online threats such as viruses, worms, and trojan horses. [Mitigating Attacks]

LearnKey

Firewall Settings

A firewall is the first line of defense in a network's security, and it monitors and blocks any malicious and unwanted incoming traffic. To best use a built-in firewall available on Windows and macOS operating systems, one should understand the firewall's settings.

Purpose

Upon completing this project, you will better understand network firewall settings.

Steps for Completion

1. List three malicious activities built-in firewalls on Windows and macOS operating systems help prevent. _____
   _____
   _____

2. Match the network type to its description.

A. Private	B. Public	C. Guest

   a. _____ Grant access to Wi-Fi without giving access to shared resources

   b. _____ Trusted network with restricted access that allows the computer to be discoverable and use network resources

   c. _____ Sets the computer to be undiscoverable and limits access to network resources

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
Topic: Describe Network Firewall Settings
Subtopic: Firewall Settings and Network Types

Objectives covered
4 Device Security
4.1 Describe network firewall settings
4.1.1 Why and how to disable or enable Windows Defender Firewall
4.1.2 Compare and contrast private, public, and guest networks

LearnKey

User Authentication and BOYD

User authentication is a common process that occurs when using a device. Understanding the different user authentication methods available to administrators can help them decide which methods to use to keep corporate-owned and bring-your-own-devices (BYODs) secure.

Purpose

Upon completing this project, you will better understand user authentication and BYOD password requirements.

Steps for Completion

1. What is user authentication?
   a. _____
2. What is a smart card?
   a. _____
3. List two examples of biometric authentication. _____
4. List the three authentication factors. _____
5. Strong password policies should include passwords with at least _____ characters.
6. What four types of characters should be required for passwords?
   a. _____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: Describe User Authentication
Subtopic: Types of Authentication; Passwords for BYOD and Corporate Devices

Objectives covered
4 Device Security
4.2 Describe user authentication
4.2.1 Multifactor authentication
4.2.2 Smart cards
4.2.3 Biometric authentication methods
4.2.4 Secure password requirements for BYOD mobile devices and corporate-managed devices

LK LearnKey

Attacks and Mitigation Methods

Attacks can frequently occur on devices and can result in data being stolen or altered. To prevent successful attacks, users should understand the different types of attacks that can affect a device.

Purpose

Upon completing this project, you will better understand common attacks and how to prevent them.

Steps for Completion

1. Match the attack to its description.

A. Virus	D. Trojan horse	G. Ransomware	J. Vishing
B. Worm	E. Keylogger	H. Phishing	K. Adware
C. Spyware	F. Physical attack	I. Social engineering	

   a. _____ A socially engineered attack where victims are tricked into revealing sensitive information or are provided with a malicious link

   b. _____ Software that can secretly track a user's computer use and collect data about the user and their activity on the computer and sends the information it collects to a third party

   c. _____ A malicious attack where individuals are tricked into providing confidential information, commonly done through vishing

   d. _____ An individual steals valuable equipment or data or harms another individual

   e. _____ Malicious code that can copy itself to a device and other devices to interrupt, damage, and steal data and can replicate and spread across devices within a network without being attached to a program

   f. _____ Software that causes pop-up windows to appear with advertisements and, once on a device, copies personal information and transmits credit card numbers, passwords, and other sensitive information

   g. _____ Systematically encrypts the computer's hard drive and locks legitimate users out of their sensitive data

   h. _____ Malicious code that can copy itself to a device and other devices to interrupt, damage, and steal data and must be attached to a program to spread

   i. _____ A program that looks legitimate but is a type of malware that a user must execute

   j. _____ Captures every keystroke, including the keystrokes used to sign in to personal accounts

   k. _____ A social engineering attack performed through voice interactions, usually over the phone

Project Details

Project file
N/A

Estimated completion time
15 minutes

Video reference
Domain 4
Topic: Attack Mitigation Methods
Subtopic: Mitigating Attacks

Objectives covered
4 Device Security
4.3 Given an attack type, describe mitigation methods
4.3.1 Methods of mitigating attacks (computer viruses, worms, trojan horses, spyware, adware, ransomware, phishing, keyloggers, social engineering attacks, and physical attacks)
4.3.2 Antivirus and antimalware program configuration options
4.3.3 Analyze antivirus and antimalware program results
4.3.4 Social engineering training

Notes for the teacher
If time permits, you may choose to demonstrate to students how they can scan for threats on a Windows device.

2. Label each statement as True or False.

    a. _____ Two ways to lower a device's risk of incurring a virus or malware are only visiting websites with an HTTPS address and enabling Windows Defender on Windows devices.

    b. _____ One way to prevent physical attacks is to ensure firewalls are enabled on all devices.

Domain 4
Lesson 2

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 4 Lesson 2, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. User Account Control (UAC) is a security feature that protects a computer from potentially harmful changes made by _____, users, viruses, and malware. [User Account Control]
2. To enable or disable User Account Controls, _____ the control, select either Enabled or Disabled, and then select Apply. [Elevate Permissions]
3. In the case of a lost or stolen device, as part of mobile device management (MDM), the agent or _____ can take control of the device. [Mobile Device Management and Installation]
4. Microsoft _____ and other applications can be used to connect mobile devices to corporate networks. [Mobile Device Connection to a Corporate Network]
5. Users can increase mobile device security by implementing a(n) _____. [Securing and Transporting Mobile Devices]

LearnKey

UAC Settings

User Account Control (UAC) is a security feature that protects a computer from potentially harmful changes made by applications, users, viruses, and malware. Understanding UAC settings and how to elevate permissions allow a user to decide which setting is best for their needs.

Purpose

Upon completing this project, you will better understand UAC settings.

Steps for Completion

1. Match the UAC setting to its description.

A. Always notify	C. Notify me only when apps try to make changes to my computer (do not dim my desktop)
B. Notify me only when apps try to make changes to my computer (default)	D. Never notify

   a. _____ The user will be able to perform other tasks on the computer while the message box is open. No changes will be made to the computer until the user has responded to the message box.

   b. _____ There are no restrictions, and changes can be made freely.

   c. _____ The message box will appear and require a response before continuing forward with the change, but only when applications are making the change.

   d. _____ No action will take place until the administrator responds to the message box, and the user will not be able to continue performing tasks on the computer until they respond. Standard users are assigned this setting by default.

2. Match the UAC setting to its recommended use.

A. Always notify	C. Notify me only when apps try to make changes to my computer (do not dim my desktop)
B. Notify me only when apps try to make changes to my computer (default)	D. Never notify

   a. _____ This setting level is recommended if a user routinely installs new software and visits unfamiliar websites.

   b. _____ This setting is not recommended.

   c. _____ This setting is only recommended if it takes a long time for the user's computer to dim.

   d. _____ This setting is recommended if a user routinely installs new software or visits many unfamiliar websites but does not want to be notified when they are the one making changes to Windows settings.

3. When deploying a policy to a domain computer, the user will need to use the _____.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 4
Topic: UAC Settings
Subtopic: User Account Control; Elevate Permissions

Objectives covered
4 Device Security
4.4 Manage User Account Control (UAC) settings
4.4.1 Describe the function of UAC
4.4.2 Identify appropriate UAC settings for specific purposes
4.4.3 Elevate permissions in UAC

Mobile Device Management

Mobile device management (MDM) enables organizations to protect themselves against device and data theft. MDM allows an organization to control devices covered by an MDM policy.

Purpose

Upon completing this project, you will better understand MDM.

Steps for Completion

1. Label each statement as True or False.

    a. _____ MDM software must be installed directly from the MDM server.

    b. _____ An MDM application cannot communicate with a device properly unless the device has been enrolled with the MDM.

    c. _____ A group that is part of a company network allows specific access controls to be set and administrators to monitor the device's use.

    d. _____ Most companies do not require that their employees have a lock on their corporate mobile devices or personal mobile devices if used for work.

    e. _____ Strong passwords should be at least four characters long.

2. List three types of locks that can be used on a device.

    _____

    _____

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 4
- **Topic**: Manage Mobile Device Security
    - **Subtopic**: Mobile Device Management and Installation; Mobile Device Connection to a Corporate Network; Securing and Transporting Mobile Devices

Objectives covered
4 Device Security
- **4.5** Manage mobile device security
    - **4.5.1** Mobile device management (MDM)
    - **4.5.2** Methods of securing mobile devices
    - **4.5.3** Installing agents on devices
    - **4.5.4** Connect mobile devices to corporate networks
    - **4.5.5** Limitations on transporting corporate devices

Domain 5
Lesson 1

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 5 Lesson 1, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. Windows has troubleshooting tools that can be used to determine possible _____ for device issues. [Windows Troubleshooting Tools]
2. In many cases, users will need to do their own _____ about how to remedy a device issue. [Gather Data and Remedy Issues]
3. Local policies apply just to the device they were _____ on, while Group Policies are applied to more than one computer in a domain. [Local and Group Policies and Precedence]
4. A(n) _____ unit group allows the administrator to place different users, groups, and computers into subdivisions within Active Directory. [Local and Group Policies and Precedence]
5. A(n) _____ Group Policy usually takes precedence over any local policy because of the order in which they are processed. [Update Policies and Recognize Applied Policy]
6. Resetting the computer allows users to _____ applications that have been installed on the system. [Reset or Roll Back the Operating System]
7. When using the _____ startup method, Windows creates a special file that logs and generates a list of drivers used during each step of the startup process. [Advanced Startup, Retention, and Safe Mode]
8. Safe Mode is a Windows startup method used to start a computer in basic mode with _____ files and drivers. [Advanced Startup, Retention, and Safe Mode]
9. Compatibility issues occur when users try to run _____ apps on a newer version of an operating system. [App Compatibility and Installation Issues]
10. After uninstalling an application, it is wise to _____ the computer to remove any leftover files. [Reinstall or Repair Desktop Applications]

LearnKey

Troubleshooting Tools

Troubleshooting is determining the cause and solution for an issue with a device. Windows troubleshooting tools can help find the problem area and sometimes resolve the issue. If troubleshooting tools do not help, the user may need to do additional research. Often, Microsoft offers online resources to troubleshoot issues on Windows computers.

Purpose

Upon completing this project, you will better understand the tools and resources available for troubleshooting Windows devices.

Steps for Completion

1. Navigate to the Additional troubleshooters page on your device. List four troubleshooters available on this page.

   _____
   _____
   _____

2. What is the next step if Windows troubleshooters do not fix an issue?

   _____
   _____
   _____

3. Browse Microsoft's support website, support.microsoft.com. Read two troubleshooting articles on a subject of your choice.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 5
- **Topic**: Perform Troubleshooting Tasks
  - **Subtopic**: Windows Troubleshooting Tools; Gather Data and Remedy Issues

Objectives covered
5 Troubleshooting
- **5.1** Perform troubleshooting tasks
  - **5.1.1** Locate and identify Windows troubleshooting tools
  - **5.1.2** Gather data to describe issues and support troubleshooting
  - **5.1.3** Research how to remedy issues

LearnKey

Group Security Policies

An administrator can set and check security policies both locally and within groups. Local policies apply to the individual computer they were created on, while Group Policies apply to more than one computer in a domain. Administrators can set Group Policies within Active Directory. Active Directory applies Group Policies in a specific order, with a device's local policy being applied first. Group Policies will usually take precedence over local policies. Windows will update policies automatically, or users can update them immediately from the command prompt.

Purpose

Upon completing this project, you will better understand group security policies and how Active Directory applies them to a device.

Steps for Completion

A.	Site Group Policy
B.	Organizational unit group
C.	Local policy
D.	Domain policy

1. Match each policy type to its description.

   a. _____ Establishes security settings for users and computers, such as password policies.

   b. _____ Only applies to the individual computer it was created on.

   c. _____ Allows administrators to control the working environments of computers and user accounts in Active Directory.

   d. _____ Allows administrators to place different users, groups, and computers into subdivisions within Active Directory.

2. Label each command prompt with its definition.

   e. gpupdate: _____

   f. gpresult: _____

3. List the order in which Active Directory applies Group Policies.

   _____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 5
- **Topic**: Perform Troubleshooting Tasks
  - **Subtopic**: Local and Group Policies and Precedence; Update Policies and Recognize Applied Policy

Objectives covered
5 Troubleshooting
- **5.1** Perform troubleshooting tasks
  - **5.1.5** Update Group Policies in a Windows domain
  - **5.1.6** Differentiate between local and group security policies and precedence
  - **5.1.7** Recognize that a policy has been applied or could cause a problem

Operating System Issues

When troubleshooting an operating system, one option is to reset the computer. Two choices are available when resetting. A user can either keep their files or remove everything on the computer before reinstalling Windows. Another option is to go back to a previous version of the operating system, known as a rollback.

Under Advanced options, users can try additional startup options to troubleshoot. These settings included boot logging and a few different types of Safe Modes.

Purpose

Upon completing this project, you will better understand the options for resetting an operating system and options available for Advanced Startup.

Steps for Completion

1. Why would a user want to remove all files as part of a reset?

   _____
   _____
   _____

2. During the _____ startup method, Windows generates a list of drivers used during each step of the process.

3. Match each Safe Mode description with its name.

   A. Safe Mode
   B. Safe Mode with Command Prompt
   C. Safe Mode with Networking

   a. _____ Only loads the drivers required to connect to other computers during startup.

   b. _____ A basic mode with limited files and drivers.

   c. _____ A limited number of drivers are used, there is no networking, and the desktop is not loaded.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 5
Topic: Troubleshoot Operating System and Application Issues
Subtopic: Reset or Roll Back the Operating System; Advanced Startup, Retention, and Safe Mode

Objectives covered
5 Troubleshooting
5.2 Troubleshoot operating system and application issues
5.2.1 Reset or roll back the operating system
5.2.2 Advanced startup
5.2.3 File and setting retention options
5.2.4 Features of Safe Mode

Troubleshooting Applications

If an application has an issue, it could be caused by a compatibility issue or the app needing an update. Users can download updates to apps from the Microsoft Store, and compatibility issues often occur following Windows operating system updates. If issues persist after a user rules out updates and compatibility, they can run the Microsoft Store Apps troubleshooter. Finally, a user can try uninstalling and reinstalling the application.

Purpose

Upon completing this project, you will better understand the options available for troubleshooting application issues.

Steps for Completion

1. Open the Microsoft Store and check for updates.
2. Take a screenshot of the Microsoft Store page that shows Updates and Downloads.
3. Save the screenshot as **525-Complete** in your Domain 5 Student folder.
4. Operating system updates can cause issues for older apps using old _____.
5. After uninstalling an application, one should _____ the computer to remove any leftover files.
6. What two options are available for apps under Troubleshoot compatibility?

_____

Project Details

Project file
N/A

Estimated completion time
5-10 minutes

Video reference
Domain 5
- **Topic**: Troubleshoot Operating System and Application Issues
  - **Subtopic**: App Compatibility and Installation Issues; Reinstall or Repair Desktop Applications

Objectives covered
5 Troubleshooting
- **5.2** Troubleshoot operating system and application issues
  - **5.2.5** Use troubleshooting tools to identify application compatibility issues
  - **5.2.6** Resolve Store app installation issues
  - **5.2.7** Reinstall or repair desktop applications

Domain 5
Lesson 2

Device Configuration and Management

LK LearnKey

Fill-in-the-Blanks

Instructions: While watching Domain 5 Lesson 2, fill in the missing words according to the information presented by the instructor. [References are found in the brackets.]

1. Device Manager displays all the _____ installed on the computer and allows users to view and manage devices and drivers. [Hardware Troubleshooting and Device Manager]
2. After a(n) _____ or operating system update, drivers also need to be updated. [Update or Roll Back Drivers]
3. Uninstalling a device removes the _____ from the user's USB hardware. [Uninstall or Reinstall a Device]
4. Devices with _____ addresses cannot connect to a network properly. [Wired and Wireless Connections]
5. A failed domain connection is caused by a PC not being on the same _____ as the domain controller or a PC being blocked by the domain controller. [Joining Devices to Domains]
6. If a device has a red exclamation point next to it in Device Manager, there is a(n) _____ error for that device. [Peripheral Device Connections]
7. If there are too many devices drawing power from a(n) _____ port, a computer may have a hard time trying to detect a device connection. [Peripheral Device Connections]

Troubleshooting Drivers

When there is an issue with device hardware, the first things a user should check are the connections to ports and power. If the device is properly connected, there may be an issue with a driver. Device Manager will display all the hardware installed on a computer and what drivers that hardware is using. Drivers may need to be updated or rolled back to a previous version. Sometimes, uninstalling and reinstalling a device will fix the issue.

Purpose

Upon completing this project, you will better understand how to troubleshoot device hardware and drivers.

Steps for Completion

1. Open Device Manager on your computer.
2. Take a screenshot of the Device Manager window.
3. Save the screenshot as **534-Complete** in your Domain 5 Student folder.
4. What are drivers?

   _____

   _____
5. After a(n) _____ or operating system update, drivers also need to be updated.
6. When troubleshooting device issues, the first cause to rule out is a proper connection to _____.
7. Uninstalling a device _____ that driver from a user's USB hardware and allows for a clean installation of the driver.

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 5
- **Topic**: Troubleshoot Device Issues
  - **Subtopic**: Hardware Troubleshooting and Device Manager; Update or Roll Back Drivers; Uninstall or Reinstall a Device

Objectives covered
5 Troubleshooting
- **5.3** Troubleshoot device issues
  - **5.3.1** Hardware troubleshooting methods (connections, ports, and power)
  - **5.3.2** Update or roll back drivers
  - **5.3.3** Uninstall or reinstall a device to reconfigure drivers
  - **5.3.4** Describe the purpose and capabilities of Device Manager

LearnKey

Troubleshooting Device Connections

Connections are made either wirelessly or through a physical wired connection. If a device does not have a connection, one should start by checking the physical cable to ensure that it is connected. If the connection is wireless, one should ensure that the device is receiving a signal. Beyond simple solutions to troubleshoot connections, users should know how to troubleshoot connections to keep their devices functioning.

Purpose

Upon completing this project, you will better understand how to troubleshoot connections.

Steps for Completion

1. Label each statement as True or False.
    a. _____ Automatic Private IP Addressing (APIPA) addresses cannot connect to a network properly.
    b. _____ APIPA addresses can result in system failure.
    c. _____ If all devices on a network have an APIPA address, then the network is out.
    d. _____ A network's IP address must match the device's IP address.
2. What three problems could an APIPA address indicate?
    a. _____
3. What are the three common causes of a failed domain connection?
    a. _____

Project Details

Project file
N/A

Estimated completion time
10 minutes

Video reference
Domain 5
Topic: Troubleshoot Device Connections to Networks and Domains
Subtopic: Wires and Wireless Connections; Joining Devices to Domains

Objectives covered
5 Troubleshooting
5.4 Troubleshoot device connections to networks and domains
5.4.1 Wired and wireless connections (physical cable, signal, APIPA)
5.4.2 Joining devices to domains

Troubleshooting Peripheral Devices

Peripheral devices are commonly used with computers, and they are auxiliary devices that connect to and work with a computer. Users should know how to troubleshoot peripheral devices to ensure connected devices are functioning as expected.

Purpose

Upon completing this project, you will better understand how to troubleshoot peripheral device connections.

Steps for Completion

1. List four examples of peripheral devices. _____
2. If unplugging a wireless device and plugging it back in does not fix a connection issue, one should consider changing the _____.
3. Where should a user go to install or update drivers for a peripheral device? _____
4. List three ways to troubleshoot a peripheral device connection.

Project Details

Project file
N/A

Estimated completion time
5 minutes

Video reference
Domain 5
- **Topic**: Troubleshoot Peripheral Device Connections
  - **Subtopic**: Peripheral Device Connections

Objectives covered
5 Troubleshooting
- **5.5** Troubleshoot peripheral device connections
  - **5.5.1** Keyboard
  - **5.5.2** Mouse
  - **5.5.3** Display
  - **5.5.4** Headset
  - **5.5.5** Microphone
  - **5.5.6** Camera
  - **5.5.7** Local and network storage devices
  - **5.5.8** Printers
  - **5.5.9** Scanners
  - **5.5.10** Drivers
  - **5.5.11** Connection cables

Notes for the teacher
If time permits, you may choose to show students how to check a device's drivers in Device Manager.

Appendix

Device Configuration and Management

LK LearnKey

Glossary

Term	Definition
Acceptable Use Policies	A document that states constraints and practices that users must agree to follow to have access to a corporate network.
Active Directory	A Windows general-purpose directory that stores network objectives such as users, accounts, and resources.
Administrator	An individual that has the highest level of control and access on a computer and can make changes that affect other users of that computer.
Adware	Software that displays or downloads advertising material like pop-up ads.
Antimalware Software	A type of security software used to detect, remove, and prevent malware attacks on a computer. Antimalware is used to detect advanced forms of malware.
Antivirus Software	A type of security software used to detect and remove traditional computer viruses.
APIPA	Automatic Private IP Addressing (APIPA) is a Windows function that provides a DHCP fail-safe autoconfiguration address that protects the computer from system failure.
Authentication	Any process a system uses to verify a user's identity.
Azure Remote App	An application that can be used to connect mobile devices to a corporate network.
Biometrics	Any physical or behavioral characteristics used to identify a person—examples of biometrics include fingerprints, retinal scans, voice readers, and facial recognition.
Boot Logging	A computer startup method where Windows creates a special file that logs the list of drivers that are used during the startup process.
BYOD	Bring your own device (BYOD) is a company practice that allows employees to bring and use their personal computers, phones, and other devices at work.
Cloud Storage	A method used to store data. Data is kept in remote servers and then accessed through the internet.
Command Prompt	A Windows application that allows users to input data in a text-based interface to execute commands.
Computer Virus	A program or malicious code that runs on a computer without the user's knowledge. A computer virus copies itself to other devices with the purpose of damaging the device and/or stealing data.
Control Panel	A part of the Microsoft graphical user interface used to view and manage basic computer settings.
Custom Install	A type of installation that allows administrators to determine the components they want to install and where they want them stored.
Differential Backup	A backup type that only backs up data that has changed or been created since the initial full backup.
DisplayPort	A port commonly found on a PC that provides high-definition video and audio between a computer and monitor.
Driver	A software component that allows the operating system and a device to communicate with each other.
File Sharing	A method used to transmit files from one computer to another or via a network or the internet.
Firewall	A network security system that controls incoming and outgoing network traffic.
Full backup	Making one or more copies of selected data on a hard drive.
Group Policies	An infrastructure that allows network administrators to implement security policy settings for users and computers.
HDMI	High-definition multimedia interface (HDMI) is a standard for connecting and transmitting high-definition digital video and audio to the computer from another source.
Incremental Backup	A backup type that backs up data that has changed from the last backup.

Term	Definition
Keyloggers	A type of spyware where a hacker captures keyboard keystrokes, including the keystrokes used to sign in to accounts.
Last Known Good Configuration	A boot-up option where Windows can be started if it is not starting normally. The drivers that successfully worked the last time Windows was started and shut down will be used to start the operating system.
Local Account	An account that exists on a single computer.
Malware	Malicious software, including viruses, ransomware, and spyware.
Memorandum of Understanding	A document outlining an agreement between parties.
Microsoft Account	A single sign-on web service that allows users to synchronize devices, websites, and applications using one account.
Microsoft Azure	A Microsoft cloud computing platform used to build, deploy, and manage applications.
Microsoft Intune	A cloud-based desktop management tool that allows organizations to provide employees with access to corporate resources.
Microsoft Store	A digital storefront that offers applications, games, and music to Windows users. Some content is free, and others cost money to download.
Mirror Backup	A backup that automatically creates copies of the data as it changes on the drive.
Mobile Device Management	A type of software that allows companies to control, secure, and automate policies on devices connected to the organization's network.
Multifactor Authentication	An authentication process that uses two or more forms of distinct authentication factors to authenticate the user.
NTFS	New Technology File System (NTFS) is a Windows file system that organizes, stores, and finds files on the hard disk.
OneDrive	A Microsoft cloud-based file storage service used to store and share files.
Patches	A set of changes made to software and operating systems that provide an update that improves security and performance within a program or product.
Permissions	The ability for a user to access a resource.
Physical Attack	An attack where an individual steals valuable equipment or data or physically harms another individual.
PIN Lock	A screen lock security method used to protect a device from unauthorized access. The PIN code must be entered any time the device is turned on to unlock it.
Ransomware	A form of malware where malicious code is installed on a computer and the legitimate user is locked out of their sensitive data.
Remote Wipe	A security feature for mobile devices that allows users to erase data remotely from a mobile device.
Retention Policy	A policy that determines what data is stored and archived on a computer along with how long that data is stored and what happens to the data after the retention period is over.
Roll Back	An operation that takes an operating system back to the previous version.
Safe Mode	A Windows boot option that starts the computer in a basic mode with limited files and drivers.
Safe Mode with Networking	A Windows boot method that only loads the minimum amount of drivers required to connect the computer to other computers.
Smart Card	A card with a microprocessor chip inside used as an authentication security token.
Social Engineering Attack	A type of malicious attack where individuals are tricked into providing confidential info.
Spyware	A type of malicious software designed to allow an individual to collect information about another user's computer activities.
Start Menu	An interface tool used in Windows environments. It is used as the main launching point for computer applications and programs.

Term	Definition
Taskbar	A bar provided on a Windows display that allows users quick access to applications in use and pinned to the taskbar.
Time Zone	A time assigned to a geographical region.
Trojan Horse	A type of malware that is not self-replicating. It presents a program that appears to be legitimate and harmless to trick users into clicking and launching the trojan horse.
Troubleshoot	The process of locating and isolating a problem in a program, computer system, or network and resolving it.
USB	Universal serial bus (USB) is an external interface that connects peripheral devices to a computer.
USB-C	A type of USB connector used to connect devices like mobile devices and game consoles.
User Account Control	A Windows feature that sets user authentication levels that require the computer administrator to allow some or all changes made to Windows system settings.
VGA	A video graphics array (VGA) is an analog connection used to link a computer to a projector or additional monitors.
Virtual Machine	A virtual environment that is created on a computer using software that emulates a separate computer.
Vishing	A social engineering attack where individuals make phone calls or leave voice messages to try and trick companies or individuals into revealing personal information.
Windows Safe Mode with Command Prompt	A method of Safe Mode that boots a computer with a limited amount of drivers and files, providing the user with access to a limited version of Windows.
Windows Troubleshooting Tools	A Windows built-in troubleshooter.
Windows Update	A Microsoft service that updates and fixes known flaws in Microsoft applications and the operating systems.
Worm	Malware that replicates and spreads itself across devices within a network.

Keyboard Shortcuts for Device Configuration and Management

Action	Shortcut
Display the Start menu	Ctrl+Esc
Launch the Settings menu	Windows+I
Lock computer	Windows+L
Open File Explorer	Windows+E
Open Task Manager window	Ctrl+Alt+Delete
Open the Run command	Windows+R

LearnKey

Objectives

Device Configuration and Management Objectives				
Domain 1 Windows Installation and Configuration	**Domain 2 Application and Peripheral Management**	**Domain 3 Data Access and Management**	**Domain 4 Device Security**	**Domain 5 Troubleshooting**
1.1 Install Windows using the default settings 1.1.1 Time zone options 1.1.2 Microsoft account vs. local account 1.1.3 Upgrade vs. custom install	2.1 Manage applications and Windows features 2.1.1 Identify user account requirements and permissions for application installation 2.1.2 Modify application installations 2.1.3 Remove desktop applications 2.1.4 Locate and identify optional Windows features 2.1.5 Describe the purpose of the Microsoft Store	3.1 Describe cloud services 3.1.1 Cloud storage and collaboration concepts 3.1.2 Common cloud storage providers 3.1.3 File sharing capabilities and permissions 3.1.4 Capabilities of local and hosted virtual machines 3.1.5 Offline file synchronization	4.1 Describe network firewall settings 4.1.1 Why and how to disable or enable Windows Defender Firewall 4.1.2 Compare and contrast private, public, and guest networks	5.1 Perform troubleshooting tasks 5.1.1 Locate and identify Windows troubleshooting tools 5.1.2 Gather data to describe issues and support troubleshooting 5.1.3 Research how to remedy issues 5.1.4 Identify when to escalate issues 5.1.5 Update Group Policies in a Windows domain (gpupdate /force, gpresult) 5.1.6 Differentiate between local and group security policies and precedence 5.1.7 Recognize that a policy has been applied or could cause a problem
1.2 Configure user account options 1.2.1 User account (cloud or local) 1.2.2 Local user and administrative account types	2.2 Compare and contrast capabilities of peripheral connection types 2.2.1 HDMI 2.2.2 DisplayPort 2.2.3 VGA 2.2.4 Mini-HDMI 2.2.5 USB 2.2.6 USB-C 2.2.7 Converting between connection types	3.2 Describe and configure file sharing and permissions 3.2.1 File and share permissions 3.2.2 Effective permissions 3.2.3 Basic and advanced permissions 3.2.4 Public, basic, and advanced shares 3.2.5 Map drives 3.2.6 Identify the effect on permissions of copying or moving data between file systems 3.2.7 Describe taking ownership of files or folders	4.2 Describe user authentication 4.2.1 Multifactor authentication 4.2.2 Smart cards 4.2.3 Biometric authentication methods 4.2.4 Secure password requirements for BYOD mobile devices and corporate-managed devices	5.2 Troubleshoot operating system and application issues 5.2.1 Reset or roll back the operating system 5.2.2 Advanced startup 5.2.3 File and setting retention options 5.2.4 Features of Safe Mode 5.2.5 Use troubleshooting tools to identify application compatibility issues 5.2.6 Resolve Store app installation issues 5.2.7 Reinstall or repair desktop applications
1.3 Configure desktop settings 1.3.1 Start menu 1.3.2 Display settings 1.3.3 Application shortcuts		3.3 Manage backup and restore 3.1.1 Describe backup types 3.3.2 Perform full backup and restore	4.3 Given an attack type, describe mitigation methods 4.3.1 Methods of mitigating attacks (computer viruses, worms, trojan horses, spyware, adware, ransomware, phishing,	5.3 Troubleshoot device issues 5.3.1 Hardware troubleshooting methods (connections, ports, power) 5.3.2 Update or roll back

Device Configuration and Management Objectives				
Domain 1 Windows Installation and Configuration	**Domain 2 Application and Peripheral Management**	**Domain 3 Data Access and Management**	**Domain 4 Device Security**	**Domain 5 Troubleshooting**
1.3.4 Time zone settings 1.3.5 Taskbar settings 1.3.6 Power settings 1.3.7 Window management (minimize, close, snap)		operations 3.3.3 Restore previous versions	keyloggers, social engineering attacks, and physical attacks) 4.3.2 Antivirus and antimalware program configuration options 4.3.3 Analyze antivirus and antimalware program results 4.3.4 Social engineering training	drivers 5.3.3 Uninstall or reinstall a device to reconfigure drivers 5.3.4 Describe the purpose and capabilities of Device Manager
1.4 Manage accessibility settings 1.4.1 Display settings 1.4.2 Mouse settings 1.4.3 Color filters 1.4.4 High-contrast settings 1.4.5 Audio settings 1.4.6 Closed captions 1.4.7 Speech Recognition 1.4.8 Magnifier 1.4.9 Narrator 1.4.10 Sticky Keys 1.4.11 On-Screen Keyboard		3.4 Describe data access and retention policies 3.4.1 Memorandums of understanding 3.4.2 Acceptable Use Policies (AUPs) 3.4.3 Ownership of and access to data and history 3.4.4 Use of remote wipe	4.4 Manage User Account Control (UAC) settings 4.4.1 Describe the function of UAC 4.4.2 Identify appropriate UAC settings for specific purposes 4.4.3 Elevate permissions in UAC	5.4 Troubleshoot device connections to networks and domains 5.4.1 Wired and wireless connections (physical cable, signal, APIPA) 5.4.2 Joining devices to domains
1.5 Manage updates 1.5.1 Windows update settings 1.5.2 Software updates and patches 1.5.3 Optional updates 1.5.4 Device driver updates 1.5.5 Update history			4.5 Manage mobile device security 4.5.1 Mobile device management (MDM) 4.5.2 Methods of securing mobile devices 4.5.3 Installing agents on devices 4.5.4 Connect mobile devices to corporate networks 4.5.5 Limitations on transporting corporate devices	5.5 Troubleshoot peripheral device connections 5.5.1 Keyboard 5.5.2 Mouse 5.5.3 Display 5.5.4 Headset 5.5.5 Microphone 5.5.6 Camera 5.5.7 Local and network storage devices 5.5.8 Printers 5.5.9 Scanners 5.5.10 Drivers 5.5.11 Connection Cables

Lesson Plan

Approximately 16 hours of video, labs, and projects

Device Configuration and Management

LearnKey

Domain 1 Lesson Plan

Domain 1 - Windows Installation and Configuration [approximately 4 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Pre-Assessment Assessment time - 00:30:00	Windows Installation and Configuration: Pre-Assessment			
Lesson 1 Video time - 00:18:20 Exercise Lab time - 00:16:00 Workbook time - 00:40:00	**Install Windows** How to Study Time Zone Options and Upgrade vs. Custom Install Microsoft Account vs. Custom Install **Configure User Account Options** Account Types **Configure Desktop Settings** Display and Time Zone Settings Start Menu Power Settings Taskbar Settings and App Shortcuts Windows Management	1.1 Install Windows using the default settings 1.1.1 Time zone options 1.1.2 Microsoft account vs. local account, 1.1.3 Upgrade vs. custom install 1.2 Configure user account options 1.2.1 User account (cloud or local) 1.2.2 Local user and administrative account types 1.3 Configure desktop settings 1.3.1 Start menu 1.3.2 Display settings 1.3.3 Application shortcuts 1.3.4 Time zone settings 1.3.5 Taskbar settings 1.3.6 Power settings 1.3.7 Window management (minimize, close, snap)	Add User Time Zone Start Menu Taskbar Personalization	Install Windows – pg. 9 N/A User Accounts – pg. 10 N/A Display Settings – pg. 11 N/A Start Menu – pg. 12 N/A Taskbar Settings and App Management – pg. 13 N/A
Lesson 2 Video time - 00:07:57 Exercise Lab time - 00:12:00 Workbook time - 00:35:00	**Manage Accessibility Settings** Display Settings and Mouse Settings Color Filters and High-Contrast Settings Audio Settings and Closed Captions Speech Recognition and Magnifier Sticky Keys and On-Screen Keyboard Narrator **Manage Updates** Windows Updates and Update History Patches, Optional, and Driver Updates	1.4 Manage accessibility settings 1.4.1 Display settings 1.4.2 Mouse settings 1.4.3 Color filters 1.4.4 High-contrast settings 1.4.5 Audio settings 1.4.6 Closed captions 1.4.7 Speech recognition 1.4.8 Magnifier 1.4.9 Narrator 1.4.10 Sticky Keys 1.4.11 On-screen keyboard 1.5 Manage updates 1.5.1 Windows update settings 1.5.2 Software updates and patches 1.5.3 Optional updates 1.5.4 Device driver updates 1.5.5 Update history	Color Filters Zoom Driver Update	Visual Accessibility – pg. 16 N/A Audio Accessibility – pg. 17 N/A Interface Accessibility – pg. 18 N/A Manage Updates – pg. 19 N/A
Post-Assessment Assessment time - 01:00:00	Windows Installation and Configuration: Post-Assessment			

LearnKey

Domain 2 Lesson Plan

Domain 2 - Application and Peripheral Management [approximately 2.5 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Pre-Assessment Assessment time - 00:30:00	Application and Peripheral Management: Pre-Assessment			
Lesson 1 Video time - 00:08:05 Exercise Lab time - 00:24:00 Workbook time - 00:30:00	**Manage Applications and Windows Features** Optional Windows Features and App Removal Microsoft Store Purpose and Modify App Installs User Account Requirements **Capabilities of Peripheral Connections** HDMI and Mini-HDMI DisplayPort VGA USB USB-C and Converting Between Connection Types	2.1 Manage applications and Windows features 2.1.1 Identify user account requirements and permissions for application installation 2.1.2 Modify application installations 2.1.3 Remove desktop applications 2.1.4 Locate and identify optional Windows features 2.1.5 Describe the purpose of the Microsoft Store 2.2 Compare and contrast capabilities of peripheral connection types 2.2.1 HDMI 2.2.2 DisplayPort 2.2.3 VGA 2.2.4 Mini-HDMI 2.2.5 USB 2.2.6 USB-C 2.2.7 Converting between connection types	App Uninstall Optional Features Storage Locations Connector Match Connector Types Port Types	Manage Applications – pg. 22 N/A Peripheral Connectors – pg. 23 N/A
Post-Assessment Assessment time - 01:00:00	Application and Peripheral Management: Post-Assessment			

LearnKey

Domain 3 Lesson Plan

Domain 3 - Data Access and Management [approximately 3 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Pre-Assessment Assessment time - 00:30:00	Data Access and Management: Pre-Assessment			
Lesson 1 Video time - 00:16:22 Exercise Lab time - 00:36:00 Workbook time - 00:50:00	**Describe Cloud Services** Cloud Storage Local and Hosted Virtual Machines **File Sharing and Permissions** File Sharing Permissions Effective Permissions and Share Types Map Drives Ownership of Files Between File Systems **Manage Backup and Restore** File Backup Types and Restore Operations **Data Access and Retention Policies** Types of Retention and Data Access Policies	3.1 Describe cloud services 3.1.1 Cloud storage and collaboration concepts 3.1.2 Common cloud storage providers 3.1.3 File sharing capabilities and permissions 3.1.4 Capabilities of local and hosted virtual machines 3.1.5 Offline file synchronization 3.2 Describe and configure file sharing and permissions 3.2.1 File and share permissions 3.2.2 Effective permissions 3.2.3 Basic and advanced permissions 3.2.4 Public, basic, and advanced shares 3.2.5 Map drives 3.2.6 Identify the effect on permissions of copying 3.3 Manage backup and restore 3.3.1 Describe backup types 3.3.2 Perform full backup and restore operations 3.3.3 Restore previous versions 3.4 Describe data access and retention policies 3.4.1 Memorandums of understanding 3.4.2 Acceptable Use Policies (AUPs) 3.4.3 Ownership of and access to data and history 3.4.4 Use of remote wipe	Offline Documents File Sharing Viewing Effective Access Public Folder Sharing Network Discovery Map Network Drive File Ownership Restore Backup Settings	Cloud Services – pg. 26 N/A File Shring Permissions – pg. 27 N/A File Ownership and Map Drives – pg. 28 322.docx Manage Backups – pg. 29 N/A Data Policies – pg. 30 N/A
Post-Assessment Assessment time - 01:00:00	Data Access and Management: Post-Assessment			

LearnKey

Domain 4 Lesson Plan

Domain 4 - Device Security [approximately 3 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Pre-Assessment Assessment time - 00:30:00	Device Security: Pre-Assessment			
Lesson 1 Video time - 00:12:25 Exercise Lab time - 00:08:00 Workbook time - 00:40:00	**Describe Network Firewall Settings** Firewall Settings and Network Types **Describe User Authentication** Types of Authentication Passwords for BYOD and Corporate Devices **Attack Mitigation Methods** Mitigating Attacks	4.1 Describe network firewall settings 4.1.1 Why and how to disable or enable Windows Defender Firewall 4.1.2 Compare and contrast private, public, and guest networks 4.2 Describe user authentication 4.2.1 Multifactor authentication 4.2.2 Smart cards 4.2.3 Biometric authentication methods 4.2.4 Secure password requirements for BYOD mobile devices and corporate-managed devices 4.3 Given an attack type, describe mitigation methods 4.3.1 Methods of mitigating attacks (computer viruses, worms, Trojan horses, spyware, adware, ransomware, phishing, keyloggers, social engineering attacks, and physical attacks) 4.3.2 Antivirus and antimalware program configuration options 4.3.3 Analyze antivirus and antimalware program results 4.3.4 Social engineering training	Firewall Virus Scan	Firewall Settings – pg. 33 N/A User Authentication and BYOD – pg. 34 N/A Attacks and Mitigation Methods – pg. 35 N/A
Lesson 2 Video time - 00:08:34 Exercise Lab time - 00:24:00 Workbook time - 00:20:00	**UAC Settings** User Account Control Elevate Permissions **Manage Mobile Device Security** Mobile Device Management and Installation Mobile Device Connection to a Corporate Network Securing and Transporting Mobile Devices	4.4 Manage User Account Control (UAC) settings 4.4.1 Describe the function of UAC 4.4.2 Identify appropriate UAC settings for specific purposes 4.4.3 Elevate permissions in UAC 4.5 Manage mobile device security 4.5.1 Mobile Device Management (MDM) 4.5.2 Methods of securing mobile devices 4.5.3 Installing agents on devices 4.5.4 Connect mobile devices to corporate networks 4.5.5 Limitations on transporting corporate devices	User Account Control Notification Settings Group Policy Management Console UIAccess Azure Network Security	UAC Settings – pg. 39 N/A Mobile Device Management – pg. 40 N/A
Post-Assessment Assessment time - 01:00:00	Device Security: Post-Assessment			

LearnKey

Domain 5 Lesson Plan

Domain 5 - Troubleshooting [approximately 3.5 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Pre-Assessment Assessment time - 00:30:00	Troubleshooting: Pre-Assessment			
Lesson 1 Video time - 00:14:52 Exercise Lab time - 00:24:00 Workbook time - 00:40:00	**Perform Troubleshooting Tasks** Windows Troubleshooting Tools Gather Data and Remedy Issues Local and Group Policies and Precedence Update Policies and Recognize Applied Policy **Troubleshoot Operating System and Application Issues** Reset or Roll Back the Operating System Advanced Startup, Retention, and Safe Mode App Compatibility and Installation Issues Reinstall or Repair Desktop Applications	5.1 Perform troubleshooting tasks 5.1.1 Locate and identify Windows troubleshooting tools 5.1.2 Gather data to describe issues and support troubleshooting 5.1.3 Research how to remedy issues 5.1.4 Identify when to escalate issues 5.1.5 Update group policies in a Windows domain (gpupdate /force, gpresult) 5.1.6 Differentiate between local and group security policies and precedence 5.1.7 Recognize that a policy has been applied or could cause a problem 5.2 Troubleshoot operating system and application issues 5.2.1 Reset or roll back the operating system 5.2.2 Advanced startup 5.2.3 File and setting retention options 5.2.4 Features of safe mode 5.2.5 Use troubleshooting tools to identify application compatibility issues 5.2.6 Resolve Store app installation issues 5.2.7 Reinstall or repair desktop applications	Troubleshoot Page Troubleshooting Printers Setting Policy App Updates App Compatibility Issues Windows Store Apps Troubleshooter	Troubleshooting Tools – pg. 43 N/A Group Security Policies – pg. 44 N/A Operating System Issues – pg. 45 N/A Troubleshooting Applications – pg. 46 N/A
Lesson 2 Video time - 00:10:12 Exercise Lab time - 00:04:00 Workbook time - 00:30:00	**Troubleshoot Device Issues** Hardware Troubleshooting and Device Manager Update or Roll Back Drivers Uninstall or Reinstall a Device **Troubleshoot Device Connections to Networks and Domains** Wires and Wireless Connections Joining Devices to Domains **Troubleshoot Peripheral**	5.3 Troubleshoot device issues 5.3.1 Hardware troubleshooting methods (connections, ports, power) 5.3.2 Update or roll back drivers 5.3.3 Uninstall or reinstall a device to reconfigure drivers 5.3.4 Describe the purpose and capabilities of Device Manager 5.4 Troubleshoot device connections to networks and domains 5.4.1 Wired and wireless	Viewing Drivers	Troubleshooting Drivers – pg. 49 N/A Troubleshooting Device Connections – pg. 50 N/A Troubleshooting Peripheral Devices – pg. 51 N/A

Domain 5 - Troubleshooting [approximately 3.5 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
	Device Connections Peripheral Device Connections	connections (physical cable, signal, APIPA) 5.4.2 Joining devices to domains 5.5 Troubleshoot peripheral device connections 5.5.1 Keyboard 5.5.2 Mouse 5.5.3 Display 5.5.4 Headset 5.5.5 Microphone 5.5.6 Camera 5.5.7 Local and network storage devices 5.5.8 Printers 5.5.9 Scanners 5.5.10 Drivers 5.5.11 Connection Cables		
Post-Assessment Assessment time - 01:00:00	Troubleshooting: Post-Assessment			