11.0 Managing Support Procedures

Support for customers and clients provides an interesting dynamic to working as an IT specialist. Every issue is something new to learn and resolve. While the issues change, the process by which we resolve them should not vary much issue to issue. Imagine you have been assigned to resolve an issue with an employee's laptop. This employee works remotely in another time zone, and you will need to rely on email and phone conversations to work through the troubleshooting steps. Ensuring that you communicate efficiently and effectively will be key to handling the issue as a professional.

As you work through the process, you will also need to ensure you are documenting the steps you have taken and the results of any test you have run. In some cases, the problem will not be resolved in the same day and other team members may need to continue to find a solution after your shift ends. Tracking and documentation of steps taken thus far allows them to continue the process rather than starting all over again with the issue. Understanding which application you are working with and ensuring the correct operating system has been identified will be helpful in finding a resolution as well.

Prepare for A+ Core 2 by:

- Understanding industry best practices in support documentation
- Understanding and use professional communication
- Identifying various operating systems and their uses

11.1.1 Standard Operating Procedure

Employees must understand how to use computers and networked services securely and safely and be aware of their responsibilities. To support this, the organization needs to create written policies and procedures to help staff understand and fulfill their tasks and follow best practices:

- A policy is an overall statement of intent.
- A **Standard Operating Procedure** (SOP) is a step-by-step list of the actions that must be completed for any given task to comply with policy. Most IT procedures should be governed by SOPs.
- Guidelines are for areas of policy where there are no procedures, either because the situation has not been fully assessed or because the decision-making process is too complex and subject to variables to be able to capture it in an SOP. Guidelines may also describe circumstances where it is appropriate to deviate from a specified procedure.

Typical examples of SOPs are as follows:

- Procedures for custom installation of software packages, such as verifying system requirements, validating download/installation source, confirming license validity, adding the software to change control/monitoring processes, and developing support/training documentation
- New-user setup checklist as part of the onboarding process for new employees and employees changing job roles. Typical tasks include identification/enrollment with secure credentials, allocation of devices, and allocation of permissions/assignment to security groups
- End-user termination checklist as part of the offboarding process for employees who are retiring, changing job roles, or have been fired. Typical tasks include returning and sanitizing devices, releasing software licenses, and disabling account permissions/access

11.1.2 Service Level Agreements

Service level agreements (SLAs) define the level of service requirements from an internal department or external, third-party vendor. Examples of services that most likely have an SLA in place include:

- Internal departments of the company that are providing resources to one another such as access to hardware resources; a company's maintenance department may also have a SLA that details how they are to provide support to the other departments within the company when it comes to building maintenance, etc.

- External agreements will normally be provided by the ISP as to the metrics of throughput they will provide a company for the internet connection; a cloud service provider will also have a SLA in place that details the service delivery metrics of the organizations cloud resources.

SLAs normally include a description of the service being provided, along with the metrics that are used to measure the level of service being provided. In some cases, the SLA may dictate the expected up time, when the service is available, and what is not considered down time (service not available) for the service. The Rule of Nines is a very popular metric used for this purpose.

Rule of 4 Nines means the service or system will be available 99.99% of the time. This allows for a maximum of 52 minutes of downtime per year. Whereas a service with the Rule of 11 Nines means the service will be up 99.999999999% of the time, would only be allowed 315.58 microseconds of downtime.

The Rule of Nines can also be used to calculate the durability of file and data storage services. The Rule of 11 Nines for durability means that even with 1 billion objects in storage, you would be able to go 100 years without losing a single object.

Should the delivery metrics not be met by the provider, the SLA will detail the recourse process to make a complaint against the service provider. It may also detail the amount of money the customer may be able to recover since the service is not meeting the requirements of the SLA.

11.1.3 Incident and Ticketing Systems

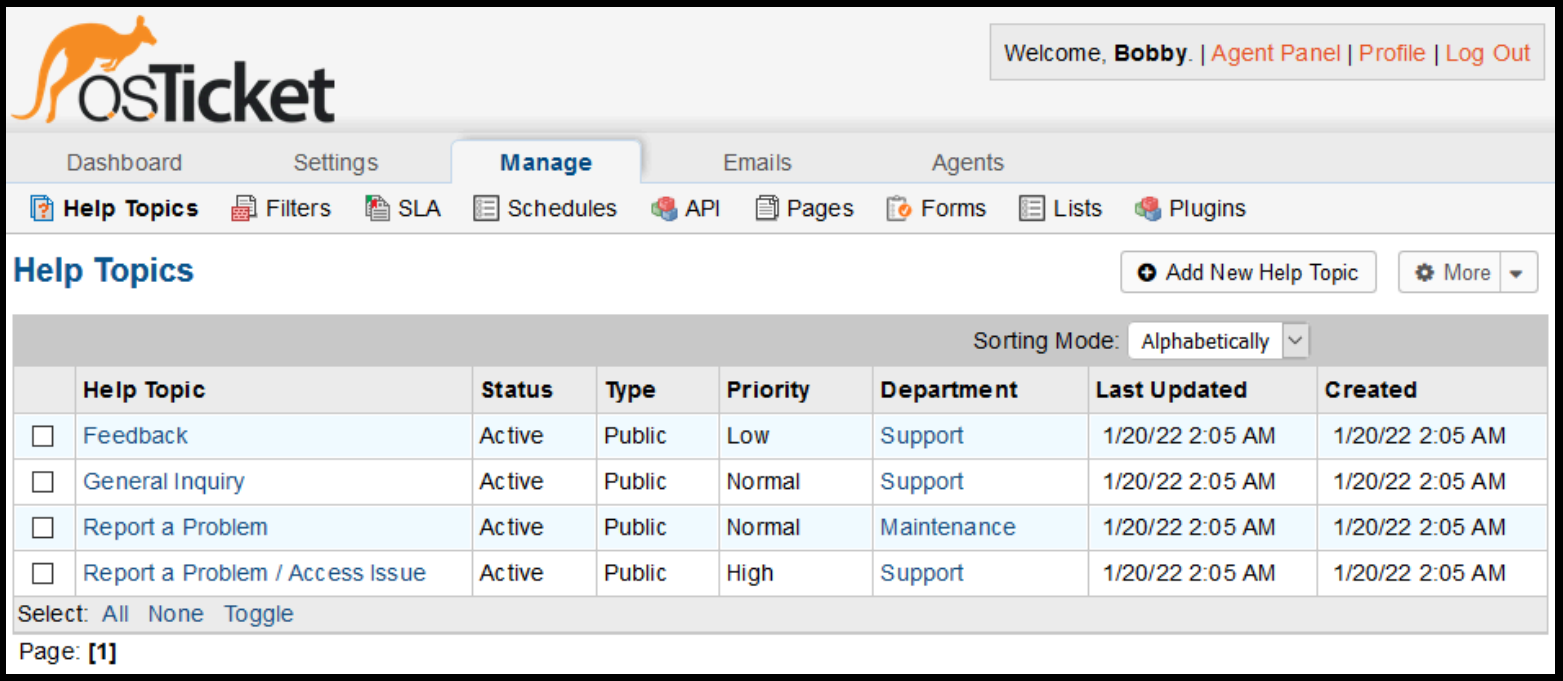
A **ticketing system** manages requests, incidents, and problems. Ticketing systems can be used to support both internal end-users and external customers.

The general process of ticket management is as follows:

1. A user contacts the help desk, perhaps by phone or email, or directly via the ticketing system.
   A unique job ticket ID is generated, and an agent is assigned to the ticket. The ticket will also need to capture some basic details:
   - User information: The user's name, contact details, and other relevant information, such as department or job role. It might be possible to link the ticket to an employee database or customer relationship management (CRM) database.
   - Device information: If relevant, the ticket should record information about the user's device. It might be possible to link to the relevant inventory record via a service tag or asset ID.
2. The user supplies a description of the issue.
   The agent might ask clarifying questions to ensure an accurate initial description.

3. The agent categorizes the support case, assesses how urgent or severe it is, and determines how long it will take to fix.
4. The agent may take the user through initial troubleshooting steps. If these do not work, the ticket may be escalated to deskside support or a senior technician.

Figure 1. Defining help-desk categories in the osTicket ticketing system



Description

A table below lists the help topics with status, type, priority, department, last updated, and created.

11.1.4 Categories and Severity

Categories

Categories and subcategories group related tickets together. This is useful for assigning tickets to the relevant support section or technician and for reporting and analysis.

Service management standards distinguish between the following basic ticket types:

- Requests are for provisioning things that the IT department has a SOP for, such as setting up new user accounts, purchasing new hardware or software, deploying a web server, and so on. Complex requests that aren't covered by existing procedures are better treated as projects rather than handled via the ticketing system.
- Incidents are related to any errors or unexpected situations faced by end-users or customers. Incidents may be further categorized by severity (impact and urgency), such as minor, major, and critical.
- Problems are causes of incidents and will probably require analysis and service reconfiguration to solve. This type of ticket is likely to be generated internally when the help desk starts to receive many incidents of the same type.

Using these types as top-level categories for an end-user facing system is not always practical, however. End-users are not likely to know how to distinguish incidents from problems, for example. Devising categories that are narrow enough to be useful but not so numerous as to be confusing or to slow down the whole ticketing process is a challenging task.

One strategy is for a few simple, top-level categories that end-users can self-select, such as New Device Request, New App Request, Employee Onboarding, Employee Offboarding, Help/Support, and Security Incident. Then, when assigned to the ticket, the support technician can select from a longer list of additional categories and subcategories to help group related tickets for reporting and analysis purposes. Alternatively, or to supplement categories, the system might support adding standard keyword tags to each ticket. A keyword system is more flexible but does depend on each technician tagging the ticket appropriately.

Severity

A severity level is a way of classifying tickets into a priority order. As with categories, these should not be overly complex. For example, three severity levels based on impact might be considered sufficient:

- Critical incidents have a widespread effect on customers or involve potential or actual data breach.
- Major incidents affect a limited group of customers or involve a suspected security violation.
- Minor incidents are not having a significant effect on customer groups.

More discrete levels may be required if the system must prioritize hundreds or thousands of minor incidents per week. A more sophisticated system that measures both impact and urgency might be required. Severity levels can also drive a notification system to make senior technicians and managers immediately aware of major and critical incidents as they arise.

11.1.5 Ticket Management

After opening an incident or problem ticket, the troubleshooting process is applied until the issue is resolved. At each stage, the system must track the ownership of the ticket (who is dealing with it) and its status (what has been done).

This process requires clear written communication and might involve tracking through different escalation routes.

Escalation Levels

Escalation occurs when an agent cannot resolve the ticket. Some of the many reasons for escalation include:

- The incident is related to a problem and requires analysis by senior technicians or by a third-party/warranty support service.

- The incident severity needs to be escalated from minor to major or major to critical and now needs the involvement of senior decision-makers.
- The incident needs the involvement of sales or marketing to deal with service complaints or refund requests.

The support team can be organized into tiers to clarify escalation levels. For example:

- Tier 0 presents self-service options for the customer to try to resolve an incident via advice from a knowledge base or "help bot." A knowledge base is a collection of FAQs and common troubleshooting procedures that a user can refer to before filing a trouble ticket.

- Tier 1 connects the customer to an agent for initial diagnosis and possible incident resolution.
- Tier 2 allows the agent to escalate the ticket to senior technicians (Tier 2 – Internal) or to a third-party support group (Tier 2 – External).
- Tier 3 escalates the ticket as a problem to a development/engineer team or to senior managers and decision-makers.

11.2 Professional Communication

Core 2 Exam Objectives Covered

- 4.7 Given a scenario, use proper communication techniques and professionalism.

It is the end of the work day and you have just received an email from the ticketing system. This newly assigned ticket states that a critical server to the organization is down and needs to be dealt with today. You make a phone call to your supervisor and explain that it is the end of your shift and that the ticket will need to wait until tomorrow or be reassigned to a technician on the night shift. The supervisor states that unfortunately, the ticket must be resolved now and you will need to stay late. Your temper begins to flare and you voice your frustration with them on the phone.

You end the call and grab your tool bag, heading off to resolve the issue. You are visibly frustrated and become very short with the user who reported the issue while on site. You dismiss their questions and become judgmental, stating that they should have just waited until tomorrow to report the issue. After correcting the issue, you post on social media about the encounter and having to stay late to fix the issue that "could" have waited until tomorrow.

Unfortunately, this conduct is unprofessional and can lead to consequences for your employer. Regardless of the incident and circumstances, a true professional maintains a positive and helpful attitude while assisting the customer. Understanding and using professional communication in all aspects of the job, on site and remotely, will be critical to your success as an IT specialist.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the characteristics of professional communication?
- How does maintaining a positive attitude affect a service call?
- How should you deal with a difficult situation such as an angry client or customer?

11.2.1 Professional Support Processes

From the point of first contact, the support process must reassure customers that their inquiry will be handled efficiently. If the customer has already encountered a problem with a product, finding that the support process is also faulty will double their poor impression of your company.

Professional Documentation

Support contact information and hours of operation should be well-advertised so that the customer knows exactly how to open a ticket. The service should have proper documentation so the customer knows what to expect regarding supported items, how long incidents may take to resolve, when they can expect an item to be replaced instead of repaired, and so on.

Set Expectations and Timeline

On receiving the request (whether it is a call, email, or face-to-face contact), acknowledge the request and set expectations. For example, repeat the request back to the customer, then state the next steps and establish a timeline. For example, "I have assigned this problem to Evan Pierce. If you don't hear from us by 3 p.m., please call me." The customer may have a complaint, a problem with some equipment, or simply a request for information. It is important to clarify the nature of these factors:

- The customer's expectations of what will be done to fix the problem and when.

- The customer's concerns about cost or the impact on business processes.
- Your constraints—time, parts, costs, contractual obligations, and so on.

Meet Expectations and Timeline

If possible, the request should be resolved in one call. If this is not possible, the call should be dealt with as quickly as possible and escalated to a senior support team if a solution cannot be found promptly. What is important is that you drive problem acceptance and resolution, either by working on a solution yourself or ensuring that the problem is accepted by the assigned person or department. Open tickets should be monitored and re-prioritized to ensure that they do not fail to meet the agreed-upon service and performance levels.

It is imperative to manage the customer's expectations of when the problem will be resolved. Customers should not feel the need to call you to find out what's happening. This is irritating for them to do and wastes time dealing with an unnecessary call.

A common problem when dealing with customer complaints is feeling that you must defend every action of your company or department. If the customer makes a true statement about your levels of service (or that of other employees), do not try to think of a clever excuse or mitigating circumstance for the failing; you will sound as though you do not care. If you have let a customer down, be accurate and honest. Empathize with the customer, but identify a positive action to resolve the situation:

```
"You're right, I'm sorry the technician didn't turn up. I guarantee that a technician
will be with you by 3 p.m., and I'll let my supervisor know that you have had to call
us. Shall I call you back just after 3 to make sure that things are OK?"
```

Repair and Replace Options

If there is a product issue that cannot be solved remotely, you might offer to repair or replace the product:

- **Repair**-—The customer will need clear instructions about how to pack and return the item to a repair center, along with a ticket-tracking number and returned-merchandise authorization (RMA). The customer must be kept up to date on the progress of the repair.
- **Replace**-—Give the customer clear instructions for how the product will be delivered or how it can be re-ordered, and whether the broken product must be returned.

Follow Up

If you have resolved the ticket and tested that the system is operating normally again, you should give the customer a general indication of what caused the issue and what you did to fix it, along with assurance that the problem is now fixed and unlikely to reoccur. Upon leaving or ending the call, thank the customer for their time and assistance, and show that you have appreciated the chance to solve the issue.

It might be appropriate to arrange a follow-up call at a later date to verify that the issue has not reoccurred and that the customer is satisfied with the assistance provided. When the solution has been tested and verified and the customer has expressed satisfaction with the resolution of the problem, log the ticket as closed. Record the solution and send verification to the customer via email or phone call.

11.2.2 Professional Support Delivery

Respect means that you treat others (and their property) as you would like to be treated. Respect is one of the hallmarks of professionalism.

Be On Time

Ensure that you are on time for each in-person appointment or contact call. If it becomes obvious that you are not going to be on time, inform the customer as soon as possible. Be accountable for your actions, both before you arrive on site and while on site. This means being honest and direct about delays, but make sure this is done in a positive manner. For example:

"I'm sorry I'm late—show me this faulty PC and I'll start work right away."

"The printer needs a new fuser and I'm afraid I don't have this type with me. What I will do is call the office and find out how quickly we can get one..."

"I haven't seen this problem before, but I have taken some notes and I'll check this out as soon as I get back to the office. I'll give you a call this afternoon—will that be OK?"

Avoid Distractions

A distraction is anything that interrupts you from the task of resolving the ticket. Other than a genuinely critical incident taking priority, do not allow interruptions when you are working at a customer's site. Do not take calls from colleagues unless they are work-related and urgent. Other than a genuine family emergency, do not take personal calls or texts. Do not browse websites, play games, or respond to posts on social media.

If you are speaking with a customer on the telephone, always ask their permission before putting the call on hold or transferring the call.

Deal Appropriately with Confidential and Private Materials

You must also demonstrate respect for the customer's property, including any confidential or private data they might have stored on a PC or smartphone, or printed as a document:

- Do not open data files, email applications, contact managers, web pages that are signed into an account, or any other store of confidential or private information. If any of these apps or files are open on the desktop, ask the

customer to close them before you start work.

- Similarly, if there are printed copies of confidential materials (bank statements or personal letters, for instance) on or near a desk, do not look at them. Make the customer aware of them, and allow time for them to be put away.
- Do not use any equipment or services such as PCs, printers, web access, or phones for any purpose other than resolving the ticket.
- If you are making a site visit, keep the area in which you are working clean and tidy, and leave it as you found it.

11.2.3 Professional Appearance

There are many things that contribute to the art of presentation. Your appearance and attire, the words you use, and respecting cultural sensitivities are particularly important.

Professional Appearance and Attire

When you visit a customer site, you must represent the professionalism of your company in the way you are dressed and groomed. If you do not have a company uniform, you must wear clothes that are suitable for the given environment or circumstance:

- Formal attire means matching suit clothes in sober colors and with minimal accessories or jewelry. Business formal is only usually required for initial client meetings.

- Business casual means smart clothes. Notably, jeans, shorts and short skirts, and T-shirts/vests are not smart workwear. Business casual is typically sufficient for troubleshooting appointments.
- You may also need to bring a dust protection suit or coveralls if any planned maintenance may dirty or soil your clothing. For example, when needing to run a new network cable through an attic or crawl space. Just be sure your company is aware and has approved the attire for use for the situation. Figure 1. Business casual can mean a wide range of smart clothes



Using Proper Language

When you greet someone, you should be conscious of making a good first impression. When you arrive on site, make eye contact, greet the customer, and introduce yourself and your company. When you answer the phone, introduce yourself and your department and offer assistance.

When you speak to a customer, you need to make sense. Obviously, you must be factually accurate, but it is equally important that the customer understands what you are saying. Not only does this show the customer that you are competent, but it also proves that you are in control of the situation, giving the customer confidence in your abilities. You need to use clear and concise statements that avoid jargon, abbreviations, acronyms, and other technical language that a user might not understand. For example, compare the following scenarios:

"Looking at the TFT, can you tell me whether the driver is signed?"

"Is a green check mark displayed on the icon?"

The first question depends on the user understanding what a TFT is, what a signed driver might be, and knowing that a green check mark indicates one. The second question gives you the same information without having to rely on the user's understanding.

While you do not have to speak very formally, avoid being over-familiar with customers. Do not use slang phrases and do not use any language that may cause any sort of offense. For example, you should greet a customer by saying "Hello" or "Good morning" rather than "Hey!"

Cultural Sensitivity

Cultural sensitivity means being aware of customs and habits used by other people. It is easy to associate culture simply with national elements, such as the difference between the way Americans and Japanese people greet one another. However, within each nation there are many different cultures created by social class, business opportunities, leisure pursuits, and so on. For example, a person may expect to be addressed by a professional title, such as "doctor" or "judge." Other people may be more comfortable speaking on a first-name basis. It is safer to start on a formal basis and use more informal terms of address if the customer signals that they are happier speaking that way.

Though people may be influenced by several cultures, their behavior is not determined by culture. Customer service and support require consideration for other people. You cannot show consideration if you make stereotyped assumptions about people's cultural backgrounds without treating them as an individual.

Accent, dialect, and language are some of the crucial elements of cultural sensitivity. These elements can make it hard for you to understand a customer and perhaps difficult for a customer to understand you. When dealing with a language barrier, use questions, summaries, and restatements to clarify customer statements. Consider using visual aids or demonstrations rather than trying to explain something in words.

Also, different cultures define personal space differently, so be aware of how close or far you are from the customer.

11.2.4 Professional Communications

You must listen carefully to what is being said to you; it will give you clues to the customer's technical level, enabling you to pace and adapt your replies accordingly.

Active Listening

Active listening is the skill of listening to an individual with your full attention without arguing with, commenting on, or misinterpreting what they have said. With active listening, you make a conscious effort to keep your attention focused on what the other person is saying, as opposed to being distracted by what your reply is going to be or by some background noise or interruption. Some of the other techniques of active listening are to reflect phrases used by the other person, or to restate the issue and summarize what they have said. This helps to reassure the other person that you have attended to what has been said. You should also try to take notes of what the customer says so that you have an accurate record.

Figure 1. Listening carefully will help you to get the most information from what a customer tells you



11.2.5 Clarifying and Questioning Techniques

There will inevitably be a need to establish some technical facts with the customer. This means directing the customer to answer your questions. There are two broad types of questioning:

- **Open-ended**—A question that invites the other person to compose a response. For example, "What seems to be the problem?" invites the customer to give an opinion about what they think the problem is.
- **Closed**—A question that can only be answered with a "Yes" or "No" or that requires some other fixed response. For example, "What error number is displayed on the panel?" can only have one answer.

The basic technique is to start with open-ended questions. You may try to guide the customer toward information that is most helpful. For example, "When you say your printer is not working, what problem are you having? Will it not switch on?" However, be careful about assuming what the problem is and leading the customer to simply affirming a guess. As the customer explains what they mean, you may be able to perceive what the problem is. If so, do not assume anything too early. Ask pertinent closed questions that clarify customer statements and prove or disprove your perception. The customer may give you information that is vague or ambiguous. Clarify the customer's meaning by asking questions like, "What did the error message say?" or "When you say the printout is dark, is there a faint image or is it completely black?" or "Is the power LED on the printer lit?"

If a customer is not getting to the point or if you want to follow some specific steps, take charge of the conversation by restating the issue and asking closed questions. For example, consider this interaction:

"It's been like this for ages now, and I've tried pressing a key and moving the mouse, but nothing happens."

"What does the screen look like?"

"It's dark. I thought the computer was just resting, and I know in that circumstance I need to press a key, but that's not working and I really need to get on with..."

In this example, the technician asks an open question that prompts the user to say what they perceive to be the problem instead of relaying valuable troubleshooting information to the technician. Compare with the following scenario:

"It's been like this for ages now, and I've tried pressing a key and moving the mouse, but nothing happens."

"OK, pressing a key should activate the monitor, but since that isn't happening, I'd like to investigate something else first. Can you tell me whether the light on the monitor is green?"

"I don't see a green light. There's a yellow light, though."

Restating the issue and using a closed question allows the agent to start working through a series of symptoms to try to diagnose the problem.

Do note that a long sequence of closed questions fired off rapidly may overwhelm and confuse a customer. Do not try to force the pace. Establish the customer's technical level, and target the conversation accordingly.

11.2.6 Difficult Situations

A difficult situation occurs when either you or the customer becomes, or risks becoming, angry or upset. There are several techniques that you can use to defuse this type of tension.

Note:

It is better to think of the situation as difficult and to avoid characterizing the customer as difficult. Do not personalize support issues.

Maintain a Positive Attitude

Understand that an angry customer is usually frustrated that things are not working properly, or feels let down. Perhaps a technician arrived late and the customer is already irritated. Or perhaps the customer has spent a large amount of money and is now anxious that it has been wasted on a poor-quality product. Empathizing with the customer is a good way to develop a positive relationship and show that you want to resolve the problem. Saying you are sorry does not necessarily mean you agree with what the customer is saying, but rather that you understand their point of view.

"I'm sorry you're having a problem with your new PC. Let's see what we can do to sort things out..."

As part of maintaining a positive attitude and projecting confidence, avoid the following situations:

- **Arguing with the customer**—Remain calm and only advance facts and practical suggestions that will push the support case toward a resolution.
- **Denying that a problem exists or dismissing its importance**—If the customer has taken an issue to the point of complaining, then they clearly feel that it is important. Whether you consider the matter trivial is not the issue. Acknowledge the customer's statement about the problem, and demonstrate how it can be resolved.
- Avoid **being judgmental**—Do not assume that the customer lacks knowledge about the system and is therefore causing the problem.

11.2.7 Dealing with Difficult Customers

It is never easy to talk to someone who is unreasonable, abusive, or shouting, but it is important to be able to deal with these situations professionally.

1. **Identify early signs that a customer is becoming angry**—Indicators of tension include a raised voice, speaking too quickly, interrupting, and so on.
   Try to calm the situation down by using a low voice and soothing language and focusing on positive actions.

2. **Do not take complaints personally**—Any anger expressed by the customer toward you is not personal but rather a symptom of the customer's frustration or anxiety.
3. **Let the customer explain the problem while you actively listen**—Draw out the facts, and use them as a positive action plan to drive the support case forward.
4. **Hang up**—Be guided by whatever policy your organization has in place, but in general terms, if a customer is abusive or threatening, issue a caution to warn them about this behavior.
   If the abuse continues, end the call or escalate it to a manager. Make sure you explain and document your reasons.

11.2.8 Do Not Post Experiences on Social Media

Everyone has bad days when they feel the need to get some difficult situation off their chest. Find a colleague for a private face-to-face chat, but under no circumstances should you ever disclose these types of experiences via social media outlets.

Technicians should always exercise discretion and professionalism when referencing specific incidents and cases they are involved in. Remember that anything posted to social media or revealed publicly is very hard to withdraw and can cause unpredictable reactions from customers and the organization you work for.

11.3 Types of Operating Systems

Core 2 Exam Objectives Covered

- 1.1 Explain common operating system (OS) types and their purposes

You have been assigned a new trouble ticket. This ticket is for a new server that runs the Linux operating system. You have not used Linux and this causes an uneasy feeling as you gather your tool bag and contact the customer needing support. While you are very familiar with the Windows operating system, Linux brings a new flavor to the enterprise environment.

Once on site, you set the server up and boot it for the first time. It boots and a login screen appears. You are unsure of the credentials to log in, so you conduct research online and in the owner's manual. You have the credentials and log in. The logon process completes and a simple black screen appears with white text. Now the fun can begin as you learn how to configure the server with a brand new operating system.

Learning Outcomes

As you study this lesson, please answer the following questions:

- What are the four main operating systems found on computer systems?
- What are the two most common mobile operating systems?
- What file systems are commonly used by each operating system?
- What happens when a system reaches end-of-life?

11.3.1 Windows and macOS

The market for operating systems is divided into four main types:

- **Business client**: Designed for use as a client in centrally managed business domain networks.
- **Network Operating System (NOS)**: Designed to run servers in business networks.
- **Home client**: Designed for standalone use or in a workgroup network in a home or small office.
- **Cell phone (smartphone)/Tablet**: Designed for handheld devices with a touch-operated interface.
  Note:

  A business client PC is often called a workstation. However, hardware vendors typically use "workstation" to refer to a powerful PC used for tasks like graphic design, video editing, or software development.

Microsoft Windows

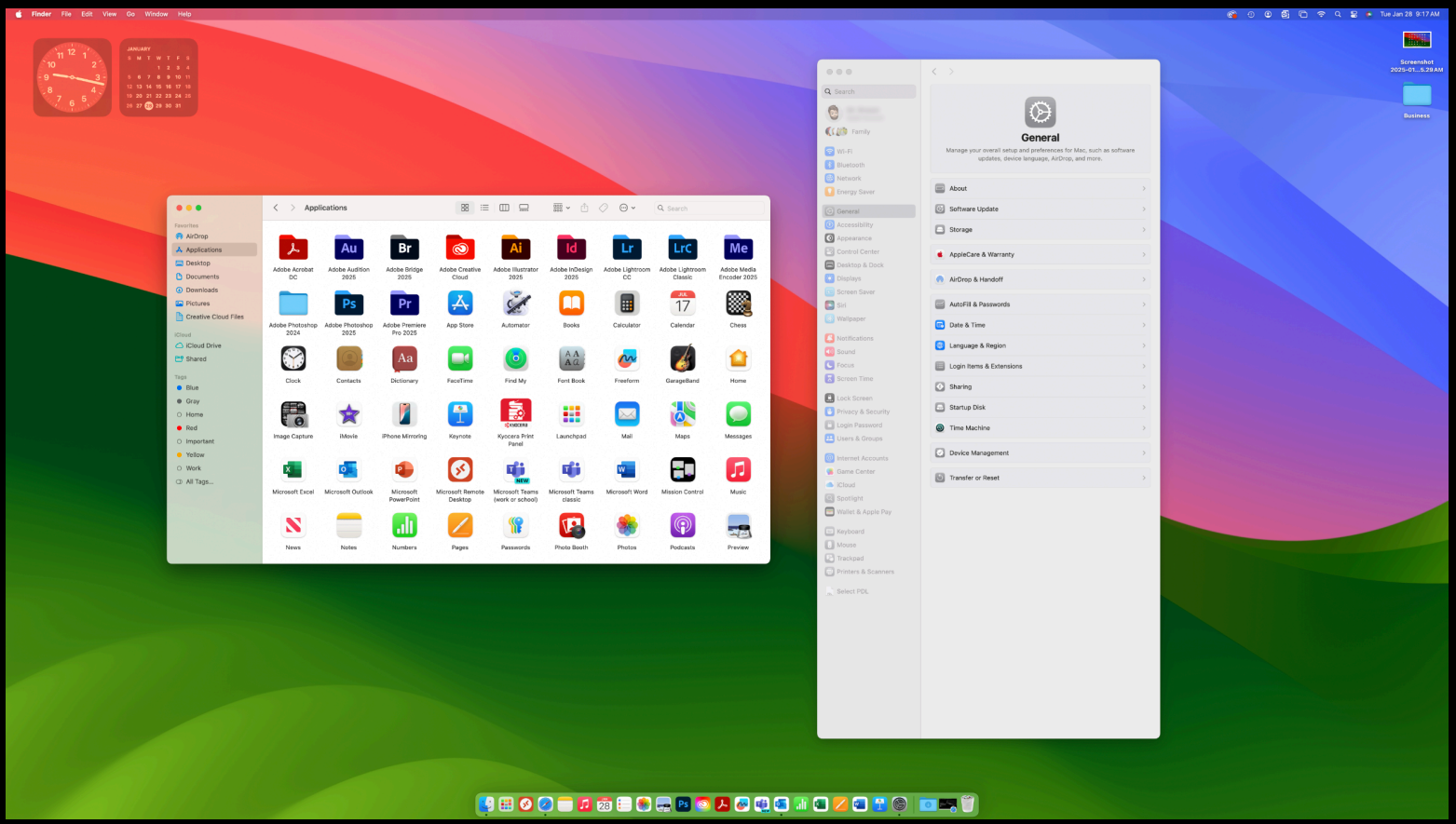
Microsoft **Windows** serves all four market segments:

- **Windows 10 and Windows 11**: Available in editions for both business workstations and home PCs, supporting touch interfaces for tablets and laptops. (Note: Windows smartphones are discontinued.)
- **Windows Server 2019, 2022, and 2025**: Optimized as Network Operating Systems (NOSs), sharing the same underlying code and desktop interface as the client versions.

Apple macOS

macOS is exclusively available on Apple-built devices, such as Mac desktops, iMac all-in-ones, and MacBooks. It cannot be purchased or installed on non-Apple PCs, which enhances stability but limits hardware options. Derived from a type of UNIX kernel, but macOS includes additional code for its graphical interface and system utilities. It supports the Magic Trackpad, but not touch screens.

Figure 1. macOS 15 Desktop



Screenshot reprinted with permission from Apple Inc.

Apple offers free periodic updates for macOS. Currently supported versions are macOS 12 (Monterey), macOS 13 (Ventura), and macOS 14 (Sonoma), while older versions like 10.15 (Catalina) and 11 (Big Sur) are gradually losing support. Each macOS release has specific hardware requirements, and compatibility with older Mac models may vary. Hardware compatibility details are available on Apple's support site (support.apple.com).

11.3.2 UNIX, Linux, and Chrome OS

While Windows and macOS dominate the desktop and workstation market, a third family of operating systems, based on UNIX-like systems, is widely used across a broad range of devices.

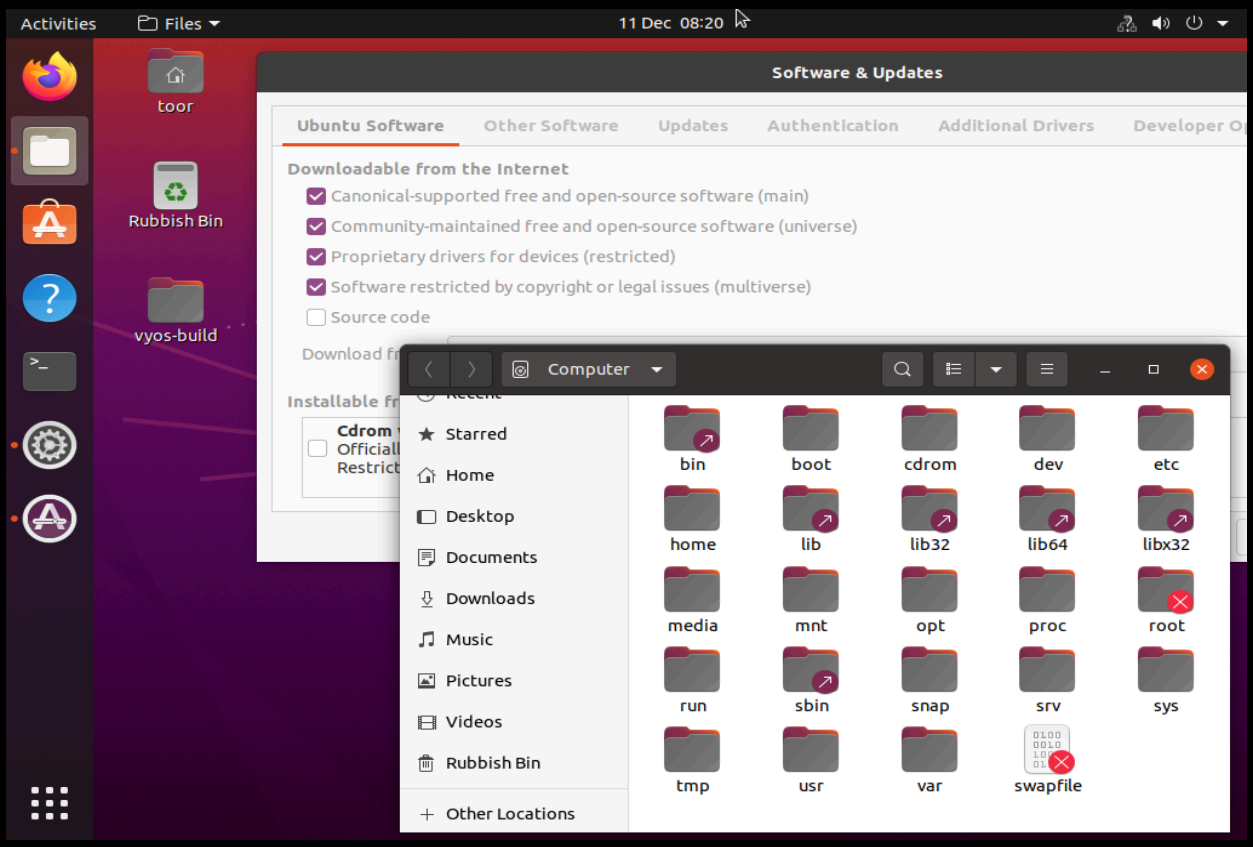
UNIX

UNIX-systems is a trademark for a family of operating systems developed at Bell Laboratories in the late 1960s. UNIX systems feature a kernel/shell architecture. The kernel manages system resources like CPU, RAM, and I/O devices, while the shell provides the user interface. Known for their portability (unlike Windows and macOS), UNIX systems can run on diverse hardware platforms, from personal computers to mainframes.

Linux

Developed by Linus Torvalds, **Linux** is an open-source OS kernel derived from UNIX. It includes features like a shell command interpreter, desktop environment, and app packages. Unlike Windows and macOS, Linux has numerous distributions (distros), each with its own package set. Notable distros include SUSE, Red Hat Enterprise Linux (RHEL), Fedora, Debian, Ubuntu, Mint, and Arch, each offering different licensing and support options. SUSE and Red Hat are subscription-based, Ubuntu offers free installation with paid enterprise support, and Fedora, Debian, Mint, and Arch are community-supported.

Figure 1. Ubuntu Linux desktop with apps for package and file management open



Linux distros follow two release models:

- **Standard Release**: Uses versioning for updates, with some versions offering long-term support (LTS).
- **Rolling Release**: Provides updates as they become stable, without version distinctions.

Linux serves as both a desktop and server OS. It is often used in schools and universities as a desktop OS and dominates the web server market as a server OS. Additionally, it is widely used in smart appliances and Internet of Things (IoT) devices.

Chrome OS

Chrome OS, developed by Google, is a proprietary operating system derived from the open-source Chromium OS, which is based on Linux. It is designed for specific hardware, such as Chromebooks (laptops) and Chromeboxes (PCs), targeting budget and education markets.

Primarily built for web applications, Chrome OS relies on server-hosted software accessed via a browser, reducing the need for powerful client hardware. Its minimal environment minimizes interference from other software or drivers, enhancing browser performance.

Chrome OS also supports offline "packaged" apps and can run Android and Linux apps, offering flexibility for users and developers.

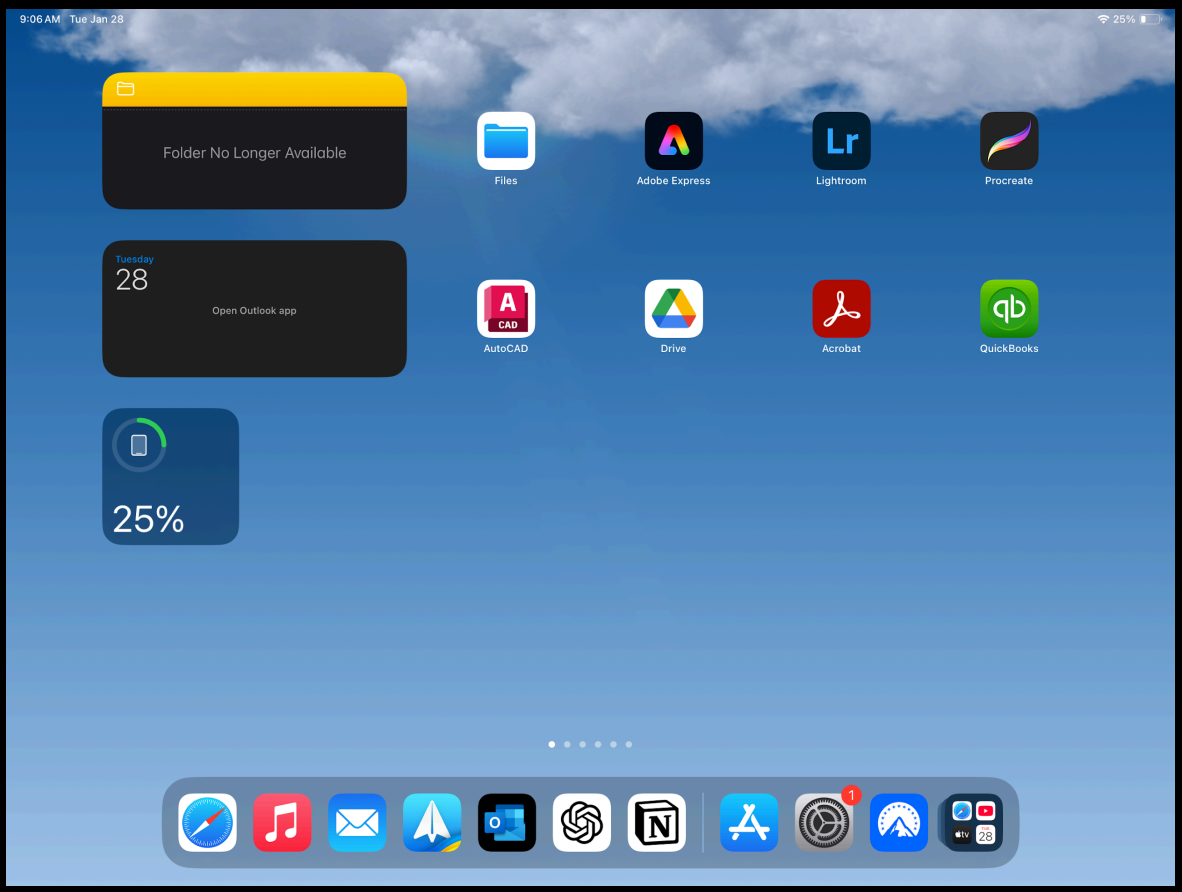
11.3.3 iOS and Android

Cell phone and tablet operating systems are designed exclusively for touch-screen interfaces. The main OSs in this category are Apple iOS/**iPadOS** and Android.

Apple iOS

iOS is the operating system for Apple's iPhone and early iPad models. iOS is based on the macOS operating system and is closed-source, meaning only Apple can modify the code, and it runs exclusively on Apple devices. This operating system provides the support for the touchscreen interface and applications.

Figure 1. iOS 18 running on an iPad



Screenshot reprinted with permission from Apple Inc.

New iOS versions are released annually, with version 17 being the latest at the time of writing. Updates are free, but older devices may not support all features or may not be supported at all. **Update limitations** are detailed at support.apple.com.

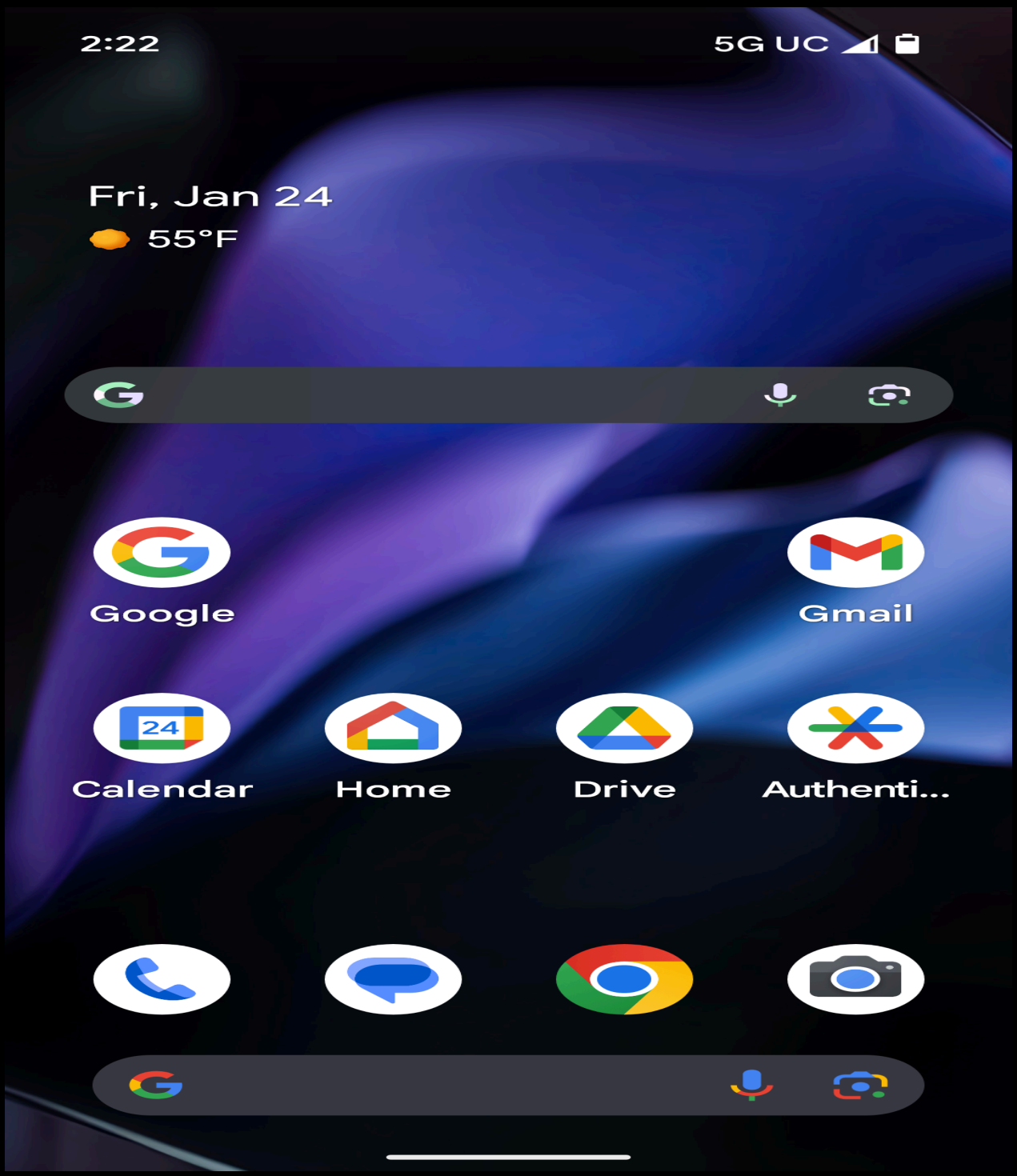
Apple iPadOS

iPadOS, developed from iOS, supports the latest iPad models (2019 and later). It offers enhanced multitasking capabilities and better support for the Apple Pencil. iPadOS versions are released alongside iOS updates.

Android™

Android is an open-source operating system developed by the Open Handset Alliance, driven by Google. Based on Linux, its source code is publicly available, allowing manufacturers to create custom versions for their devices. This results in a wide variety of Android-powered smartphones and tablets from brands like Acer, Asus, HTC, LG, Motorola, Samsung, Google (Pixel), Xiaomi, OnePlus, and Oppo, each with unique features or interfaces.

Figure 2. Android 15 home screen


2:22
5G UC
Fri, Jan 24
55°F
Google
Gmail
Calendar
Home
Drive
Authenti...

Screenshot courtesy of Android platform.

The current stable version is Android 14 (at the time of writing). A key challenge with Android is fragmentation—while Google issues regular updates, manufacturers decide when or if their devices receive them, leading to varied compatibility and support across devices.

A+ Core 1 and Core 2 CertMaster Perform 15.0

11.3.4 Windows File System Types

High-level formatting prepares a partition on a disk device for use with an operating system. The format process creates a **file system** on the disk partition. Each OS is associated with various types of file systems.

New Technology File System

The New Technology File System (NTFS) is a proprietary file system developed by Microsoft for use with Windows. It provides a 64-bit addressing scheme, allowing for very large volumes and file sizes. In theory, the maximum volume size is 16 Exabytes, but actual implementations of NTFS are limited to between 137 GB and 256 Terabytes, depending on the version of Windows and the allocation unit size. The key NTFS features are:

- **Journaling**—When data is written to an NTFS volume, it is re-read, verified, and logged. In the event of a problem, the sector concerned is marked as bad and the data relocated. Journaling makes recovery after power outages and crashes faster and more reliable.
- **Snapshots**—This allows the Volume Shadow Copy Service to make read-only copies of files at given points in time even if the file is locked by another process. This file version history allows users to revert changes more easily and supports backup operations.
- **Security**—Features such as file permissions and ownership, file access audit trails, quota management, and encrypting file system (EFS) allow administrators to ensure only authorized users can read/modify file data.
- **POSIX Compliance**—To support UNIX/Linux compatibility, Microsoft engineered NTFS to support case-sensitive naming, hard links, and other key features required by UNIX/Linux applications. Although the file system is case-sensitive capable and preserves case, Windows does not insist upon case-sensitive naming.
- **Indexing**—The Indexing Service creates a catalog of file and folder locations and properties, speeding up searches.
- **Dynamic Disks**—This disk management feature allows space on multiple physical disks to be combined into volumes.

Note:

Windows Home editions do not support dynamic disks or encryption. The latest Windows feature updates have increased the maximum possible NTFS volume size to 8 Petabytes (PB), or 8,000 TB.

Windows can only be installed to an NTFS-formatted partition. NTFS is also usually the best choice for additional partitions and removable drives that will be used with Windows. The only significant drawback of NTFS is that it is not fully supported by operating systems other than Windows. macOS can read NTFS drives, but cannot write to them. Linux distributions and utilities may be able to support NTFS to some degree.

Resilient File System

The **Resilient File System** (ReFS) is Microsoft's newest file system for use with Windows. This new file system is designed for making data easy to access, handle large amounts of data efficiently for different tasks, and keep data safe and protected from damage. The key benefits of ReFS include:

- Resiliency—ability to detect corrupted files and data and repair them while still online and in use, even in virtualized environments.
- High Performance—storage solution improvement along with optimization of data increases the performance with large data sets and workloads through configuration of two logical storage groups or tiers.
- Scalability—supports millions of terabytes of data without impacting performance metrics.

While NTFS remains the predominant file system for many general users, Microsoft supports ReFS for specialized customers requiring the increased availability, resiliency, and scaling that it provides.

Note:

Detailed information on the ReFS and Microsoft's support of the file system can be found at: https://learn.microsoft.com/en-us/windows-server/storage/refs/refs-overview

FAT32

The FAT file system is a very early type named for its method of organization—the file allocation table. The FAT provides links from one allocation unit to another. **File allocation table** (FAT) is a variant of FAT that uses a 32-bit allocation table, nominally supporting volumes up to 2 TB. The maximum file size is 4 GB minus 1 byte.

FAT32 does not support any of the reliability or security features of NTFS. It is typically used to format the system partition (the one that holds the boot loader). It is also useful when formatting removable drives and memory cards intended for multiple operating systems and devices.

exFAT

Extended File Allocation Table(exFAT) is a 64-bit version of FAT designed for use with removable hard drives and flash media. Like NTFS, exFAT supports large volumes, up to a recommended maximum size of 512 Terabytes (TB). There is also support for access permissions but not encryption.

11.3.5 Linux and macOS File System Types

While Linux and macOS provide some degree of support for FAT32 and NTFS as removable media, they use dedicated file systems to format fixed disks.

Linux File Systems

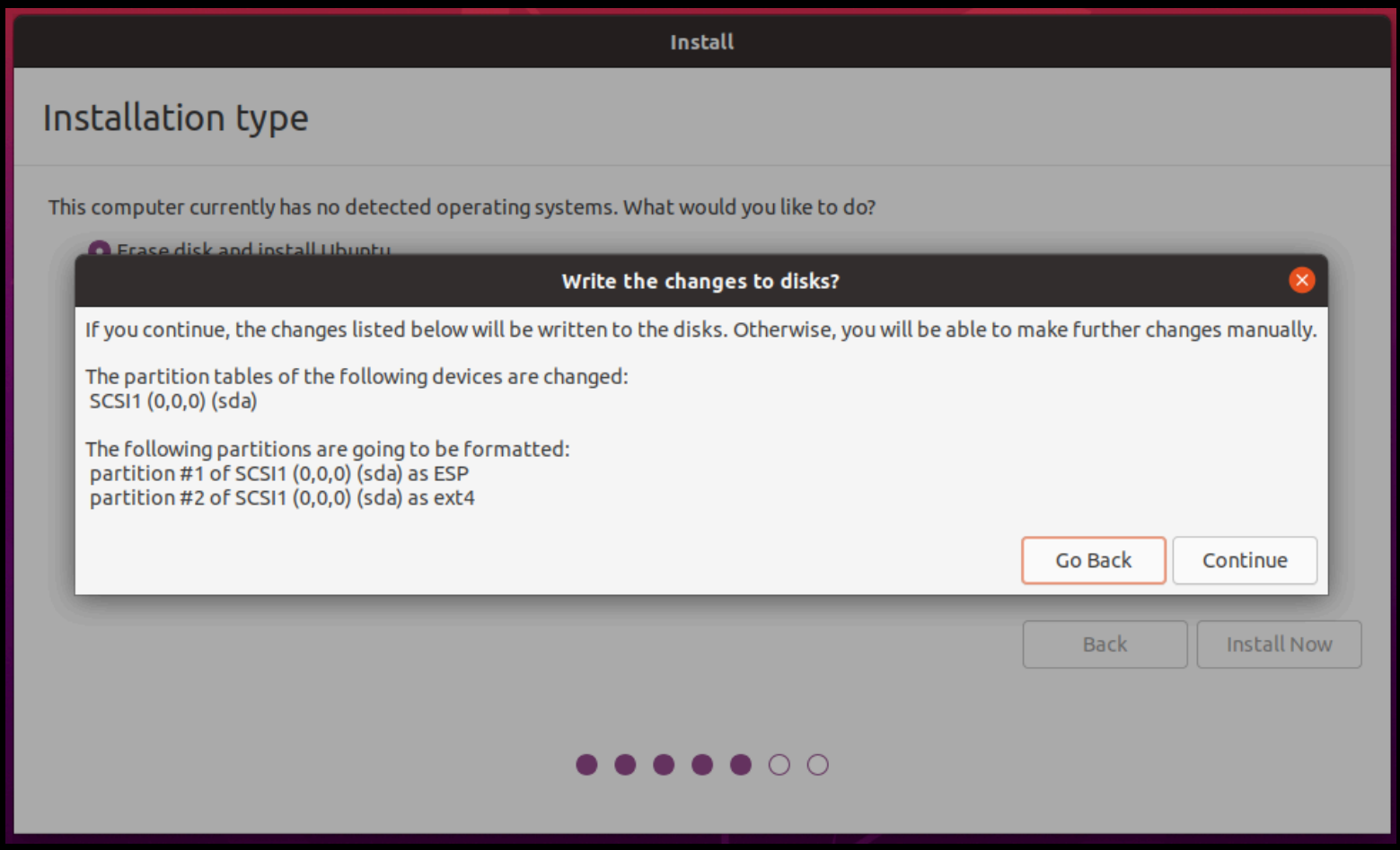
Most Linux distributions use some version of the extended (ext) file system to format partitions on mass storage devices. **ext4** delivers better performance and supports journaling.

Linux will also support FAT/FAT32 (designated as VFAT) and XFS as alternatives to ext.

XFS was introduced in 1993 as the High Performance Scalable File System and provided a 64-bit journaling file system. It is the default file system for Red Hat Enterprise Linux (RHEL) installations and is supported by other Linux distributions.

Additional protocols such as the Network File System (NFS) can be used to mount remote storage devices to the local file system of the Linux OS. This can be used to connect to a file resource on another physical system as if the file system was directly attached to the user's own system.

Figure 1. Ubuntu installer applying default ext4 formatting to the target disk



Description

The pop up reads, if you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually. The partition tables of the following devices are changed: SCSI 1 (0, 0, 0) (sda). The following partitions are going to be formatted: partition 1 of SCSI 1 (0, 0, 0) (sda) as ESP. Partition 2 of SCSI 1 (0, 0, 0) (sda) as ext4.

Apple File System

Where Windows uses NTFS and Linux typically uses ext3 or ext4, Apple Mac workstations and laptops use the proprietary **Apple File System (APFS)**, which supports journaling, snapshots, permissions/ownership, and encryption.

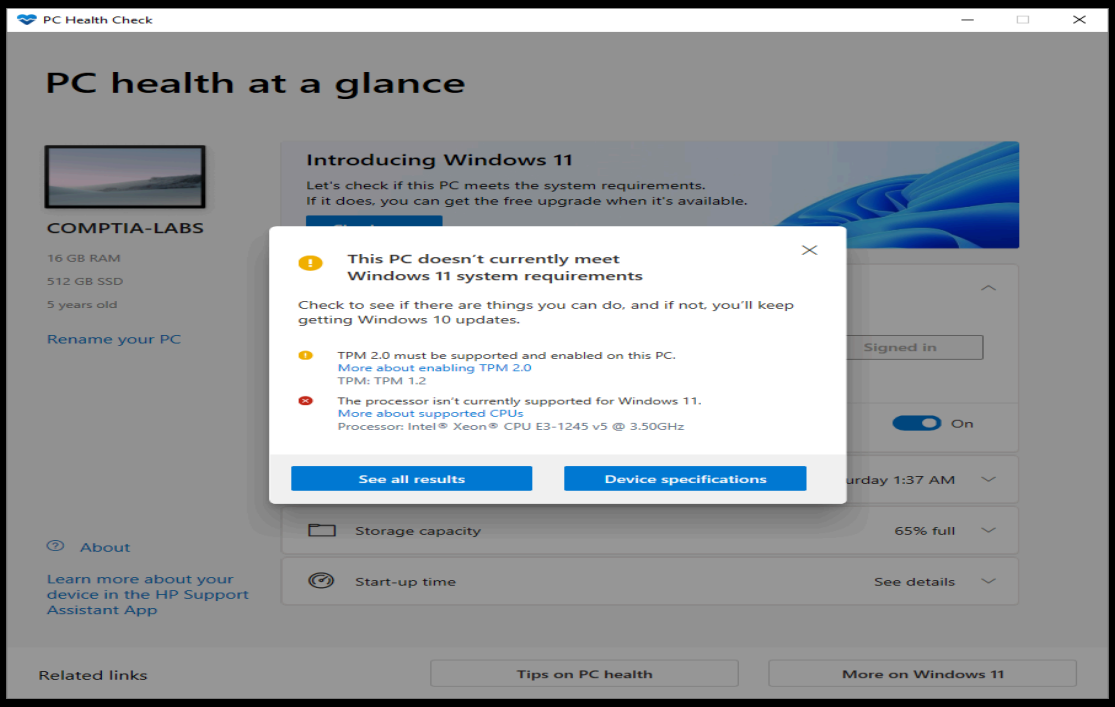
11.3.6 OS Compatibility Issues

One of the major challenges of supporting a computing environment composed of devices that use different operating systems is compatibility concerns. **Compatibility concern** can be considered in several categories: OS compatibility with device hardware, software app compatibility with an OS, host-to-host compatibility for exchanging data over a network, and user training requirements.

Hardware Compatibility and Update Limitations

When you plan to install a new version of an operating system as an upgrade or replace one OS with another, you must check that your computer meets the new hardware requirements. There is always a chance that some change in a new OS version will have update limitations that make the CPU and memory technology incompatible or cause hardware device drivers written for an older version not to work properly. For example, Windows 11 requires a CPU or motherboard with support for Trusted Platform Module (TPM) version 2. This strongly limits its compatibility with older PCs and laptops.

Figure 1. Running PC Health Check to verify compatibility with Windows 11



Description

The pop up reads, this PC doesn't currently meet windows 11 system requirements. Check to see if there are things you can do, and if not, you'll keep getting Windows 10 updates. TPM 2.0 must be supported and enabled on this PC. The processor isn't currently supported by Windows 11. The see all results and device specification buttons are at the bottom.

Software Compatibility

A software application is coded to run on a particular OS. You cannot install an app written for iOS on an Android smartphone, for instance. The developer must create a different version of the app. This can be relatively easy for the developer or quite difficult, depending on the way the app is coded and the target platforms. The app ecosystem—the range of software available for a particular OS—is a big factor in determining whether an OS becomes established in the marketplace.

Network Compatibility

Compatibility is also a consideration for how devices running different operating systems can communicate on data networks. Devices running different operating systems cannot "talk" to one another directly. The operating systems must support common network protocols that allow data to be exchanged in a standard format.

User Training and Support

Different desktop styles introduced by a new OS version or changing from one OS to another can generate issues as users struggle to navigate the new desktop and file system. An upgrade project must take account of this and prepare training programs and self-help resources as well as prepare technicians to provide support on the new interface.

In the business client market, upgrade limitations and compatibility concerns make companies reluctant to update to new OS versions without extensive testing. As extensive testing is very expensive, they are generally reluctant to adopt new versions without a compelling need to do so.

Note:

These compatibility concerns are being mitigated somewhat using web applications and cloud services. A web application only needs the browser to be compatible, not the whole OS. The main compatibility issue for a web application is supporting a touch interface and a very wide range of display resolutions on the different devices that might connect to it.

11.3.7 Vendor Life-cycle Limitations

A vendor life cycle describes the policies and procedures an OS developer or device vendor puts in place to support a product. Policy specifics are unique to each vendor, but the following general life-cycle phases are typical:

- A public beta phase might be used to gather user feedback. Microsoft operates a Windows Insider Program where you can sign up to use early release Windows versions and feature updates.
- During the supported phase when the product is being actively marketed, the vendor releases regular patches to fix critical security and operational issues and feature upgrades to expand OS functionality. Supported devices should be able to install OS upgrade versions.
- During the extended support phase, the product is no longer commercially available, but the vendor continues to issue critical patches. Devices that are in extended support may or may not be able to install OS upgrades.
- An **end-of-life** system is one that is no longer supported by its developer or vendor. EOL systems no longer receive security updates and therefore represent a critical vulnerability for a company's security systems if any remain in active use.

Note:

Microsoft designated October 14, 2025 as the end-of-life date for Windows 10. No free support or updates will be provided by Microsoft after this date.

12.0 Configuring Windows

The operating system (OS) is the software that provides a user interface to the computer hardware and provides an environment in which to run software applications and create computer networks. As a professional IT support representative or PC service technician, your job will include installing, configuring, maintaining, and troubleshooting personal computer (PC) operating systems.

Before you can perform any of these tasks, you need to understand the basics of what an operating system is, including the various versions, features, components, and technical capabilities. With this knowledge, you can provide effective support for all types of system environments.

In this lesson, you will learn how the basic administrative interfaces for Microsoft® Windows 10® and Microsoft® Windows 11® can be used to configure user and system settings.

Prepare for A+ Core 2 by:

- Configuring Windows user settings
- Configuring Windows system settings

12.1 Windows User Settings

Core 2 Exam Objectives Covered

- 1.6 Given a scenario, configure Microsoft Windows settings.

A user has reported that their computer is not working correctly. They are complaining the text is too small for them to read and the clock is not showing the right time. Additionally, they are having issues with the laptop they use for working remotely. When they close the lid on the laptop, the computer does not turn off like it used to. This caused the system to drain its battery while the user was driving to a customer's location. Being able to configure the settings of the operating system will help this user while they utilize the system and are traveling with it.

Learning Outcomes

As you study this lesson, answer the following questions:

- How can you adjust the privacy settings in the Windows OS?
- How would you change the system date and time?
- What options are available under the Ease of Access settings menu?
- How can you view hidden files and folders in File Explorer?

12.1.1 Windows Interfaces

An OS is made up of kernel files and device drivers to interface with the hardware plus programs to provide a user interface and configuration tools. The earliest operating systems for PCs, such as Microsoft's Disk Operating System (DOS), used a command-line user interface or simple menu systems. Windows and software applications for Windows were marked by the use of a graphical user interface (GUI). This helped to make computers easier to use by non-technical staff and home users.

The GUI desktop style favored by a particular OS or OS version is a powerful factor in determining customer preferences for one OS over another.

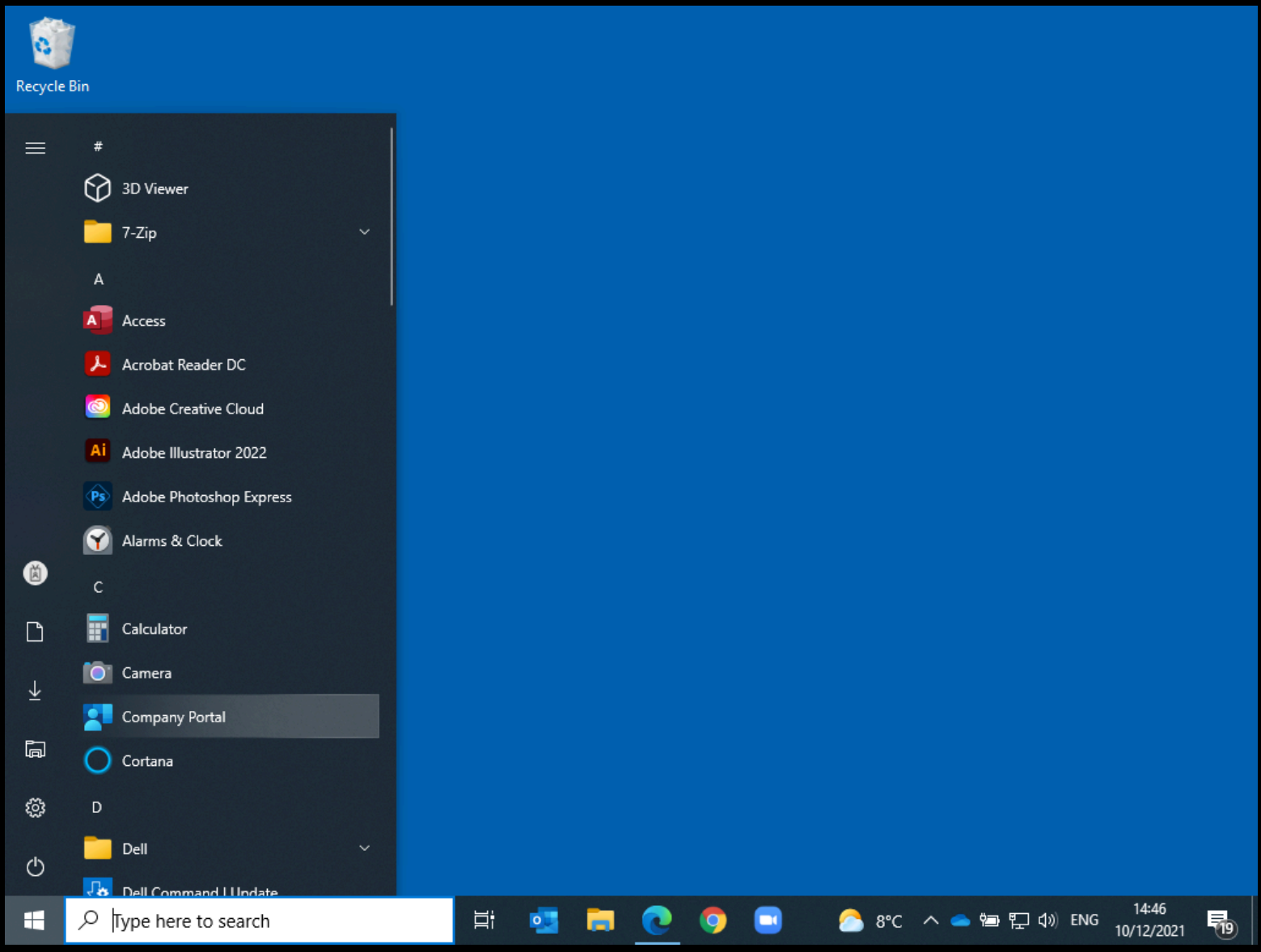
Windows 10 Desktop

One of the main functions of an OS is to provide an interface (or shell) for the user to configure and operate the computer hardware and software. Windows has several interface components designed both for general use and for more technical configuration and troubleshooting.

The top level of the user interface is the desktop. This is displayed when Windows starts, and the user logs on. The desktop contains the Start menu, taskbar, and shortcut icons. These are all used to launch and switch between applications.

Windows 10 uses a touch-optimized Start menu interface. The Start menu is activated by selecting the **Start** button or by pressing the **START** or Windows logo key on the keyboard.

Figure 1. Windows 10 (21H2) desktop and Start menu



Screenshot courtesy of Microsoft.

As well as the Start button, the taskbar contains the **instant search** box, Task View button, and notification area. The notification area contains icons for background processes. The middle part of the taskbar contains icons for apps that have an open window. Some app icons can also be pinned to the taskbar. The taskbar icons are used to switch between program windows.

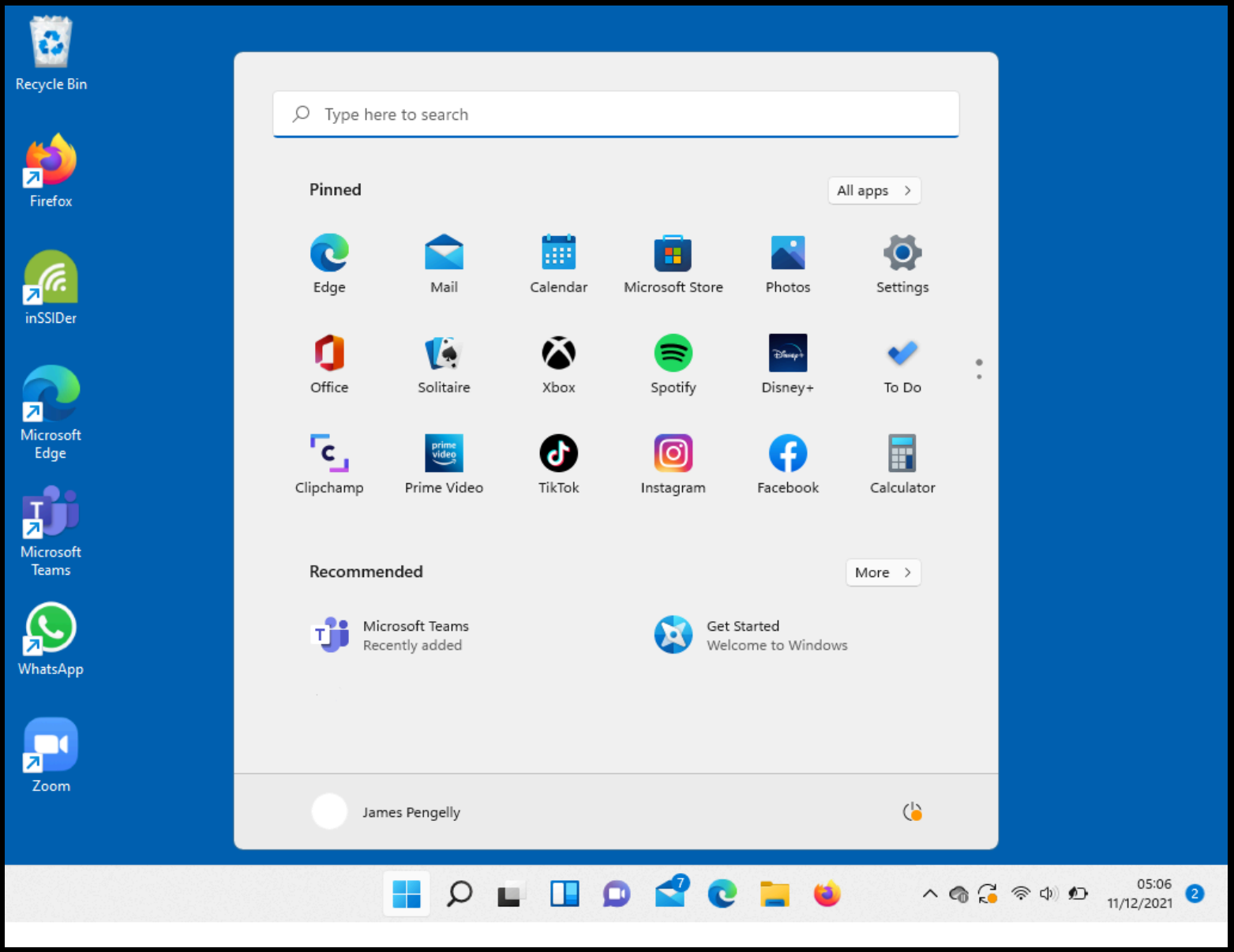
Note:

It is worth learning the keyboard shortcuts to navigate the desktop and program windows quickly. A complete list is published at support.microsoft.com/en-us/windows/keyboard-shortcuts-in-windows-dcc61a57-8ff0-cffe-9796-cb9706c75eec.

Windows 11 Desktop

Windows 11 refreshes the desktop style by introducing a center-aligned taskbar, better spacing for touch control, and rounded corners. It also makes the multiple desktops feature more accessible. Multiple desktops allow the user to set up different workspaces, such as one desktop that has windows for business apps open and another with windows and shortcuts for personal apps and games.

Figure 2. Windows 11 desktop and Start menu


Recycle Bin
Firefox
inSSIDer
Microsoft Edge
Microsoft Teams
WhatsApp
Zoom
Type here to search
Pinned
All apps
Edge
Mail
Calendar
Microsoft Store
Photos
Settings
Office
Solitaire
Xbox
Spotify
Disney+
To Do
Clipchamp
Prime Video
TikTok
Instagram
Facebook
Calculator
Recommended
More
Microsoft Teams
Recently added
Get Started
Welcome to Windows
James Pengelly
05:06
11/12/2021

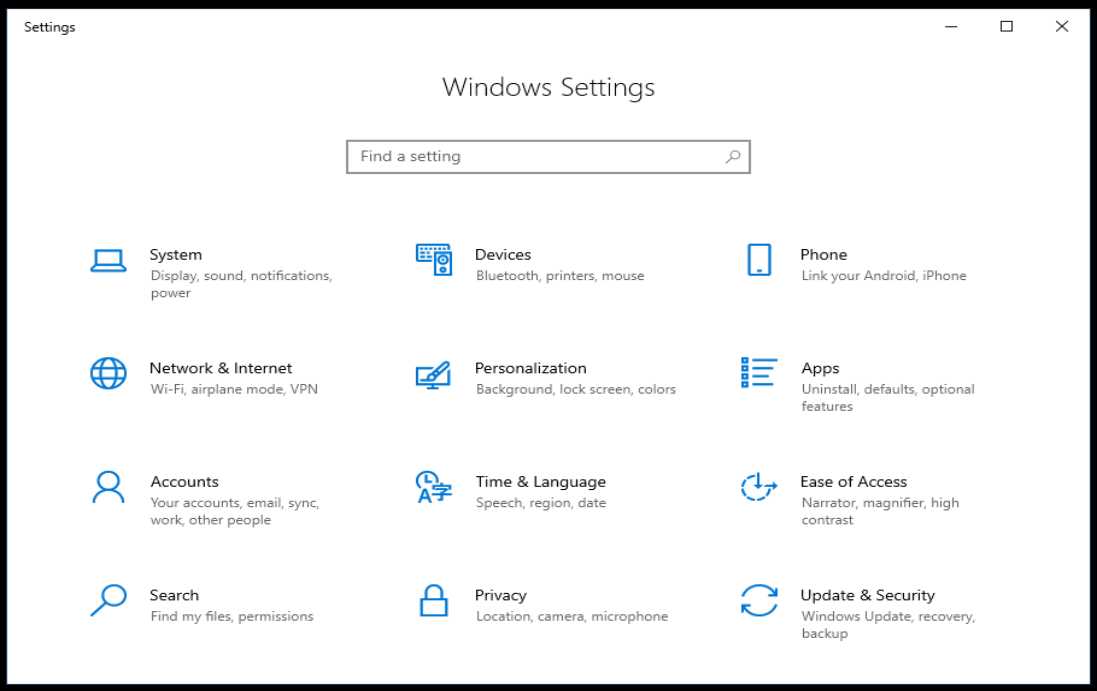
12.1.2 Windows Settings and Control Panel

The Windows Settings app and Control Panel are the two main interfaces for administering Windows. Administering an OS means configuring options, setting up user accounts, and adding and removing devices and software. All Windows configuration data is ultimately held in a database called the registry. Windows Settings and Control Panel contain graphical pages and applets for modifying these configuration settings.

Windows Settings

Windows Settings is a touch-enabled interface for managing Windows. The Settings app is the preferred administrative interface. Configuration option "pages" are divided between a few main headings.

Figure 1. Home page in the Windows 10 Settings app showing the top-level configuration headings or groups



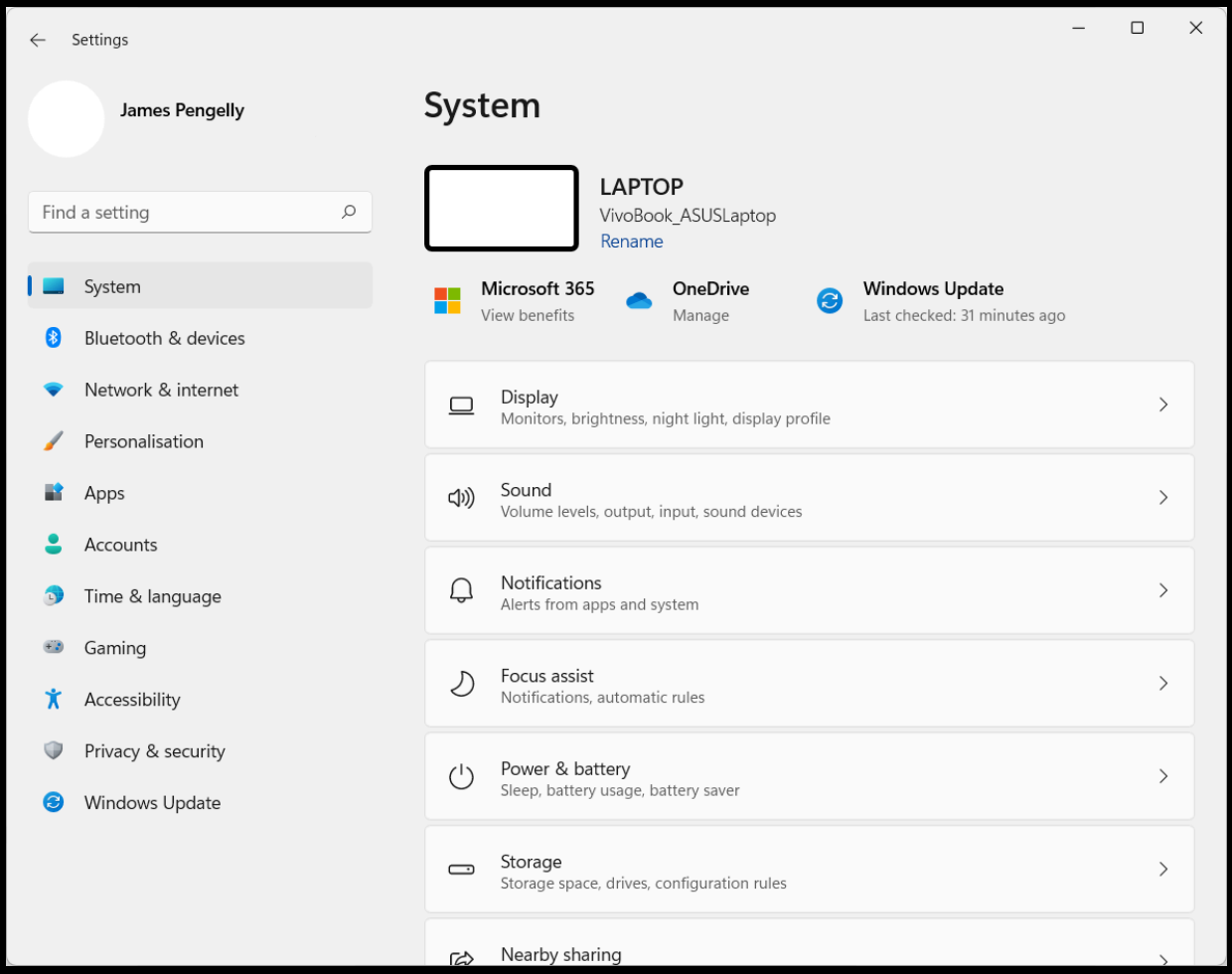
Description

The following options are listed below: System: Display, sound, notifications, power. Devices: Bluetooth, printers, mouse. Phone: Link your Android, iPhone. Network and Internet: Wi-Fi, airplane mode, VPN Personalization: Background, lock screen, colors Apps: Uninstall, defaults, optional features Accounts: Your account, email, sync, work,

other people Time and Language: Speech, region, date Ease of Access: Narrator, magnifier, high contrast Search: Find my files, permissions Privacy: Location, camera, microphone Update and Security: Window Update, recovery, backup

In Windows 11, the Settings app has no "home" page. Use the navigation Menu icons to navigate between the headings groups:

Figure 2. Settings apps in Windows 11



Description

A find a setting search bar is on the top left. The menu below has the options system, Bluetooth and devices, network and internet, personalization, apps, accounts, time and language, gaming, accessibility, privacy and security, and windows update. The Laptop name is displayed as vivo book underscore ASUSLLaptop. The options below include,

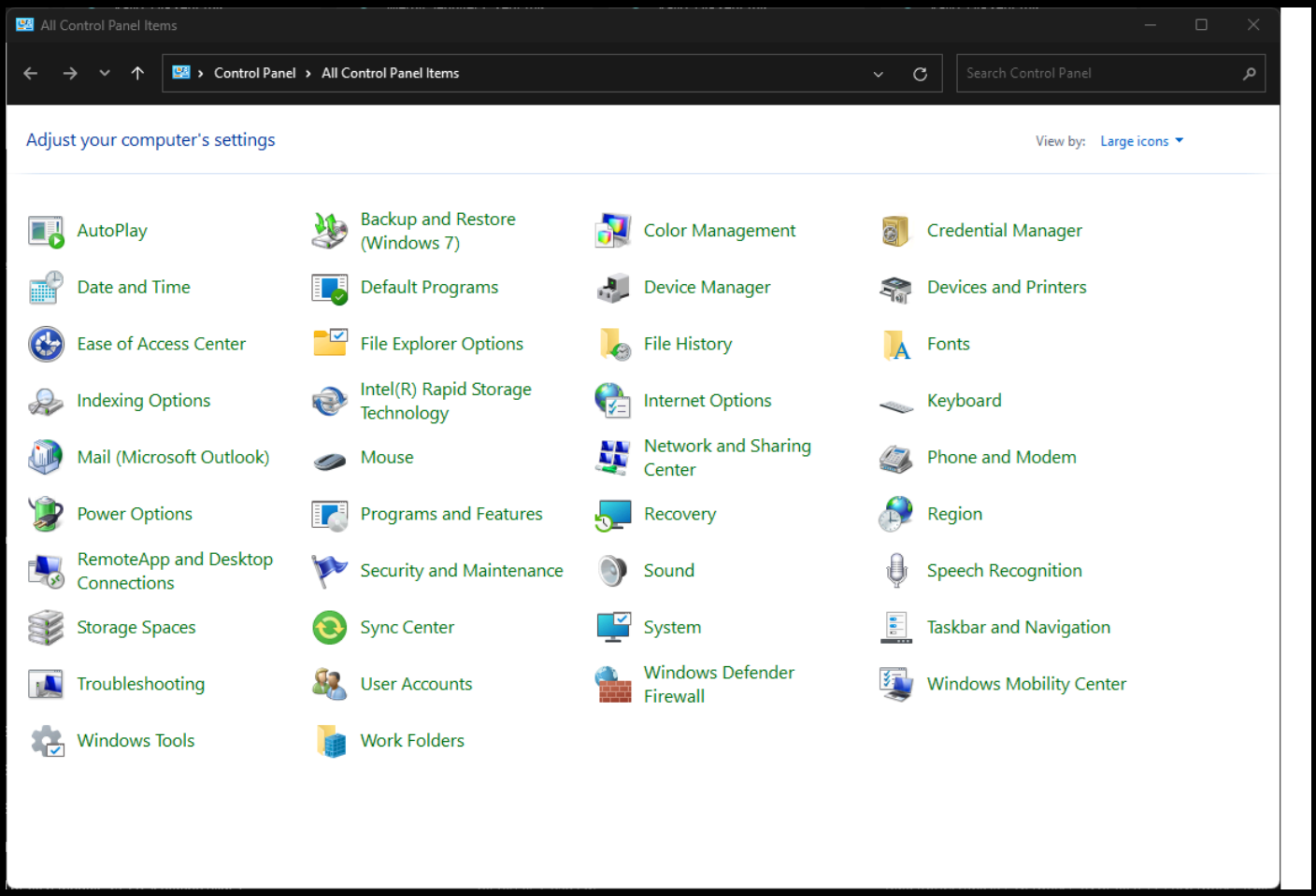
view benefits of Microsoft 365, manage One Drive, and windows update is last checked: 31 minutes ago. The other options below are as follows: Display: Monitors, brightness, night light, display profile Sound: Volume levels, output, input, sound devices Notifications: Alerts from apps and system Focus assist: Notifications, automatic rules Power and Battery: Sleep, battery usage, battery saver Storage: Storage space, drives, configuration rules

Control Panel

Most of the standard Windows 10 and Windows 11 configuration settings can be located within Windows Settings, but not all of them. Some options are still configured via the legacy **Control Panel** interface.

Each icon in the Control Panel represents an applet used for some configuration tasks. Most applets are added by Windows, but some software applications, such as antivirus software, add their own applets.

Figure 3. Windows 11 Control Panel showing all items



Description

The options are as follows: Autoplay Backup and Restore (Window 7) Color Management Credential Manager Date and Time Default Programs Device Manager Devices and Printers Ease of Access Center File Explorer Options File

History Fonts Indexing Options Intel (R) Rapid Storage Technology Internet Options Keyboard Mail (Microsoft Outlook) Mouse Network and Sharing Center Phone and Modem Power Options Programs and Features Recovery Region RemoteApp and Desktop connections Security and Maintenance Sound Speech Recognition Storage Spaces Sync Center System Taskbar and Navigation Troubleshooting User Accounts Windows Defender Firewall Windows Mobility Center Windows Tools Work Folders

A+ Core 1 and Core 2 CertMaster Perform 15.0

12.1.4 Accounts Settings

A **user account** controls access to the computer. Each account can be assigned rights or privileges to make OS configuration changes. Accounts can also be assigned permissions on files, folders, and printers.

A user account is protected by authenticating the account owner. Authentication means that the person must provide some data that is known or held only by the account owner to gain access to the account. For example, this can be done by signing in using a username and password or using facial recognition to login to the system.

Each user account is associated with a profile. The profile contains default folders for personal documents, pictures, videos, and music. Software applications might also write configuration information to the profile.

The first user of the computer is configured as the default administrator account. An administrator account has privileges to change any aspect of the system configuration. Additional accounts are usually configured as standard users. Standard users have privileges on their profile only, rather than the whole computer.

Windows Account Settings

A Windows account can either be configured as a local-only account or linked to a **Microsoft Account**. A local account can be used to sign in on a single computer only. A Microsoft account gives access to Microsoft's cloud services and allows sign-in and syncs desktop settings and user profile data across multiple devices.

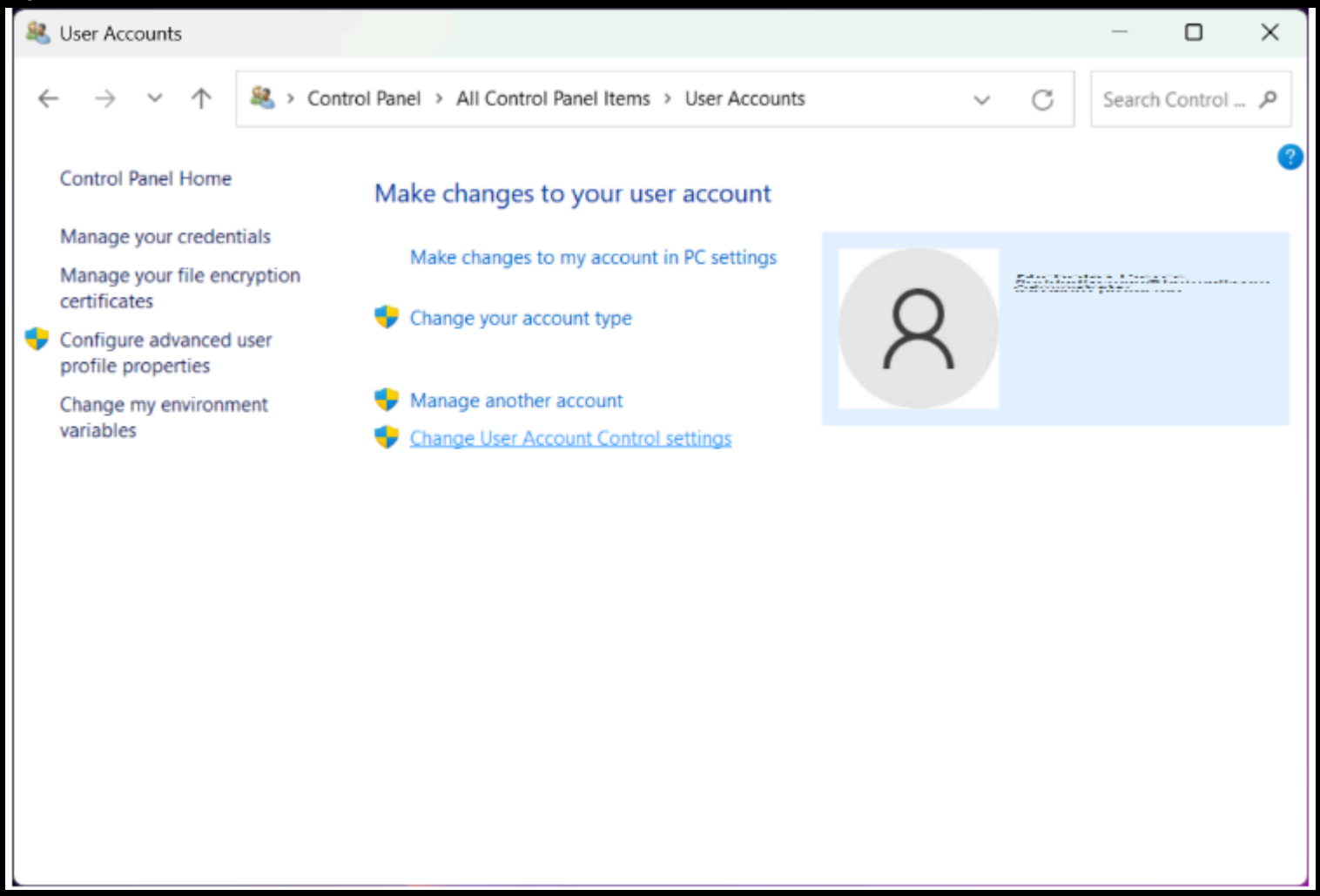
The **Account Settings** app is used for the following configuration tasks:

- **Your info**- Manage the current user account. If the account type is a Microsoft account, this links to a web portal.
- **Email & accounts**- Add sign-in credentials for other accounts, such as email or social networking, so that you can access them quickly.
- **Configure sign-in options**- Use a fingerprint reader or PIN to access the computer rather than a password. The computer can also be set to lock automatically from here.
- **Access work or school**- Join the computer to a centrally managed domain network.
- **Family and other users**- Permit other local or Microsoft accounts to log on to the computer. Generally speaking, these accounts should be configured as standard users with limited privileges.
- **Sync settings**- Use the cloud to apply the same personalization and preferences for each device that you use a Microsoft account to sign in with.

User Accounts Control Panel Applet

The **User Accounts Applet** in Control Panel is the legacy interface. Many of its functions are obfuscated or hidden and may not readily be used to add new accounts. It does provide options for adjusting the account name and changing the account privilege level between the administrator and the standard user. It can also be used to change the User Account Control (UAC) settings. UAC is a system to prevent unauthorized use of administrator privileges. At the default setting level, changing an administrative setting requires the user to confirm a prompt or input the credentials for an administrator account.

Figure 1. User Accounts Applet



Screenshot courtesy of Microsoft.

Description

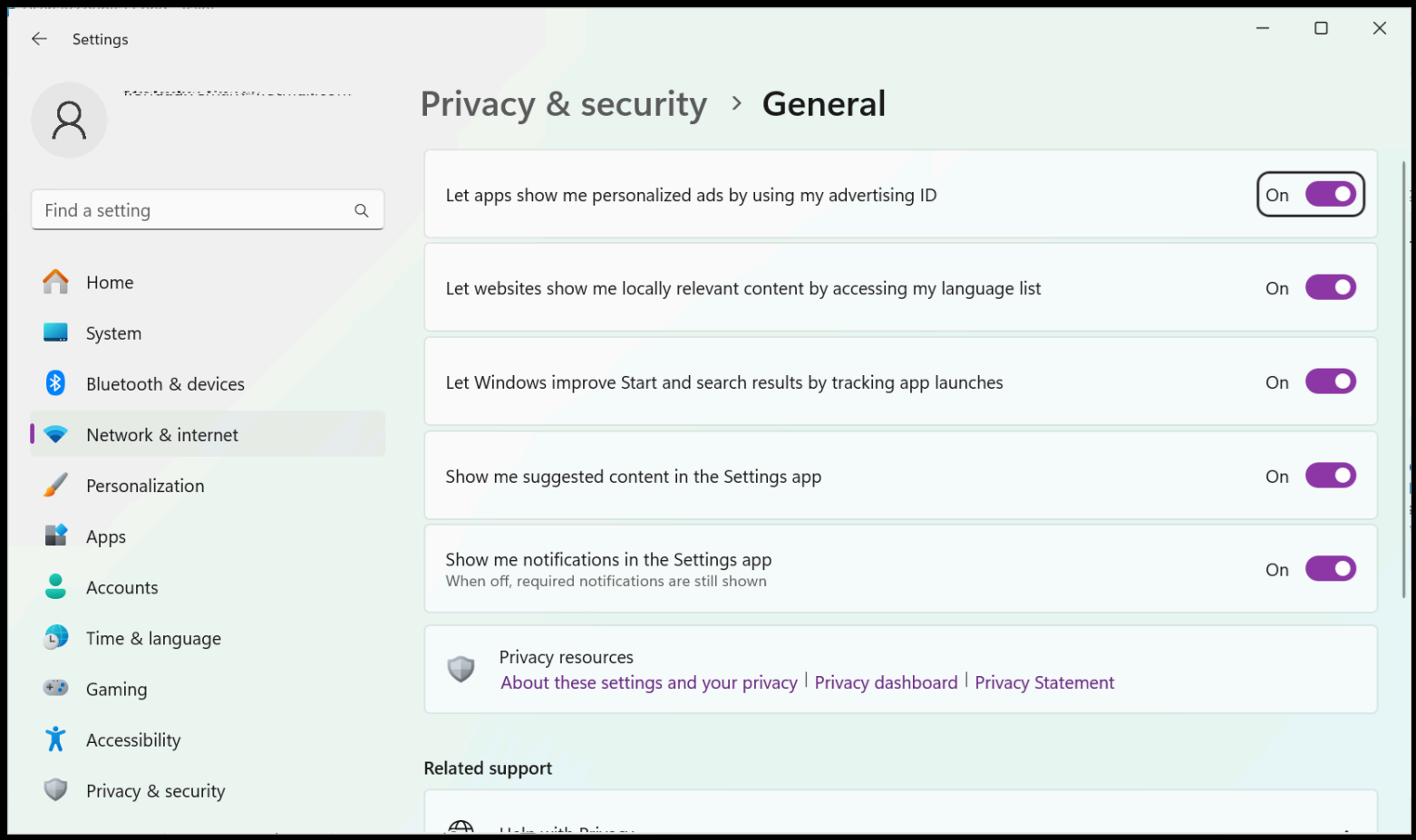
At the left are the links to control panel home, manage your credentials, manage your file encryption certificates, configure advanced user profile properties, and change my environment variables. The head at the top reads, make changes to your user account. The link below are as follows: Make changes to my account in PC settings. Change your account type. Manage another account. Change user account control settings.

12.1.6 Privacy Settings

Privacy and Security Settings govern what usage data Windows is permitted to collect and what device functions are enabled and for which apps. The security settings allow a user to change antivirus, browser, and firewall settings. There are multiple settings toggles to determine what data collection and app permissions are allowed:

- Data collection allows Microsoft to process usage telemetry. It affects use of speech and input personalization, language settings, general diagnostics, and activity history.
- App permissions allow or deny access to devices such as the location service, camera, and microphone and to user data such as contacts, calendar items, email, and files.

Figure 1. General privacy settings in Windows 11



Description

The network and internet tab on the left menu is selected. The toggles at the center are as follows: Let apps show me personalized ads by using my advertising ID. Let websites show me locally relevant content by accessing my language list. Let windows improve start and search results by tracking app launches. Show me suggested content in the settings app. Show me notifications in the settings app. Privacy resources: About these settings and your privacy. Privacy dashboard. Privacy Statement.

12.1.7 Desktop Settings

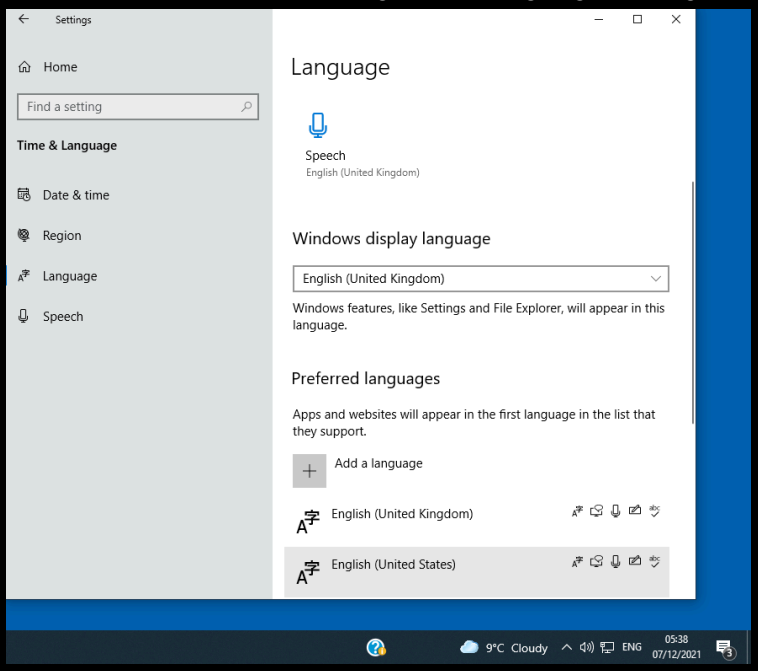
The desktop can be configured to use local settings and personalized to adjust its appearance.

Time and Language Settings

The Time and Language settings pages are used for two main purposes:

- Set the correct date/time and time zone. Keeping the PC synchronized to an accurate time source is important for processes such as authentication and backup.

- Set region options for appropriate spelling and localization, keyboard input method, and speech recognition. Optionally, multiple languages can be enabled. The active language is toggled using an icon in the notification area (or **START+SPACE**). Figure 1. Language settings



Description

The Windows display language is set to English (United Kingdom). Window features, like settings and file explorer, will appear in this language. The Preferred languages, both English (United Kingdom) and English (United States) are listed with an option to add a language at the top.

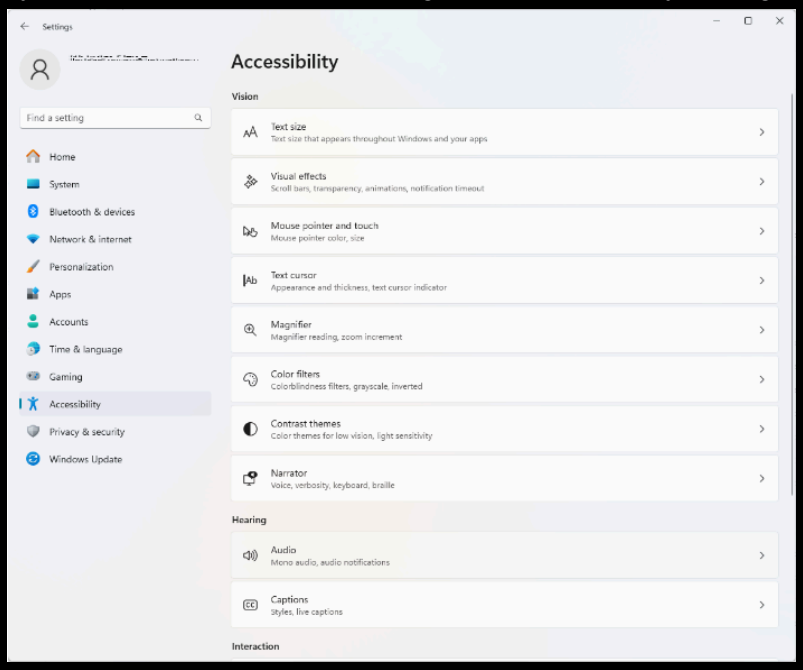
Personalization Settings

The **Personalization Settings** allow you to select and customize themes, which set the appearance of the desktop environment. Personalization and theme settings include the desktop wallpaper, screen saver, color scheme, font, and properties for the Start menu and taskbar.

12.1.9 Ease of Access Settings

Ease of Access (or Ease of Access/Accessibility) settings configure input and output options to best suit each user. There are three main settings groups:

- Vision configures options for cursor indicators, high-contrast and color-filter modes, and the Magnifier zoom tool. Additionally, the Narrator tool can be used to enable audio descriptions of the current selection.
- Hearing configures options for volume, mono sound mixing, visual notifications, and closed-captioning.
- Interaction configures options for keyboard and mouse usability. The user can also enable speech- and eye-controlled input methods. Figure 1. Accessibility settings in Windows 11



Description

The menu on the left has a field to find a setting followed by options Home, System, Bluetooth and devices, Network and internet, personalization, apps, accounts, time and language, gaming, accessibility, privacy and security, and windows update. The center features the following options categorized under the head Vision: Text Size, Visual Effects, Mouse pointer and touch, Text cursor, Magnifier, color filters, contrast themes, and narrator. The options under the head hearing are audio and captions. Another head interaction is below.

Note:

Ease of Access can be configured via Settings or via Control Panel. In Windows 11, these settings are found under the **Accessibility** heading.

A+ Core 1 and Core 2 CertMaster Perform 15.0

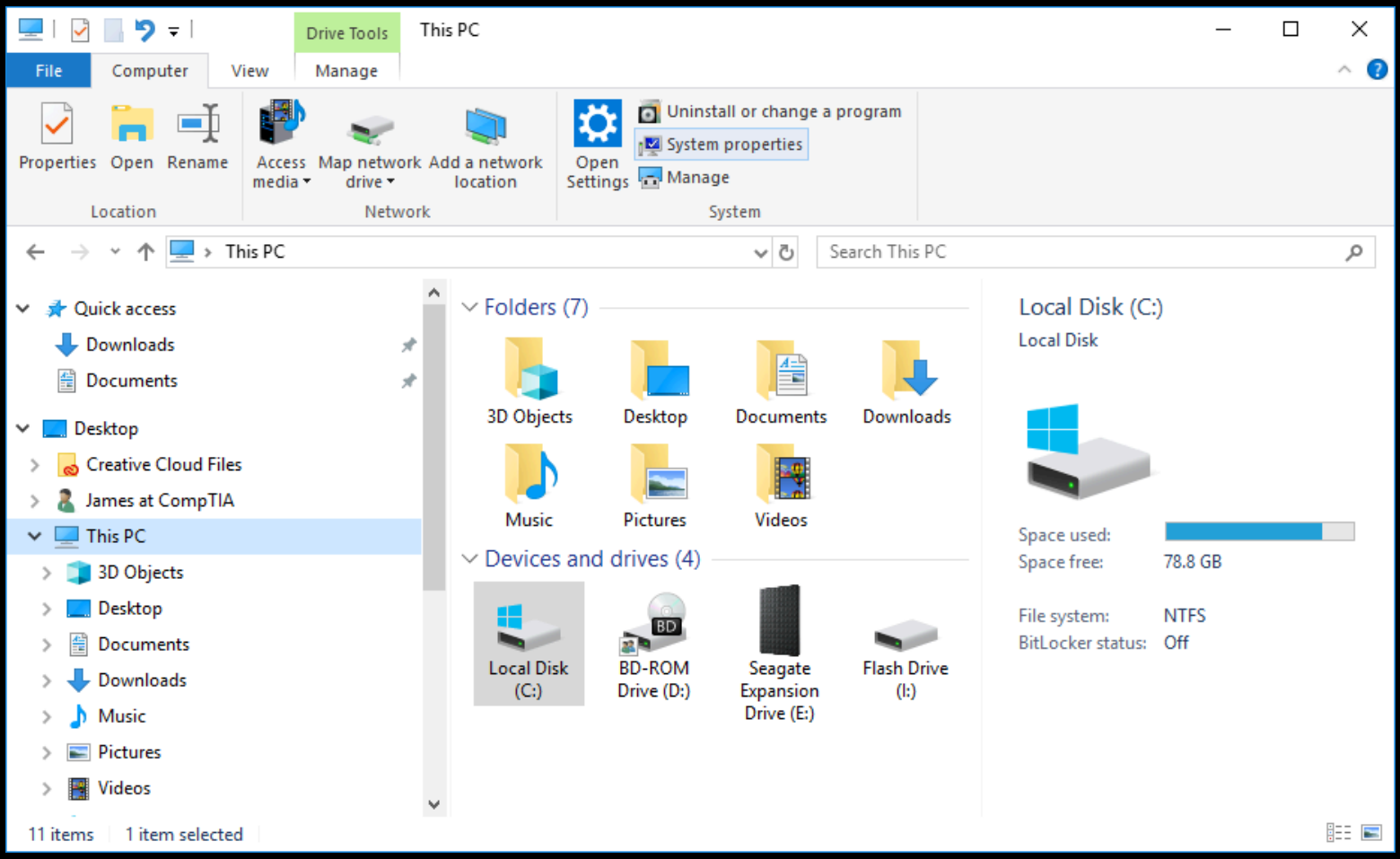
12.1.10 File Explorer

File management is a critical part of using a computer. As a computer support professional, you will often have to assist users with locating files. In Windows, file management is performed using the File Explorer app. File Explorer enables you to open, copy, move, rename, view, and delete files and folders.

Note:

File Explorer is often just referred to as "Explorer," as the process is run from the file explorer.exe .

Figure 1. File Explorer in Windows 10



Screenshot courtesy of Microsoft.

Description

The screen shows 7 folders 3D Objects, Desktop, Documents, Downloads, Music, Pictures, and Videos. On the bottom, a section for Devices and drives is visible, listing Local Disk (C), B D - ROM Drive (D), Seagate Expansion Drive (E), and Flash Drive (I). The description of the Local Disk (C) is listed on the right as follows: Space Used: More than 75 percent Space free: 78.8 G B File system: N T F S Bitlocker status: Off

System Objects

In Windows, access to data files is typically mediated by system objects. These are shown in the left-hand navigation pane in File Explorer. Some of the main system objects are:

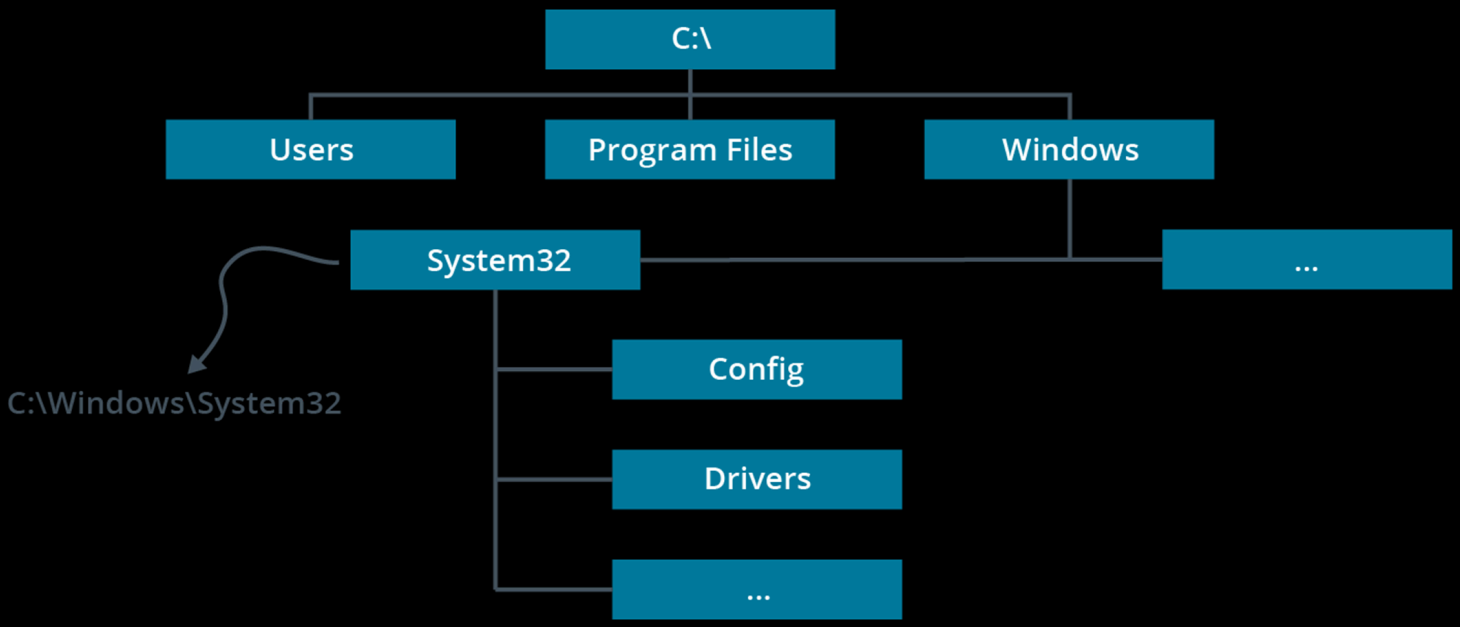
- **User account**- Contains personal data folders belonging to the signed-in account profile. For example, in the previous screenshot, the user account is listed as "James at CompTIA."
- **One Drive**- If you sign into the computer with a Microsoft account, this shows the files and folders saved to your cloud storage service on the Internet.
- **This PC**- Also contains the personal folders from the profile but also the fixed disks and removable storage drives attached to the PC.
- **Network**- Contains computers, shared folders, and shared printers available over the network.
- **Recycle Bin**- Provides an option for recovering files and folders that have been marked for deletion.

Drives and Folders

While the system objects represent logical storage areas, the actual data files are written to disk drives. Within the This PC object, drives are referred to by letters and optional labels. A "drive" can be a single physical disk or a partition on a disk, a shared network folder mapped to a drive letter, or a removable disk. By convention, the A: drive is the floppy disk (very rarely seen these days) and the C: drive is the partition on the primary fixed disk holding the Windows installation.

Every drive contains a directory called the root directory. The root directory is represented by the backslash (\ ). For example, the root directory of the C: drive is C:\. Below the root directory is a hierarchy of subdirectories, referred to in Windows as folders. Each directory can contain subfolders and files.

Figure 2. Typical Windows directory structure



Description

Key subdirectories include Users, Program Files, and Windows. Under Windows, a subdirectory System 32 is highlighted, containing further subdirectories like Config, Drivers, and others.

System Files

System files are the files that are required for the operating system to function. The root directory of a typical Windows installation normally contains the following folders to separate system files from user data files:

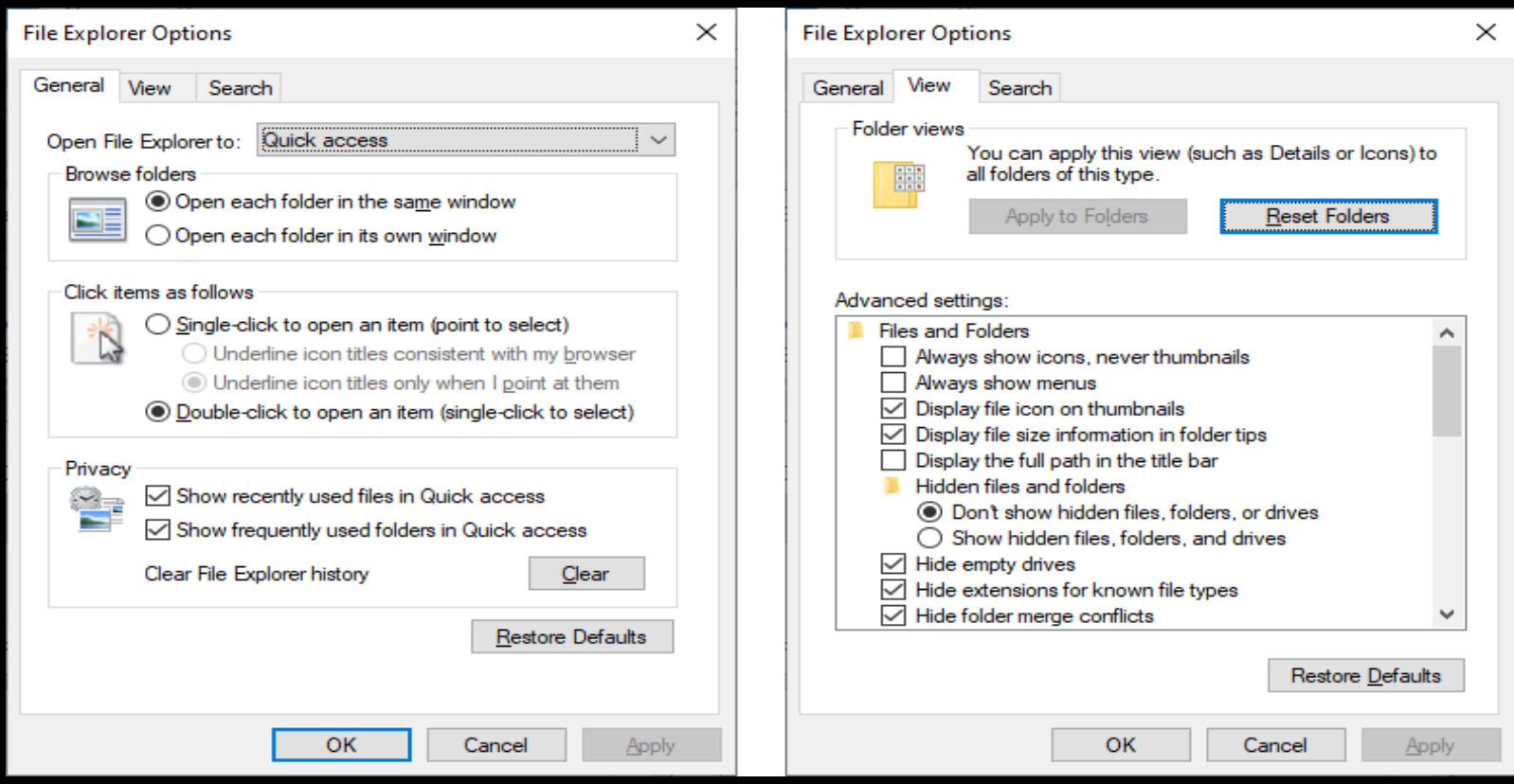
- **Windows**- The system root, containing drivers, logs, add-in applications, system and configuration files (notably the System32 subdirectory), fonts, and so on.
- **Program Files/Program Files (x86)**- Subdirectories for installed applications software. In 64-bit versions of Windows, a Program Files (x86) folder is created to store 32-bit applications.
- **Users**- Storage for users' profile settings and data. Each user has a folder named after their user account. This subfolder contains NTUSER.DAT (registry data) plus subfolders for personal data files. The profile folder also contains hidden subfolders used to store application settings and customizations, favorite links, shortcuts, and temporary files.

12.1.11 File Explorer Options

File Explorer has configurable options for view settings and file search.

The **File Explorer Options** applet in Control Panel governs how Explorer shows folders and files. On the **General** tab, you can set options for the layout of Explorer windows and switch between the single-click and double-click styles of opening shortcuts, among other options.

Figure 1. General and view configuration settings in the File Explorer Options dialog



Description

Left Panel: The General tab with options to open File Explorer to Quick Access. The radio buttons under the head Browse folders are open each folder in the same window and open each folder in its own window. The radio buttons under the head click items as follows are single click to open an item (point to select) and double-click to open an item (single-click to select). The radio buttons under the head privacy are show recently used files in Quick access and Show frequently used folders in Quick access.

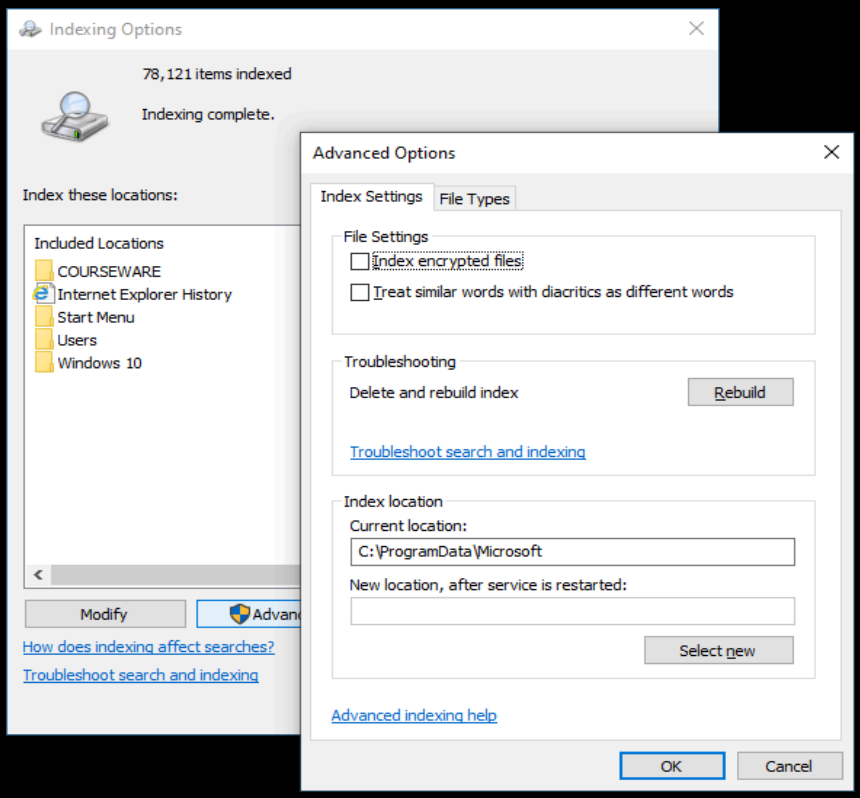
On the **View** tab, among many other options, you can configure the following settings:

- **Hide extensions** for known file types- Windows files are identified by a three- or four-character extension following the final period in the file name. The file extension can be used to associate a file type with a software application. Overtyping the file extension (when renaming a file) can make it difficult to open, so extensions are normally hidden from view.
- **Hidden files and folders**- A file or folder can be marked as "Hidden" through its file attributes. Files marked as hidden are not shown by default but can be revealed by setting the "Show hidden files, folders, and drives" option.
- **Hide protected operating system files**- This configures files marked with the System attribute as hidden. It is worth noting that in Windows, File/Resource Protection prevents users (even administrative users) from deleting these files anyway.
- Other Options- Default folder/item view, search options, and search behavior settings can also be modified here.

12.1.12 Indexing Options

You can configure file search behavior on the **Search** tab of the File Explorer Options dialog. Search is also governed by settings configured in the **Indexing Options** applet. This allows you to define indexed locations and rebuild the index. Indexed locations can include both folders and email data stores. A corrupted index is a common cause of search problems.

Figure 1. Indexing Options dialogs.



Screenshot courtesy of Microsoft.

Description

The text reads, 78,121 items indexed. Indexing complete. Index these locations: Included locations are COURSEWARE, Internet Explorer History, Start Menu, Users, and Window 10. Modify and Advanced buttons are at the bottom. How does indexing affect searches and Troubleshoot search and indexing links are located below. Another window titled Advanced Options has tabs for Index Settings and File Types. The Index Settings is selected. The

checkboxes under the head file settings are index encrypted files and treat similar words with diacritics as different words. The text under the head troubleshooting is delete and rebuild index. A rebuild button is on the right. Below is a link to troubleshoot search and indexing. The head index location has fields for current location and new location, after service is restarted. A select new button is at the bottom. An advanced indexing help is below it and ok and cancel buttons are below.

12.2 Windows System Settings

Core 2 Exam Objectives Covered

- 1.6 Given a scenario, configure Microsoft Windows settings.

While most users will find default settings sufficient for their use of the Windows OS, some users may wish to customize how their system functions in their own unique environment. For example, a personal home user may be fine with the automatic updates provided by Microsoft for the OS and firewall, but enterprise environments may require the auto-update feature to be turned off so that updates can be evaluated by system administrators. The Windows Defender Firewall may also be disabled and replaced by an enterprise security monitoring application. Understanding the features and settings of the Windows environment will play a role in ensuring the system functions for the end user environment.

Learning Outcomes

As you study this lesson, answer the following questions:

- What information is presented on the System Settings page?
- What is the default setting for Windows Update?
- What is the difference between the hibernate and sleep power options?
- What are the two rule sets listed in Windows Defender Firewall?
- How can you access the Administrative Tools menu in Windows?

12.2.4 Device Settings

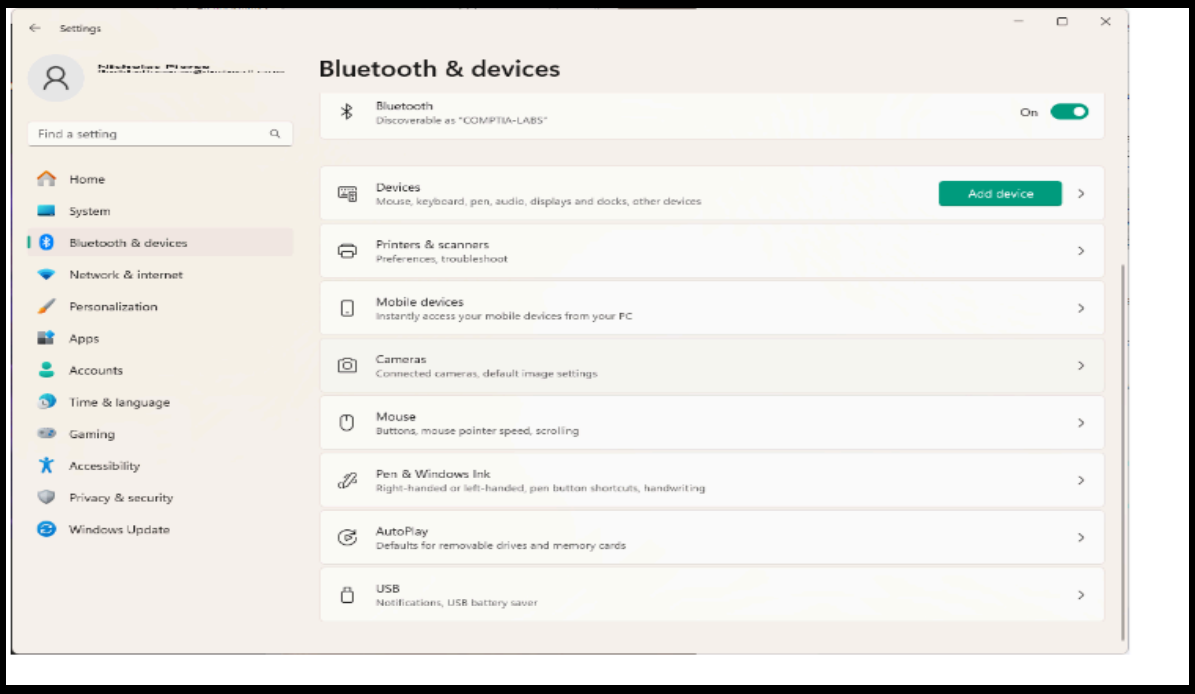
Most Windows-compatible hardware devices use Plug and Play. This means that Windows automatically detects when a new device is connected, locates drivers for it, and installs and configures it with minimal user input. In some cases, you may need to install the hardware vendor's driver before connecting the device. The vendor usually provides a setup program to accomplish this. More typically, device drivers are supplied via Windows Update.

Note:

When using a 64-bit edition of Windows, you must obtain 64-bit device drivers. 32-bit drivers will not work.

Several interfaces are used to perform hardware device configuration and management:

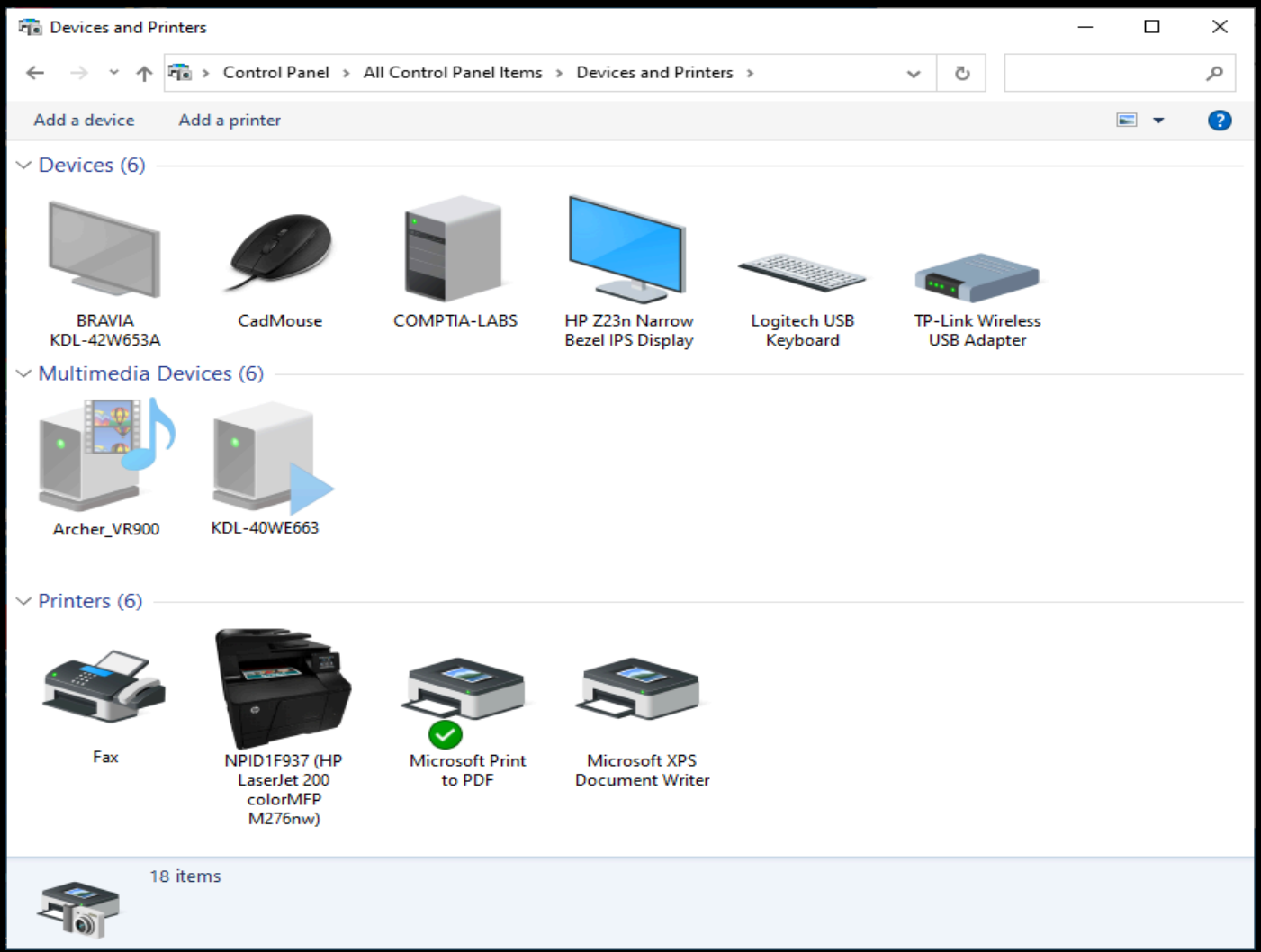
- The System settings pages contain options for configuring **Display** and **Sound** devices.
- The **Bluetooth & Devices** settings pages contain options for input devices (mice, keyboards, and touch), print/scan devices, and adding and managing other peripherals attached over Bluetooth or USB. Figure 1. Devices settings in Windows 11



Description
The menu on the left has a field to find a setting followed by options Home, System, Bluetooth and devices,

Network and internet, personalization, apps, accounts, time and language, gaming, accessibility, privacy and security, and windows update. The Bluetooth and devices is selected. Bluetooth is toggled on, showing a connected device like COMPTIA-LABS. Below are options for devices (along with a add device button on the right), printers and scanners, mobile devices, cameras, mouse, pen and windows link, autoplay, and USB.

- **Mobile Devices** settings allow a smartphone to be linked to the computer.
- The **Devices and Printers** applet in Control Panel provides an interface for adding devices manually and shortcuts to the configuration pages for connected devices. Figure 2. Devices and Printers applet in Control Panel



Screenshot courtesy of Microsoft.
Description
The devices are BRAVIA KDL-42W653A, CadMouse, COMPTIA-LABS, HP Z23n Narrow Bezel IPS Display, Logitech USB Keyboard, and TP-Link Wireless USB Adapter. The multimedia devices are Archer underscore VR900 and KDL-40WE663. The printers are Fax, NPID1F937 (HP LaserJet 200 colorMFP M276nw), Microsoft Print to PDF, and Microsoft XPS Document Writer.

- Device Manager provides an advanced management console interface for managing both system and peripheral devices. Device properties, details, driver settings, and events pertaining to each device can also be accessed from Device Manager.

A+ Core 1 and Core 2 CertMaster Perform 15.0

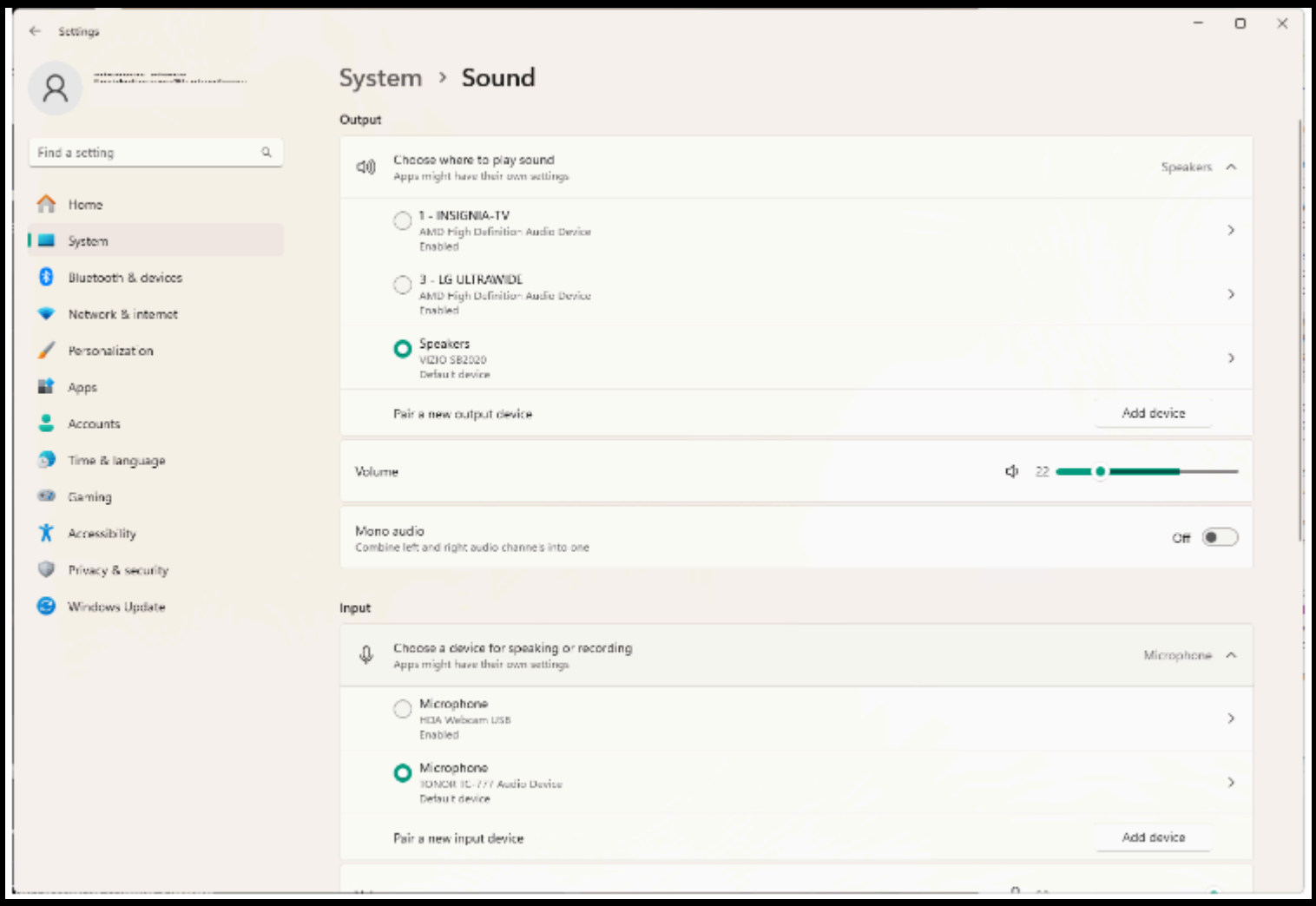
12.2.5 Display and Sound Settings

The principal **Display** configuration settings are:

- **Scale**—A large high-resolution screen can use quite small font sizes for the user interface. Scaling makes the system use proportionally larger fonts.
- **Color**—When the computer is used for graphics design, the monitor must be calibrated to ensure that colors match what the designer intends.
- **Multiple displays**—If the desktop is extended over multiple screens, the relative positions should be set correctly so that the cursor moves between them in a predictable pattern.
- **Resolution and refresh rate**—Most computers are now used with TFT or OLED display screens. These screens are designed to be used only at their native resolution and refresh rate. Windows should detect this and configure itself appropriately, but they can be manually adjusted if necessary.

Use the **Sound Applet** in Settings or in Control Panel to choose input (microphone) and output (headphones/speakers) devices and to set and test audio levels.

Figure 1. Settings for output and input audio devices



Description

The menu on the left has a field to find a setting followed by options Home, System, Bluetooth and devices, Network and internet, personalization, apps, accounts, time and language, gaming, accessibility, privacy and security, and windows update. The system is selected. The output section reads, choose where to play sound. The three options are listed below. A bar to adjust the volume is below the output section. The input section reads, choose a device for speaking or recording. The two options are listed below.

12.2.6 Power Options

Power management allows Windows to selectively reduce or turn off the power supplied to hardware components. The computer can be configured to enter a power-saving mode automatically; for example, if there is no use of an input device for a set period. This is important to avoid wasting energy when the computer is on but not being used and to maximize run-time when on battery power. The user can also put the computer into a power-saving state rather than shutting down.

The Advanced Configuration and Power Interface (ACPI) specification is designed to ensure software and hardware compatibility for different power-saving modes. There are several levels of ACPI power mode, starting with S0 (powered on) and ending with S5 (soft power off) and G3 (mechanically powered off). In between these are different kinds of power-saving modes:

- **Standby/Suspend to RAM**- Cuts power to most devices (for example, the CPU, monitor, disk drives, and peripherals) but maintains power to the memory. This is also referred to as ACPI modes S1–S3.
- **Hibernate/Suspend to Disk**- Saves any open but unsaved file data in memory to disk (as hiberfil.sys in the root of the boot volume) and then turns the computer off. This is also referred to as ACPI mode S4.

In Windows, these ACPI modes are implemented as the **Sleep**, hybrid sleep, and modern standby modes:

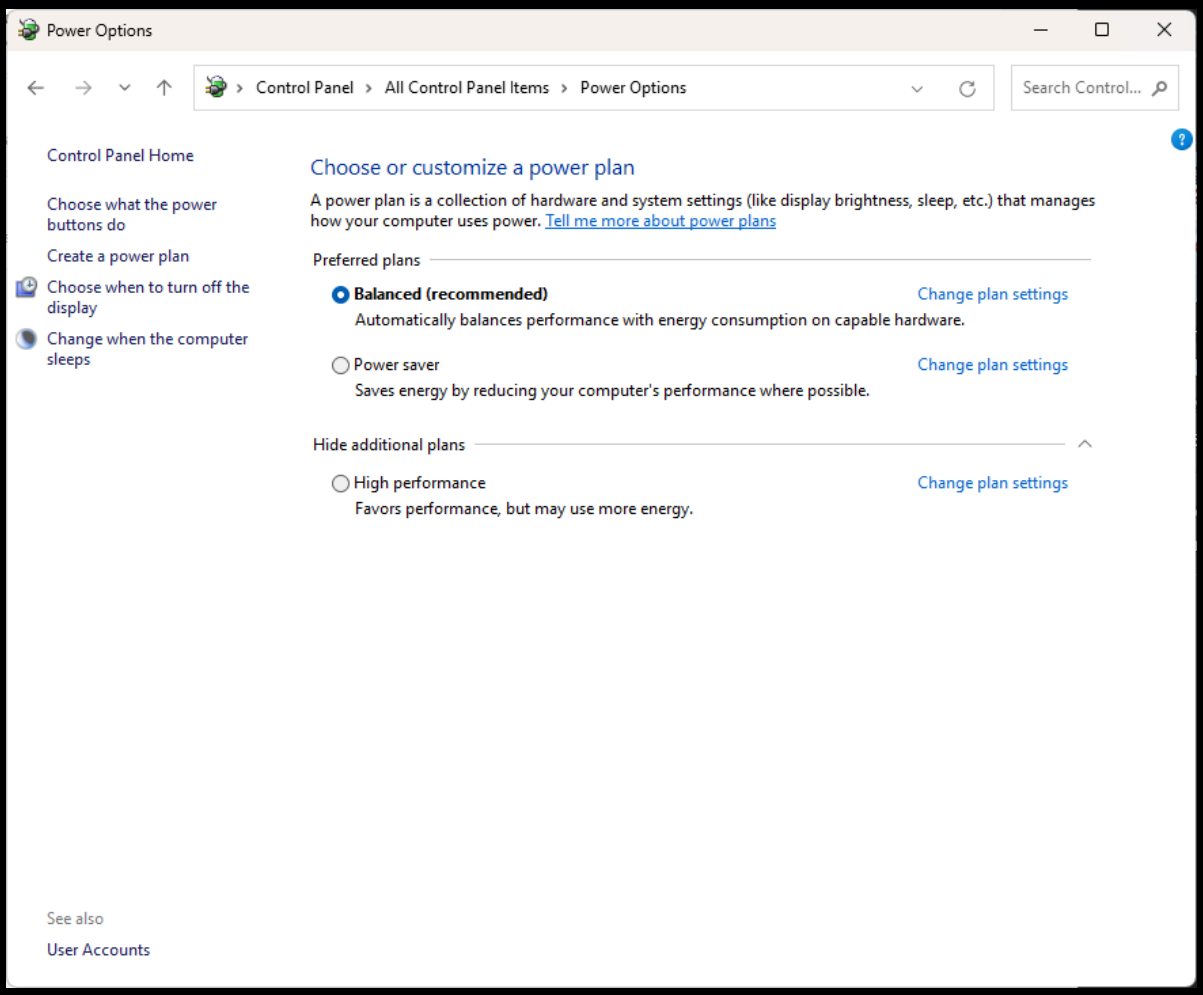
- A laptop goes into the standby state as normal; if running on battery power, it will switch from standby to hibernate before the battery runs down.
- A desktop creates a hibernation file and then goes into the standby state. This is referred to as hybrid sleep mode. It can also be configured to switch to the full hibernation state after a defined period.
- Modern Standby utilizes a device's ability to function in an S0 low-power idle mode to maintain network connectivity without consuming too much energy.

You can also set sleep timers for an individual component, such as the display or hard drive so that it enters a power-saving state if it goes unused for a defined period.

The **System Power** settings provide an interface for configuring timers for turning off the screen and putting the computer to sleep when no user activity is detected. The Control Panel **Power Options** applet exposes additional configuration options.

One such option is defining what pressing the power button and/or closing the lid of a laptop should perform (shut down, sleep, or hibernate, for instance).

Figure 1. Configuring power settings via the Power Options applet in Control Panel



Screenshot courtesy of Microsoft.

Description

The head choose or customize a power plan is followed by the text, A power plan is a collection of hardware and system settings (like display, brightness, sleep, etc) that manages how your computer uses power. A link reads, tell me more about power plans. The head preferred plans has subheads, balanced (recommended) and power saver. The head, hide additional plans has a subhead high performance. A link to change plan settings in on the right of each plan.

You can also use the Power Options applet to enable or disable **Fast Startup**. This uses the hibernation file to instantly restore the previous system RAM contents and make the computer ready for input more quickly than with the traditional hibernate option.

If necessary, a more detailed **power plan** can be configured via Power Options. A power plan enables the user to switch between different sets of preconfigured options easily. Advanced power plan settings allow you to configure a very wide range of options, including CPU states, search and indexing behavior, display brightness, and so on. You can also enable **Universal Serial Bus (USB) selective suspend** to turn off power to peripheral devices.

12.2.8 Apps, Programs, and Features

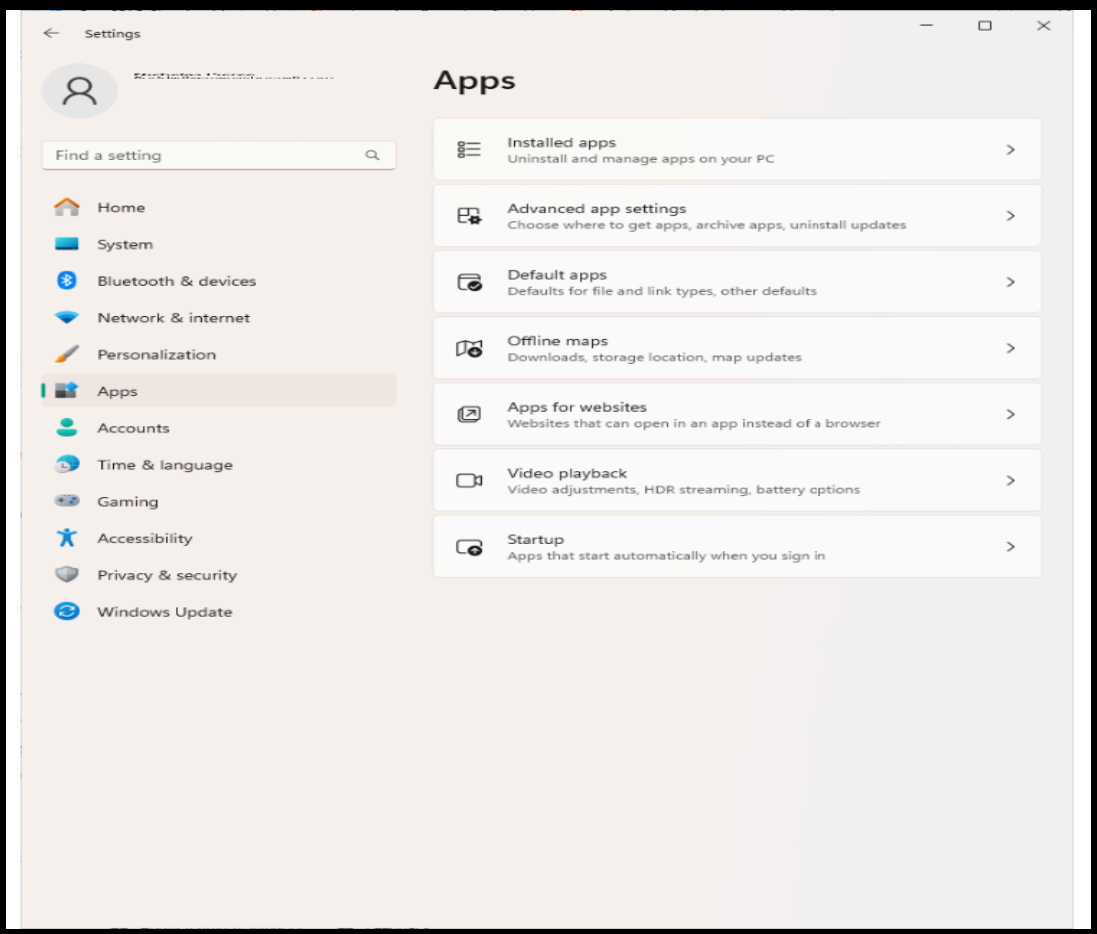
Windows supports several types of installable software:

- Windows Features are components of the operating system that can be enabled or disabled. For example, the Hyper-V virtualization platform can be installed as an optional feature in supported Windows editions.
- Store apps are installed via the Microsoft Store. Store apps can be transferred between any Windows device where the user signs in with that Microsoft account. Unlike desktop applications, store apps run in a restrictive sandbox. This sandbox is designed to prevent a store app from making system-wide changes and prevent a faulty store app from "crashing" the whole OS or interfering with other apps and applications. This extra level of protection means that users with only standard permissions are allowed to install store apps. Installing a store app does not require confirmation with UAC or computer administrator-level privileges.
- User-context applications can be installed in a user's AppData folder. These applications do not need administrative credentials to install, as they do not install in either the System folders or Program Files folders.
- Desktop apps are installed by running a setup program or MSI installer. These apps require administrator privileges to install.
- Windows Subsystem for Linux (WSL) allows the installation of a Linux distribution and the use of Linux applications without the use of a virtual machine or configuring dual boot options.

12.2.9 Apps Settings

In the Settings app, the **Apps Settings** group is used to view and remove installed apps and Windows Features. You can also configure which app should act as the default for opening, editing, and printing particular file types and manage which apps run at startup.

Figure 1. Apps & features settings can be used to uninstall software apps, add/remove Windows features, and set default apps



Screenshot courtesy of Microsoft.

Description

The menu on the left has a field to find a setting followed by options Home, System, Bluetooth and devices, Network and internet, personalization, apps, accounts, time and language, gaming, accessibility, privacy and security, and windows update. The apps is selected. The tabs under the head apps are as follows: Installed Apps, Advanced app settings, Default apps, Offline maps, Apps for websites, Video playback, and Startup.

Note:

To uninstall a program successfully, you should exit any applications or files that might lock files installed by the application, or the PC will need to be restarted. You may also need to disable antivirus software. If the uninstall program cannot remove locked files, it will normally prompt you to check its log file for details (the files and directories can then be deleted manually).

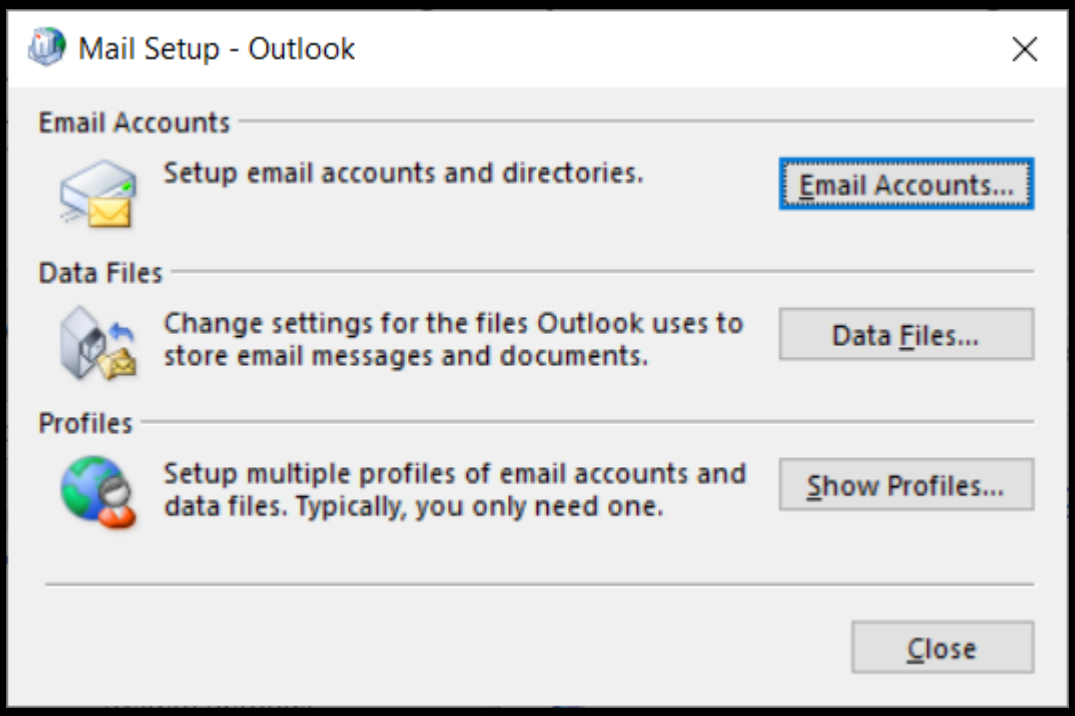
Programs and Features

The **Programs and Features** Control Panel applet is the legacy software management interface. You can use it to install and modify desktop applications and Windows Features.

Mail

The **Mail Applet** in Control Panel is added if the Microsoft Outlook client email application is installed on the computer. It can be used to add email accounts/profiles and manage the .OST and .PST data files used to cache and archive messages. Detailed configuration of the email account, sync settings, and data file selections will be managed within the Microsoft Outlook Settings menu, the Mail Applet just contains basic settings.

Figure 2. Mail applet configuration options for accounts and data files in the Microsoft Outlook email, contact, and calendar client app



Screenshot courtesy of Microsoft.

Description

The text under the head Email Accounts reads, setup email accounts and directories. A button reads, email accounts on the right. The text under the head data files reads, change settings for the files outlook uses to store email messages and documents. A button reads, data files on the right. The text under the head profile reads, setup multiple profiles of email accounts and data files. Typically, you only need one. A button reads, show profiles on the right. A close button is on the bottom right.

Gaming

The **Gaming settings** page is used to toggle game mode on and off. Game mode suspends Windows Update and dedicates resources to supporting the 3-D performance and frame rate of the active game app rather than other software or background services.

There are also options for managing captures, recording preferences, and in-game chat/broadcast features.

12.2.10 Network Settings

A Windows host can be configured with one or more types of network adapters. Adapter types include Ethernet, Wi-Fi, cellular radio, and virtual private network (VPN). Each adapter must be configured with Internet Protocol (IP) address information. Each network that an adapter is used to connect to must be assigned a trust profile, such as public, private, or domain. The network profile type determines firewall settings. A public network is configured with more restrictive firewall policies than a private or domain network.

This network connection status and adapter information is managed via various configuration utilities:

- **Network and Internet settings** is the modern settings app used to view network status, change the IP address properties of each adapter, and access other tools.
- **Network Connections (ncpa.cpl)** is a Control Panel applet for managing adapter devices, including IP address information.
- **Network and Sharing Center** is a Control Panel applet that shows status information.
- **Advanced sharing settings** is a Control Panel applet that configures network discovery (allows detection of other hosts on the network) and enables or disables file and printer sharing.

Windows Defender Firewall

Windows Defender firewall determines which processes, protocols, and hosts are allowed to communicate with the local computer over the network. The Windows Security settings app and the applet in Control Panel allow the firewall to be enabled or disabled. Complex firewall rules can be applied via the Windows Defender with Advanced Security management console.

Internet Options

The **Internet Options** Control Panel applet exposes the configuration settings for web browsers installed on the Windows system. The Security tab is used to restrict what types of potentially risky active content are allowed to run. While these settings do affect all browsers installed on the system, modern browsers such as Microsoft's Edge browser and the Chrome browser from Google, will have their own built-in settings menu also.

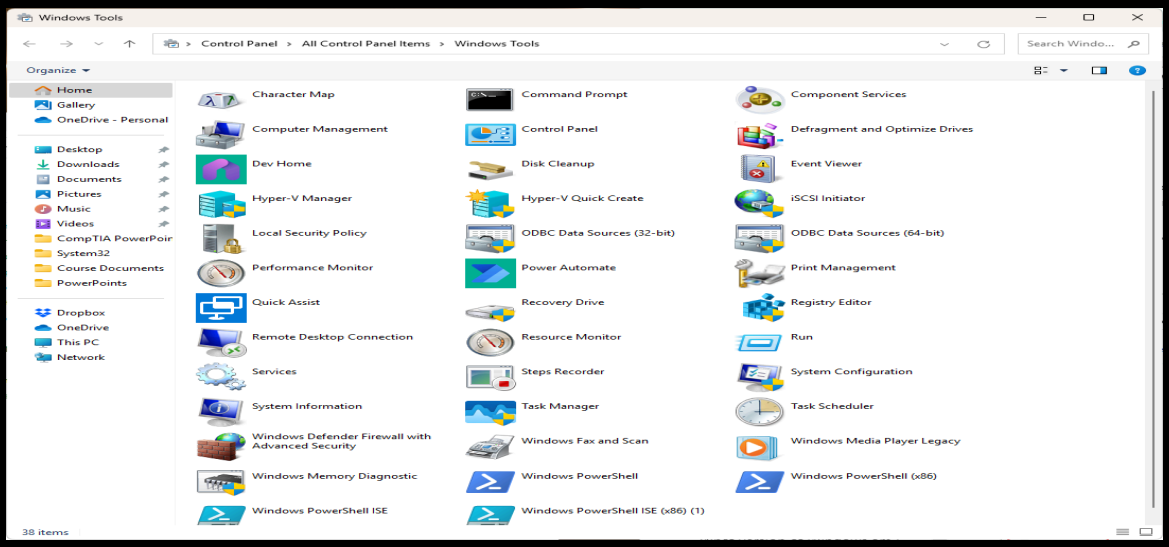
Note:

Windows network, firewall, and configuration of modern browsers, such as Microsoft Edge, Google Chrome, Apple Safari, and Mozilla Firefox, are covered in more detail later in the course.

12.2.11 Administrative Tools

Settings and most Control Panel applets provide interfaces for managing basic desktop, device, and app configuration parameters. One of the options in Control Panel is the **Administrative Tools** or **Windows Tools** shortcut. This links to a folder of shortcuts to several advanced configuration consoles.

Figure 1. Windows Tools folder Windows 11



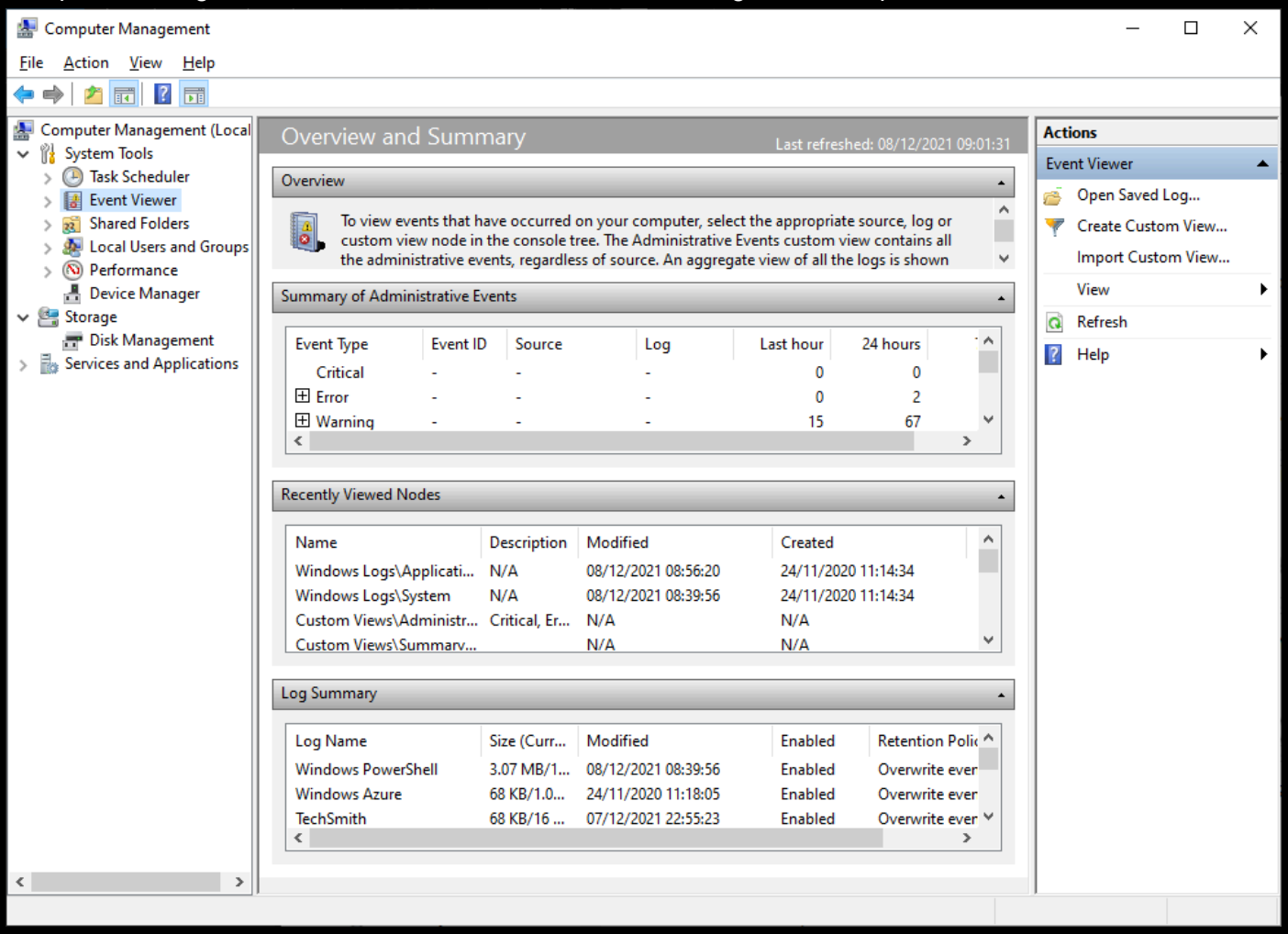
Description

The home option is selected from the menu on the left. The options are as follows: Character Map, Command Prompt, Component Services, Computer Management, Control Panel, Defragment and Optimize Drives, Dev Home, Disk Cleanup, Event Viewer, Hyper-V Manager, Hyper-V Quick Create, iSCSI Initiator, Local Security Policy, ODBC Data Sources (32 bit), ODBC Data Sources (64 bit), Performance Monitor, Power Automate, Print Management, Quick Assist, Recovery Drive, Registry Editor, Remote Desktop Connection, Resource Monitor, Run, Services, Steps Recorder, System Configuration, System Information, Task Manager, and Task Scheduler.

A Microsoft Management Console (MMC) contains one or more snap-ins that are used to modify advanced settings for a subsystem, such as disks or users. The principal consoles available via Administrative Tools are:

- **Computer Management (compmgmt.msc)**- The default management console with multiple snap-ins to schedule tasks and configure local users and groups, disks, services, devices, and so on. Figure 2. The default

Computer Management console in Windows 10 with the configuration snap-ins shown on the left.



Description

The event viewer option is selected from the menu on the left. The center is titled, overview and summary. The overview is followed by summary of administrative events, recently viewed nodes, and log summary. The actions are listed on the right. The event viewer tab is selected.

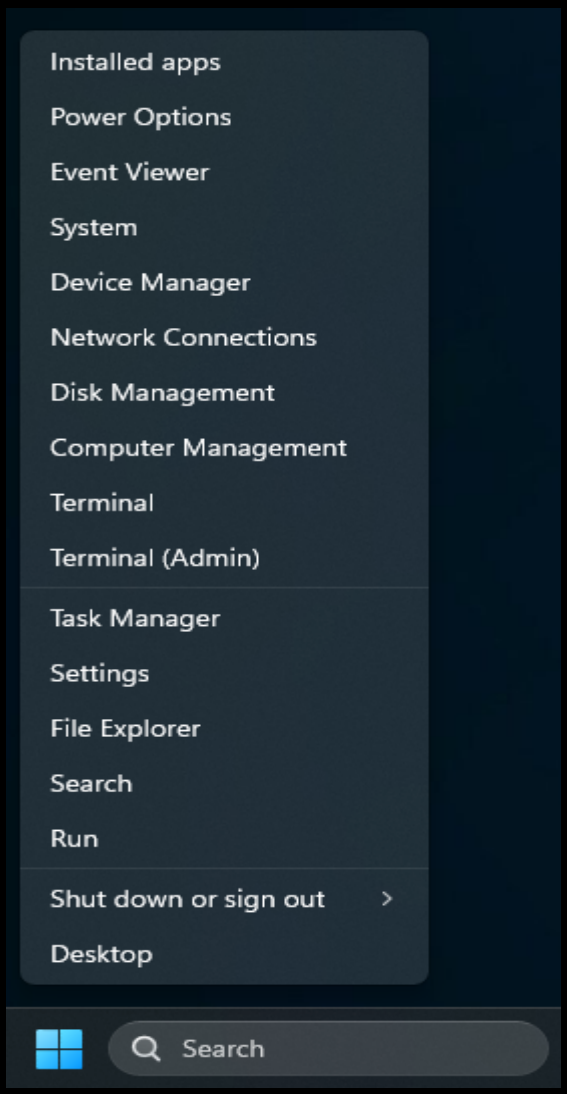
- **Defragment and Optimize Drives (dfrgui.exe)**- Maintain disk performance by optimizing file storage patterns.
- **Disk Cleanup (cleanmgr.exe)**- Regain disk capacity by deleting unwanted files.
- **Event Viewer (eventvwr.msc)**- Review system, security, and application logs.
- **Local Security Policy (secpol.msc)**- View and edit the security settings.

- **Resource Monitor (resmon.exe)** and **Performance Monitoring (perfmon.msc)**- View and log performance statistics.
- **Registry Editor (regedit.exe)**- Make manual edits to the database of Windows configuration settings.
- **Services console (services.msc)**- Start, stop, and pause processes running in the background.
- **Task Scheduler (taskschd.msc)**- Run software and scripts according to calendar or event triggers.

12.2.12 Management Shortcuts

To access the various administrative interfaces and management consoles quickly, it is worth learning shortcut methods for opening them.

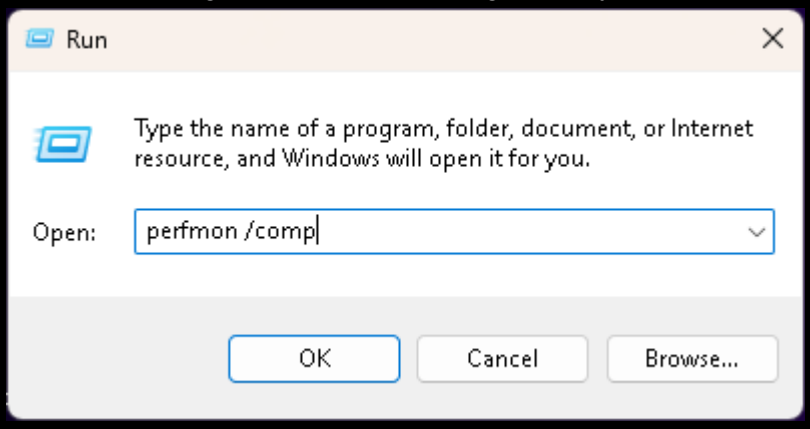
- Pressing **WINDOWS** + **X** or right-clicking the **Windows** button shows a shortcut menu with links to the main management utilities, such as Device Manager, Computer Management, Command Prompt, and Windows Terminal (PowerShell). Figure 1. Windows 11 WinX menu (right-click the Windows button)



Screenshot courtesy of Microsoft.

Description
The menu lists, installed apps, power options, event viewer, system, device manager, network connections, disk management, computer management, terminal, terminal (admin), task manager, settings, file explorer, search, run, shut down or sign out, and desktop. A search bar is given below.

- The **Instant Search** box on the Windows menu will execute programs and configuration options using simple names. Press the **WINDOWS** key, and then simply type the program file name or utility name. You can also open files or unregistered programs by typing the path to the file.
- The **Run** dialog (**WINDOWS** + **R**) can be used to execute a program with switches that modify the operation of the software. Figure 2. The Run dialog allows you to execute a command with switches



Screenshot courtesy of Microsoft.
Description
The text above reads, type the name of a program, folder, document, or internet resource, and windows will open it for you. The command perfmon slash comp is entered in the input field. Ok, Cancel, and Browse buttons are at the bottom.

The shortcut menus for system objects and notification area icons contain links to configuration tools. For example, the **Properties** item for This PC opens the System settings app, while **Manage** opens the Computer Management console.
Note:

Individual Settings app pages can be accessed from the Run dialog using uniform resource indicators such as `ms-settings:system`. Control Panel applets can be opened using commands in the form `control ncpa.cpl`.

12.3 Install and Configure Applications

Core 2 Exam Objectives Covered

- 1.10 Given a scenario, install applications according to requirements.

While the operating system provides the basic functionality and GUI for a user, the applications you choose to install on the system expand its capabilities. A new service ticket has just been assigned to you for installation of several applications necessary for the employee to complete their work tasks. The applications include the company's financial software and access to the database application. This will allow the user to query the database of completed work for the project and then utilize the financial software to invoice the customer for the work completed. There are many types of applications you will utilize for productivity and work assignments and there are others meant for entertainment, such as playing a game or watching online content. Either type of application installation will require examining not only if the application is appropriate for the user, but is supported by the system hardware.

Learning Outcomes

As you study this lesson, answer the following questions:

- What requirements are included in the listing for minimum system requirements?
- What are common application distribution methods for applications?
- What considerations should be evaluated before installing an application?
- Are there any risks involved with installation of applications? If so, what are they?

12.3.1 System Requirements for Applications

System requirements for applications refers to the PC specification required to run third-party software. The app vendor should publish the requirements as support information.

Central Processing Unit, System Memory, and Storage Requirements

Central Processing Unit (CPU) requirements refers to the performance and features of the computer's main processor. Like operating systems, software applications can be developed as **32-bit or 64-bit** software. Some apps may have both 32-bit and 64-bit versions. A 64-bit application requires a 64-bit CPU and OS platform. It cannot be installed on a 32-bit platform. 32-bit software applications can usually be installed on 64-bit platforms, however.

Some applications will define minimum requirements for the CPU generation, clock speed, or number of cores. An application may also require a particular CPU feature, such as hardware-assisted virtualization or a trusted platform module (TPM).

Note:

If a required feature is not detected, check the system setup program to make sure it hasn't just been disabled.

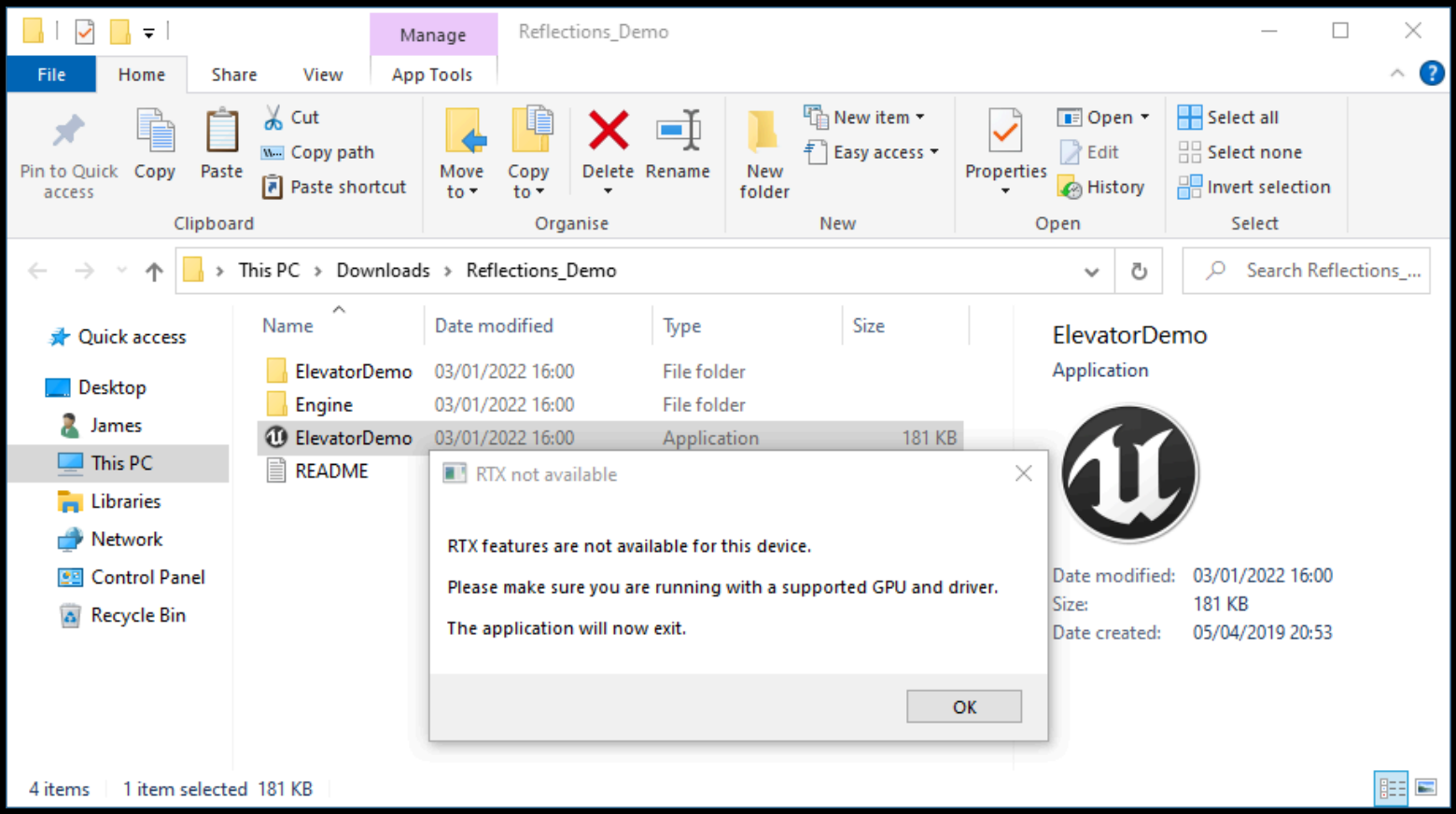
There may also be a specific **RAM requirement**. This will generally assume that no other foreground software will run at the same time. Running multiple programs simultaneously will require more RAM.

Storage requirements refers to the amount of installation space the software will take up on the fixed disk. Of course, you must also provision space for additional file creation, such as user-generated data, temporary files, and log files.

Dedicated Graphics Card Requirements

A PC's graphics subsystem can be implemented as a feature of either the CPU or the motherboard chipset. This is referred to as **integrated graphics**. A demanding application, such as graphic design software or a game, is likely to require a **dedicated graphics card** with its own **video RAM** , separate from the general system RAM.

Figure 1. This computer's graphics adapter does not meet the minimum specification, so setup cannot proceed



Screenshot courtesy of Microsoft.

Description

The error message reads, R T X features are not available for this device. Please make sure you are running with a supported G P U and driver. The application will now exit. An OK button is at the bottom.

External Hardware Token Requirements

An app might have a requirement or recommendation for using a more secure authentication method than a simple password. An **external hardware token** is a smart card or USB form factor device that stores some cryptographic user identification data. The user must present the token and supply a password, PIN, or fingerprint scan to authenticate.

12.3.2 OS Requirements for Applications

Software apps also have **OS requirements**. One of these is **application to OS compatibility**. Every software application is designed to run under a specific operating system. When purchasing, you need to make sure you select the version for your OS. If you buy the macOS version, it will not run on Windows. Additionally, a software application might not be supported for use under newer operating systems. For example, if you have been using version 1 of the Widget App on Windows 7 and you subsequently upgrade to Windows 10, the Widget App might need to be upgraded to version 2 for full compatibility.

In Linux there are different package formats, but compatibility between distros is not generally an issue. Even if an app has not been released in a compatible package for a specific distro, it can still be compiled from its source code manually.

As noted above, if the application software is **64-bit**, then the CPU and the OS must also both be 64-bit. If the application is **32-bit**, it can be installed under either a 32-bit or 64-bit platform. For example, many of the software applications available for Windows are still 32-bit. In 64-bit Windows, they run within a special application environment called WOW64 (Windows on Windows 64-bit). This environment replicates the 32-bit environment expected by the application and translates its requests into ones that can be processed by the 64-bit CPU, memory, and file subsystems.

In a 64-bit Windows environment, 32-bit application files are installed to the `Program Files (x86)` folder, while 64-bit applications are stored in `Program Files` (unless the user chooses custom installation options). Windows' 64-bit shared system files (DLLs and EXEs) are stored in `%SystemRoot%\system32`; that is, the same system folder as 32-bit versions of Windows. Files for the 32-bit versions are stored in `%SystemRoot%\syswow64`.

Note:

To view program application compatibility settings, simply locate the executable file (.exe) for the application, Right Click, and open the Properties menu. Then select the Compatibility tab.

12.3.3 Distribution Methods

An app **distribution method** is the means by which the vendor makes it available to install. Many apps are published through app stores, in which case the installation mechanics are handled automatically.

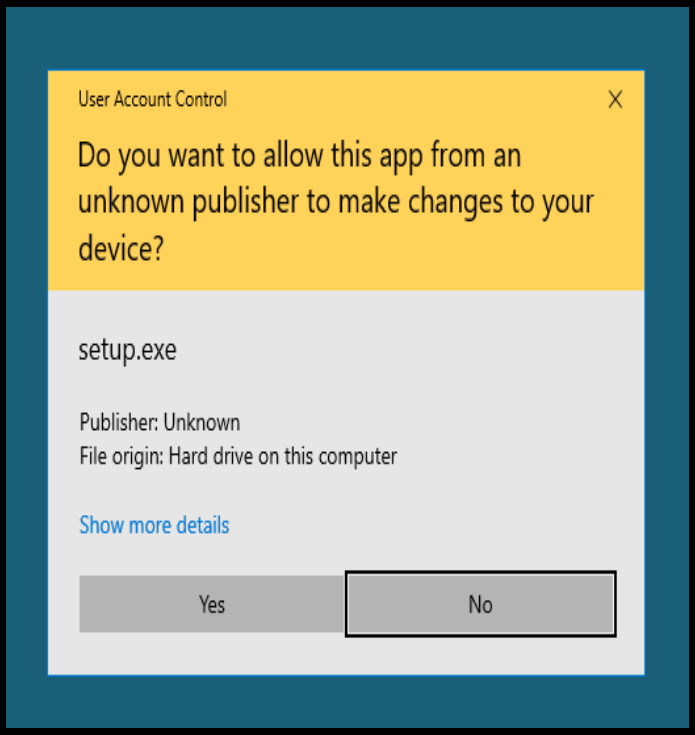
Desktop applications are installed from a setup file. In Windows, these use either .EXE or .MSI extensions. Apps for macOS can use DMG or PKG formats. Linux packages use DEB packages with the APT package manager or RPM for Dandified YUM (DNF).

The setup file packs the application's executable(s), configuration files, and media files within it. During setup, the files are extracted and copied to a directory reserved for use for application installation.

This type of setup file can be distributed on **physical media**, such as CD/DVD or a USB thumb drive, or it could be **downloaded** from the Internet. When downloading an installer from an Internet location, it is imperative to verify the authenticity and integrity of the package and to scan it for malware. Windows uses a system of digital signatures to identify valid developers and software sources. Linux software is verified by publishing a hash value of the package. After downloading, you should generate your own hash of the package and compare it to the value published by the package maintainer.

Alternatively, enterprise networks may utilize a network push of an application through an image deployment. This requires a system image of the workstation to be completed. The image file will contain all of the operating system settings and files, application settings and files, and licensing and activation settings. This image deployment deploys as an entire installation unit rather than simply installing one application at a time.

Figure 1. Unknown publisher UAC notification



Description

The question at the top reads, Do you want to allow this app from an unknown publisher to make changes to your device? The app is from an unknown publisher with file origin as hard drive on this computer. A link to show more details is at the bottom. Yes and No buttons are present below.

As an alternative to physical media, an ISO file contains the contents of an optical disc in a single file. ISO files stored on removable media or a host system are often used to install virtual machine operating systems. A mountable ISO is often used to install complex apps, such as databases, where there are many separate components and large file sizes to install. In Windows, right-click an ISO file and select Mount. The ISO file will appear in File Explorer with the next available drive letter.

12.3.4 Other Considerations

To maintain a secure and robust computing environment, impact on business, operations, and network devices from deploying new applications must be assessed and mitigated. It is important that the IT department maintains control and oversight of all third-party software installed to network hosts. Unsanctioned software and devices- shadow IT- raises substantial operational and business risks.

Impact to Business

In a corporate environment, any application that is installed must also be supported.

- **Licensing**- Commercial software must be used within the constraints of its license. This is likely to restrict either the number of devices on which the software can be installed or the number of users that can access it. Installing unlicensed software exposes a company to financial and legal penalties.
- **Support**- Software might be available with paid-for support to obtain updates, monitor and fix security issues, and provide technical assistance. Alternatively, security monitoring and user assistance could be performed by internal staff, but the impact on IT operations still needs assessing.
- **Training**- Complex apps can have a substantial and expensive user-training requirement. This can be an ongoing cost as new versions can introduce interface or feature changes that require more training or new employees require initial training. If the app is supported internally, there might also be a technical training requirement to ensure that staff can provide support and maintain the application in a secure state.

Impact to Operation

As well as the broader business impacts, a project to deploy a new application must also consider impacts to operations. Where there are hundreds of desktops, the IT department will need to use automated tools to deploy, update, and support the app.

When an organization wants to deploy an application to several desktops, it is likely to use a network-based installer. In this scenario, the setup file is simply copied to a shared folder on the network, and client computers run the setup file from the network folder. In Windows, you can use policies- Group Policy Objects (GPOs)- to set a computer to remotely install an application from a network folder without any manual intervention from an administrator. Products such as centrally managed antivirus suites often support "push" deployment tools to remotely install the client or security sensor on each desktop.

"Pushing" an installation or system image deployment over the network will cause network congestion and increase latency. Many organizations will limit over-the-network deployments to non-critical times such as overnight or on weekends to prevent disruptions during normal operations.

One advantage of using a tool such as GPO to deploy applications is that a user does not have to log on to the local client with administrator privileges. Writing/modifying permissions over folders to which the application-executable files are installed are restricted to administrator-level accounts. This prevents unauthorized modification of the computer or the installation of programs that could threaten security policies. The setup file for a deployed application can run using a service account.

To run an application, the user needs to be granted read/execute permission over the application's installation directory. Any files created using the application or custom settings/preferences specific to a particular user should be saved to the user's home folder/profile rather than the application directory.

Impact to Device and to Network

When selecting applications for installation on desktops, proper security considerations need to be made regarding potential **impacts to the device** (computer) and **to the network**. The principal threat is that of a Trojan Horse; that is, software whose true (malicious) purpose is concealed. Such malware is likely to be configured to try to steal data or provide covert remote access to the host or network once installed. A setup file could also be wittingly or unwittingly infected with a computer virus. These security issues can be mitigated by ensuring that software is only installed from trusted sources and that the installer code is digitally signed by a reputable software publisher.

As well as overt malware threats, software could impact the stability and performance of a computer or network. The software might consume more CPU and memory resources than anticipated or use an excessive amount of network bandwidth. There could be compatibility problems with other local or network applications. The software could contain unpatched vulnerabilities that could allow worm malware to propagate and crash the network. Ideally, applications should be tested in a lab environment before being deployed more widely. Research any security advisories associated with the software, and ensure that the developer has a robust approach to identifying and resolving security issues.

12.4 Cloud-Based Applications

Core 2 Exam Objectives Covered

- 1.11 Given a scenario, install and configure cloud-based productivity tools.

While many users are familiar with locally installed and run applications, many companies have begun to deploy their applications to a cloud environment. This means that the application is not running on your local hardware, but rather it is run on the cloud infrastructure of the cloud service provider. Office productivity software such as Microsoft Office® and Adobe Photoshop® are now available in a cloud-based application format. There are many benefits to deploying applications in this manner, but there are also drawbacks. Understanding how cloud-based applications work and how they should be installed and configured will ensure your organization is using the right application format for its environment.

Learning Outcomes

After you study this lesson, answer the following questions:

- What is a cloud-based application?
- How do cloud-based applications work in comparison to local installation of the application?
- What benefits and drawbacks exist with the utilization of cloud-based applications?
- What are some examples of cloud-based applications used today?

12.4.1 Email Systems

Online or cloud based email programs have existed since the dawn of the internet. From the early years to today, many personal email accounts are considered cloud-based since they are accessed and managed through an internet browser. While many enterprise organizations may still have an on premises email server using Microsoft Exchange or another email server application, some have moved their email operations into the cloud.

Examples of enterprise cloud-based email systems include Outlook Web through the **Microsoft** 365 portal and Gmail accounts from Google's Workspace environment. The email accounts are able to be accessed through their respective web portals by users, as long as they have an internet connection available. This connection allows the email system to not only be accessed from any web browser but also ensures the account syncs the email and folders across many devices. Many organizations have chosen cloud based email solutions as a way to handle synchronization and collaboration between employees.

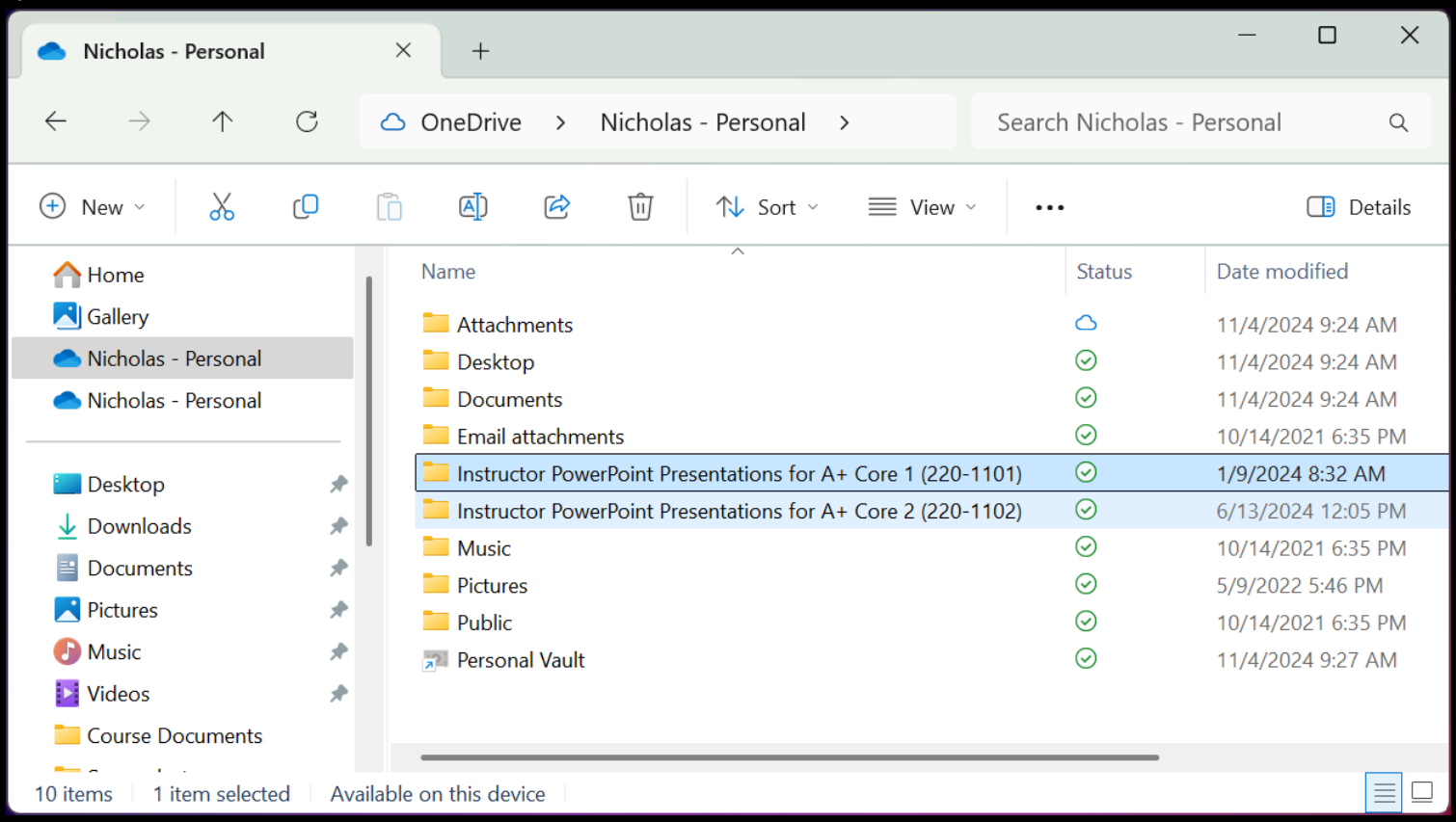
12.4.2 Storage

Cloud storage solutions are very popular today. From iCloud from Apple to Google Drive or even Microsoft's OneDrive, being able to easily store documents and files that can be accessed from any location and any device with internet access is very convenient.

Some storage providers also include a file management application that makes the access and management of the storage solution very easy. From simple file storage for your resume to personal pictures and videos, the ease of sharing and accessing these files is increased by having them located in a cloud environment.

You can also select certain files and folders from your personal computer or device to synchronize any changes to the cloud storage solution. This ensures that files are up to date and can be easily accessed from other locations. You also have the option to pause or suspend synchronization. This can be helpful when utilizing a metered connection in which there is limited bandwidth or an increased monetary cost for the network connection and data throughput.

Figure 1. Microsoft OneDrive® folder in File Explorer. Note the green check mark symbol showing the files are synchronized to the cloud. .



Description

Files are listed with sync statuses, including green checkmarks for completed synchronization and timestamps for last modifications. The files instructor PowerPoint presentations for A plus core 1 (220 - 1101) and instructor PowerPoint presentations for A plus core 2 (220 - 1102) is highlighted.

12.4.3 Collaboration Tools

Collaboration tools allow multiple users to work together simultaneously or allows users to connect remotely to work together on projects and have meetings.

Documents such as spreadsheets and presentations may require multiple users to be working within the same file. By using a cloud-based application suite such as Microsoft Office 365 or Google's Google Docs and Slides applications, users across the globe can edit and manage the same document in real-time. These applications can also track which user made edits within the document. This ensures that while users may not be located in the same location, they can still work together to accomplish their work or personal tasks easily.

Videoconferencing software such as Microsoft Teams, Slack, and Zoom provides an easy way to connect via video and audio calls. This allows users to meet, discuss, and work together as if they were sitting in the same office or conference room. Over the last several years, remote work opportunities have expanded due to the widespread use of videoconferencing software. Teams and Slack also include the ability to instant message users when asking questions or needing quick updates on the status of a task or project. Other programs may include the ability to provide reactions to emails such as a thumbs up or an OK emoji.

These additional software packages and installs may need to have permissions adjusted to access files from your local computer to allow for synchronization, access the web camera and microphone for video and audio calls, or other hardware resources to support their functionality.

Some cloud based collaboration tools are used directly in the web browser and may have an option to switch to the desktop version of the application. For example, when using Office 365 in the web portal a user can switch to their desktop installed version of the application. This is useful as there may be a feature that is available on the desktop version and not available in the cloud-based application.

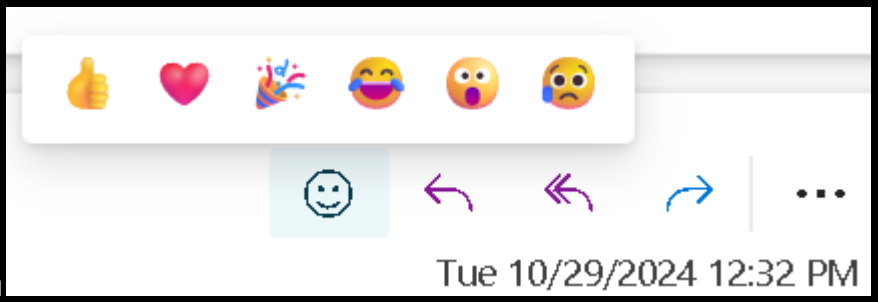


Figure 1. Outlook reactions menu

Screenshot courtesy of Microsoft.

Description

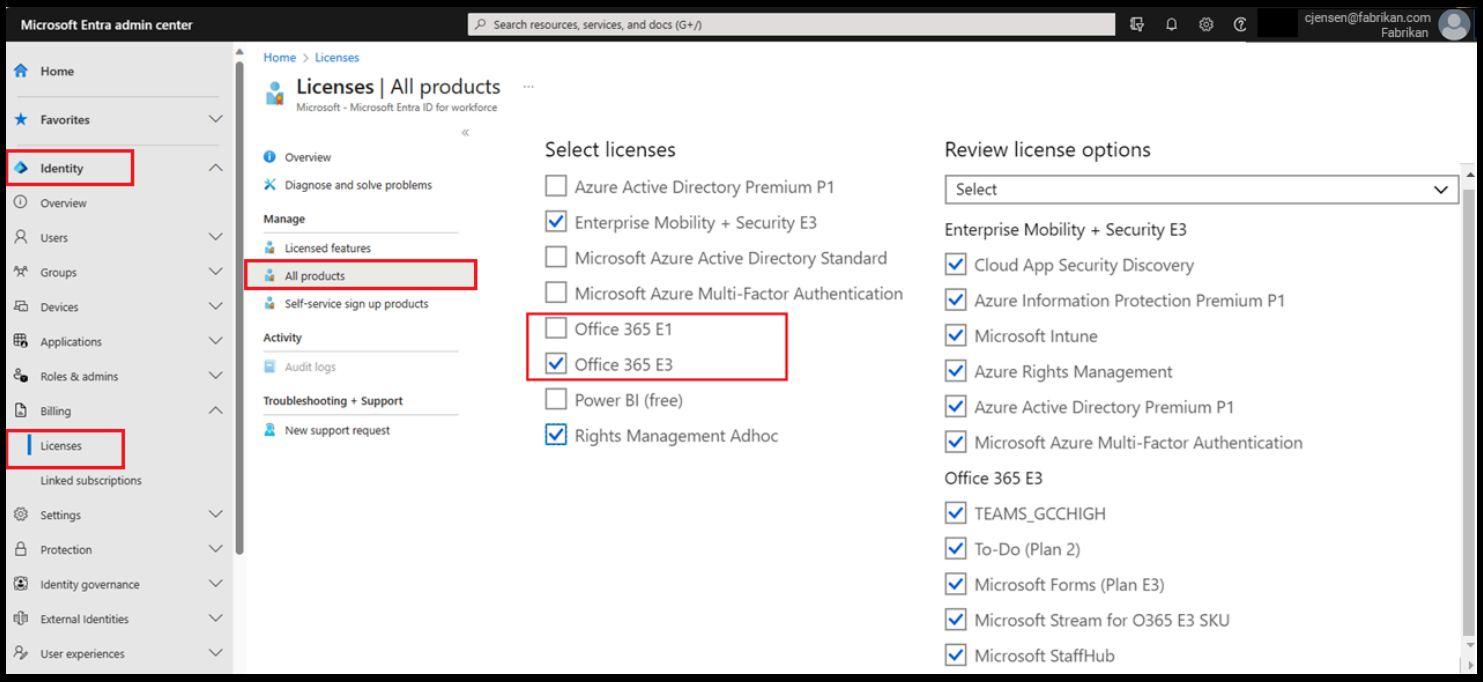
The emojis are thumbs up, heart, party, face with tears of joy, surprised face, panic face above a chat timestamp. Arrows are marked at the bottom.

12.4.4 User Licensing

Licensing of cloud-based applications may be similar to the locally installed application license agreements in that they provide the terms and conditions of the use of the software application and its limitations. For example, when you purchase a single installation, single-user license for an application, you are normally authorized to install it on one system and it is to be used by a single user. If you were to buy this type of license and then install it on several systems and/or allow multiple users to use the application, this could be considered a violation of the terms of the license. Many applications have both individual licenses and also commercial or business license terms, depending on the desired use.

When it comes to cloud-based applications, there may be some differences such as who owns the works created by the software, and that may be further complicated if you are using a cloud-based storage solution as well to store the completed works. You must read and understand the terms and conditions of any software licenses you purchase for personal or commercial use. Problems can be minimized by ensuring the appropriate license types are utilized by the organization. If the wrong license is assigned, this should be corrected by changing the license or going through an uninstall and re-installation with the correct license.

This includes the assignment of licenses to cloud applications for employees. This can easily be managed through an administrative portal such as the Microsoft Entra admin center. Figure 1. Microsoft Entra administration center license assignment window



Description

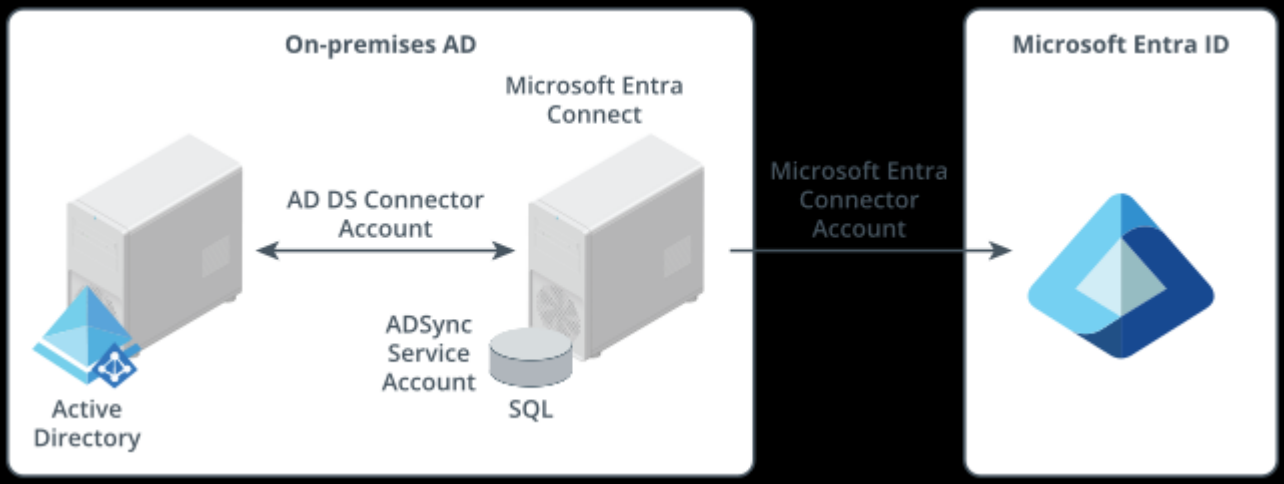
The identify and Licenses options from the menu on the left is highlighted. The center is titled, Licenses, all products. All product option on the left is selected. The lists of licenses is to its right. The Enterprise Mobility plus Security E 3, Office 365 E 3, and Rights Management Adhoc licenses options are checked in. The review license options are checked in on the right.

12.4.5 Identity Synchronization

The use of an online or cloud-based identity provider can simplify how users sign in and access resources in an enterprise environment. Having a single set of credentials to log into a cloud resource and then being able to use those same credentials to access an on-premise resource, such as their workstation, decreases the number of credentials a user must remember. It also reduces how an organization will manage the rights and permissions in the two environments. The same control policies of access to resources can be synchronized across the cloud and on-premise systems, ensuring a cohesive environment is maintained and the same permissions are applied across the entire environment.

You can also synchronize access between cloud service providers such as Google Cloud and Microsoft's Azure environment. Instead of having two sets of credentials for each service provider, synchronization of permissions and rights can easily be configured. This reduces the management and administrative burden when troubleshooting issues with permissions as well.

Figure 1. Microsoft Entra Connect synchronization



Screenshot courtesy of Microsoft.

Description

The left section represents On-premises A D and contains Active Directory connected to A D Sync Service Account, Microsoft Entra Connect, and S Q L by a double sided arrow labeled A D D S connector account.

A+ Core 1 and Core 2 CertMaster Perform 15.0

13.1.1 Device Manager

Device Manager (devmgmt.msc) lets you view and edit installed hardware properties, change configuration settings, update drivers, and remove or disable devices.

Updating and Troubleshooting Devices

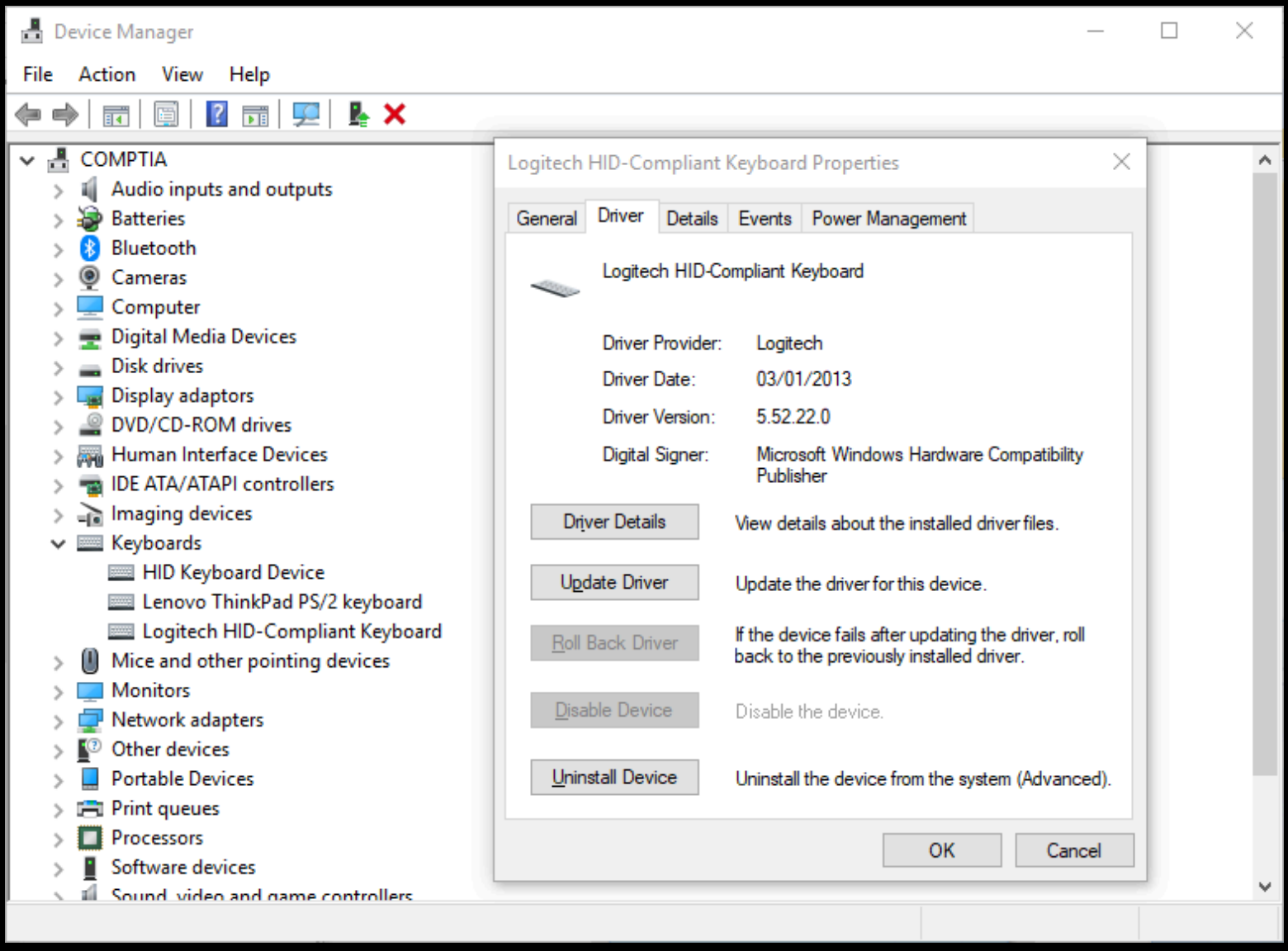
Windows may identify a device's type and function but fail to find a driver, resulting in an "Unknown Device" or a "generic" type with a yellow exclamation mark in Device Manager. If the device never worked, ensure compatibility of the device and driver with the OS. Manufacturers often provide updated drivers on their websites, which may need manual installation or come with a setup program.

Note:

Driver updates may also be available through Windows Update as optional updates.

To manually update or troubleshoot a device, locate it in Device Manager, right-click, and select **Properties**. Check the **General** tab for status information and use the **Update Driver** button on the **Drivers** tab to install a new driver.

Figure 1. Using device properties to investigate driver and roll back to a previous version



Screenshot courtesy of Microsoft.

Description

A Device Manager window on a Windows operating system. The menu on the left lists several options. A separate properties window titled Logitech H I D Compliant Keyboard Properties displays details under the Driver tab as follows: Driver Provider: Logitech Driver Date: 03/01/2013 Driver Version: 5.52.22.0 Digital Signer: Microsoft Windows Hardware Compatibility Publisher Below this, there are buttons labeled: Driver Details (to view installed driver files)

Update Driver (to update the driver) Roll Back Driver (grayed out, indicating it's unavailable) Disable Device (to disable the keyboard) Uninstall Device (to remove the keyboard driver) At the bottom, there are two buttons: O K and Cancel.

Removing, Uninstalling, and Disabling Devices

For Plug and Play, hot-swappable devices, you can remove them without uninstalling. Before removing a storage device, close any active applications, click the **Safely Remove Hardware** icon in the taskbar, and select the option to stop or eject the device.

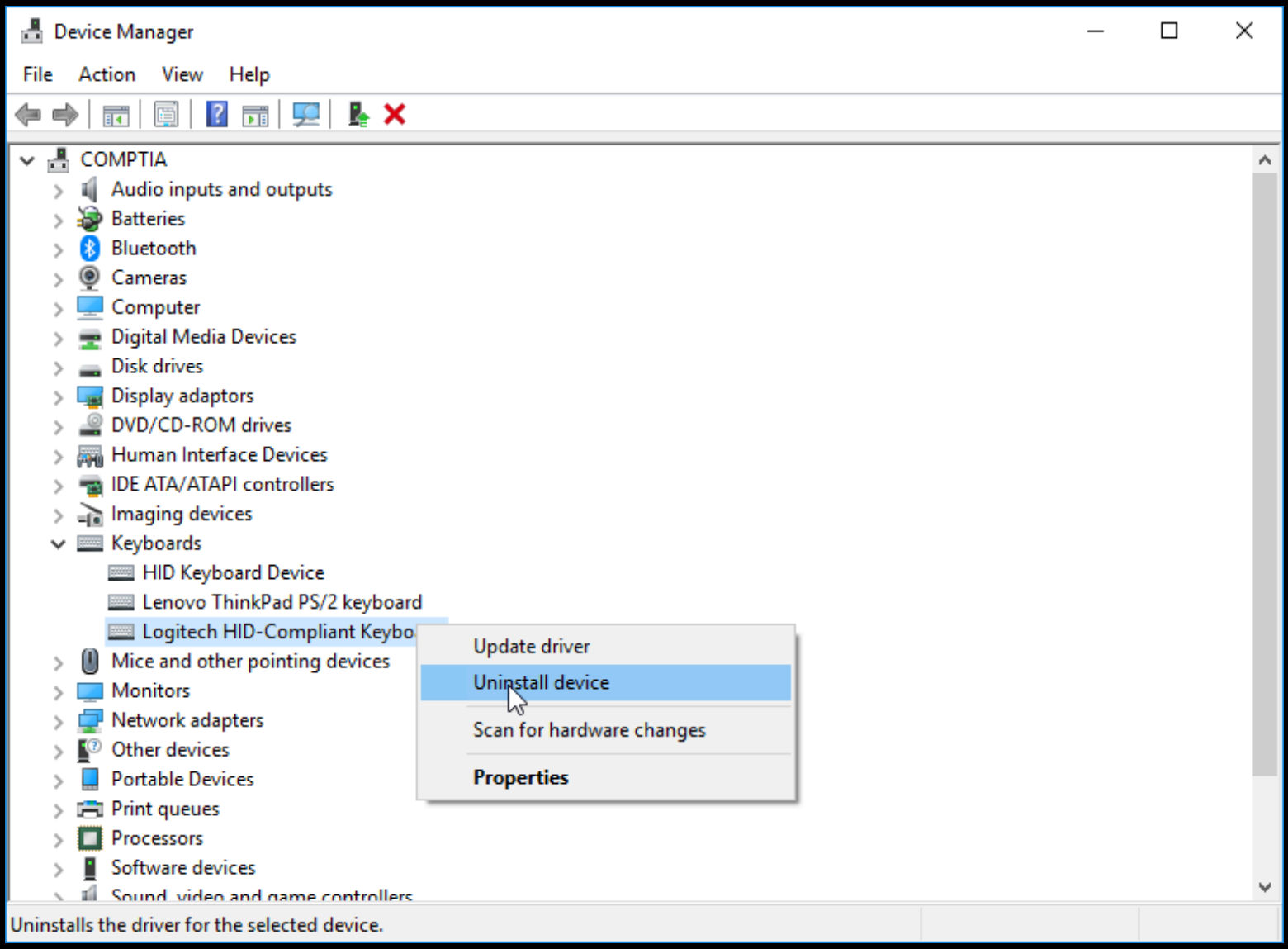
Physically removing a device keeps the driver installed for future detection. To uninstall the driver, right-click the device in Device Manager and select **Uninstall device** before unplugging.

Figure 2. Safely Remove Hardware icon



Screenshot courtesy of Microsoft.

Figure 3. Using Device Manager to uninstall a device



Screenshot courtesy of Microsoft.

Description

The Device Manager window in a Windows operating system shows a hierarchical list of device categories on the left. The Keyboards section is expanded, displaying three devices: H I D Keyboard Device Lenovo ThinkPad P S slash 2 Keyboard Logitech H I D Compliant Keyboard A right-click context menu is open for the Logitech H I D Compliant Keyboard. The menu presents the following options: Update Driver Uninstall Device (highlighted with a cursor pointing

at it) Scan for Hardware Changes Properties At the bottom of the window, a tooltip states: Uninstalls the driver for the selected device.

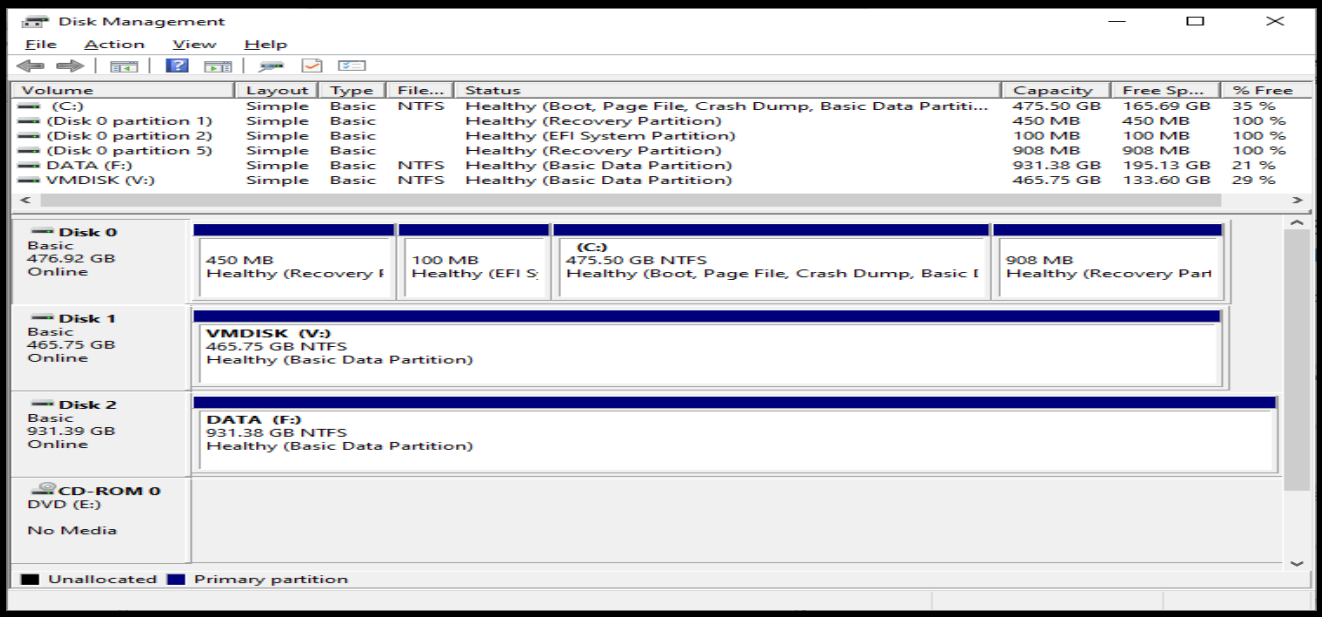
In Device Manager, you can **disable** a device if it's malfunctioning or to restrict user access while seeking a replacement. Disabling is also useful for devices that are hard to physically uninstall, enhancing system security. Disabled devices are indicated by a down arrow.

13.1.2 Disk Management Console

The disk subsystem stores all data generated by the operating system and applications. As the primary store of so much data, ensuring its reliability and performance is a critical management task.

The **Disk Management console** summarizes all fixed and removable disks—HDDs (Hard disk drives), SSDs (solid state drives), and optical drives—attached to the system. HDDs and SSDs can be divided into logical partitions, each represented as a volume in the top pane.

Figure 1. Disk Management console



Screenshot courtesy of Microsoft.

Description

The table lists the volume, layout, type, file, status, capacity, free space, and percent free for c, Disk 0 Partition 1, Disk 0 Partition 2, Disk 0 Partition 5, DATA (F), VMDISK (V).

Note:

The terms drives, volumes, and partitions can be confusing. Partitions are set up on HDDs and SSDs. A volume is a logical storage unit for the OS, often mapped 1:1 with a partition. However, volumes can also be created using a redundant drive configuration (RAID), involving multiple devices and partitions. In Windows, "drive" typically refers to a volume assigned a letter, but it can also mean a hardware storage device.

Typically, Disk 0 holds the operating system with at least three volumes:

- System Volume: Contains boot files, usually using a boot system called extensible firmware interface (EFI), and is not assigned a drive letter.
- Boot Volume: Contains operating system files, typically assigned the drive letter C:.
- Recovery partitions: Contain tools for repair or factory reset, using either the PC vendor's tool or Microsoft's WinRE, and are not assigned drive letters.

The Disk Management console supports the following disk and partitioning tasks:

- **Initializing disks**: When adding an unformatted HDD, SSD, or thumb drive, you must initialize it using master boot record (MBR) or Globally Unique ID (GUID) Partition Table (GPT) partition style for the new disk. MBR and GPT refer to the way the partition information is stored on the disk.
- **Partitioning**: Configure each disk with at least one partition. Create new partitions by right-clicking the unpartitioned space and following the wizard.
- **Formatting**: Write a file system, typically NTFS, to new partitions allowing Windows to read and write files. FAT32 may be used for small, removable drives. Reformatting existing partitions deletes all files. You can also select a volume label and allocation unit size.
  Note:

  Traditionally, the smallest storage unit is a 512-byte sector. File systems can group sectors into clusters of 2, 4, or 8 sectors. Smaller clusters use disk capacity efficiently, while larger clusters improve I/O performance for large files. Some disks use Advanced Format with 4K sectors. If supported, these can be used in native mode; otherwise, they use 512e mode. System or boot partitions cannot be formatted or deleted. *During setup, the boot partition must be NTFS, and the system partition must be FAT32.*

  .

- **Repartitioning**: Expand existing partitions when needed if there is unpartitioned space or remove/shrink partitions to free space.

The dynamic disks feature is deprecated. Windows now supports a software RAID feature called **Storage Spaces** for redundant disk configurations.

13.1.3 Disk Maintenance Tools

Of all the computer's subsystems, disk drives, and the file system probably require the most attention to keep in optimum working order. File storage is subject to three main problems:

- **Fragmentation**: On a hard disk, files ideally occupy contiguous clusters. Over time, they become fragmented across non-contiguous clusters, reducing read performance.
- **Capacity**: Typically, more files are created than deleted, reducing capacity. Performance suffers if the boot volume has less than 20% free space, and a Low Disk Space warning appears below 200 MB.
- **Damage**: HDDs are prone to physical damage, especially during power cuts, leading to corrupted files. SSDs can degrade, resulting in bad blocks, and are vulnerable to impacts, overheating, and electrical issues.

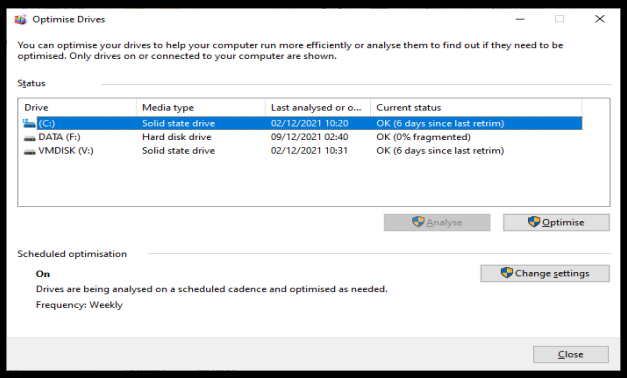
Regular use of disk maintenance tools, at least monthly and before software installations, can address these problems.

Disk Defragmenter

The **Defragment and Optimize Drives tool** enhances HDD and SSD performance:

- **HDDs**: On an HDD, defragmenting reorganizes file data into contiguous clusters, reducing the time the controller needs to seek across the disk to read a file.
- **SSDs**: On an SSD, data is stored in blocks managed by the drive controller, not the OS. The controller uses wear-leveling routines to reduce cell degradation. The optimizer tool runs TRIM operations, allowing the controller to mark OS-deletable data as writable. If the SSD holds the OS and Volume Shadow Copy is enabled, the optimizer may also perform defragmentation.

Figure 1. Optimize Drives (Defragmenter) in Windows 11



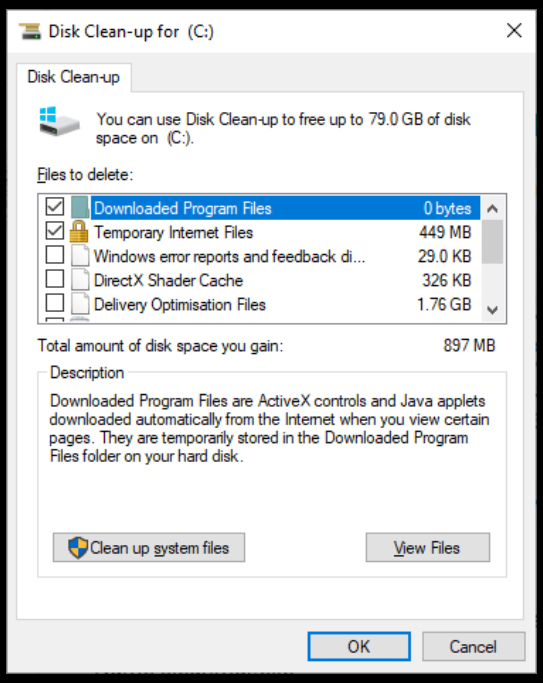
The text above reads, you can optimize your drives to help your computer run more efficiently or analyze them to find out if they need to be optimized. Only drives on or connected to your computer are shown. A table under the head status lists the drive, media type, last analyzed, and current status. An analyze and optimize button is on the bottom right. The scheduled optimization is on. A change settings button is on the right above the close button.

Windows uses Task Scheduler to automatically run the disk optimizer. Regularly check for any issues, such as unsuccessful runs.

Disk Clean-up

The **Disk Clean-up** tool identifies files safe for deletion to free up space, including those in the Recycle Bin and temporary files. Running it in administrator mode with **the Clean up system files** option reclaims space from caches like Windows Update and Defender.

Figure 2. Disk Clean-up utility



Screenshot courtesy of Microsoft.

Description

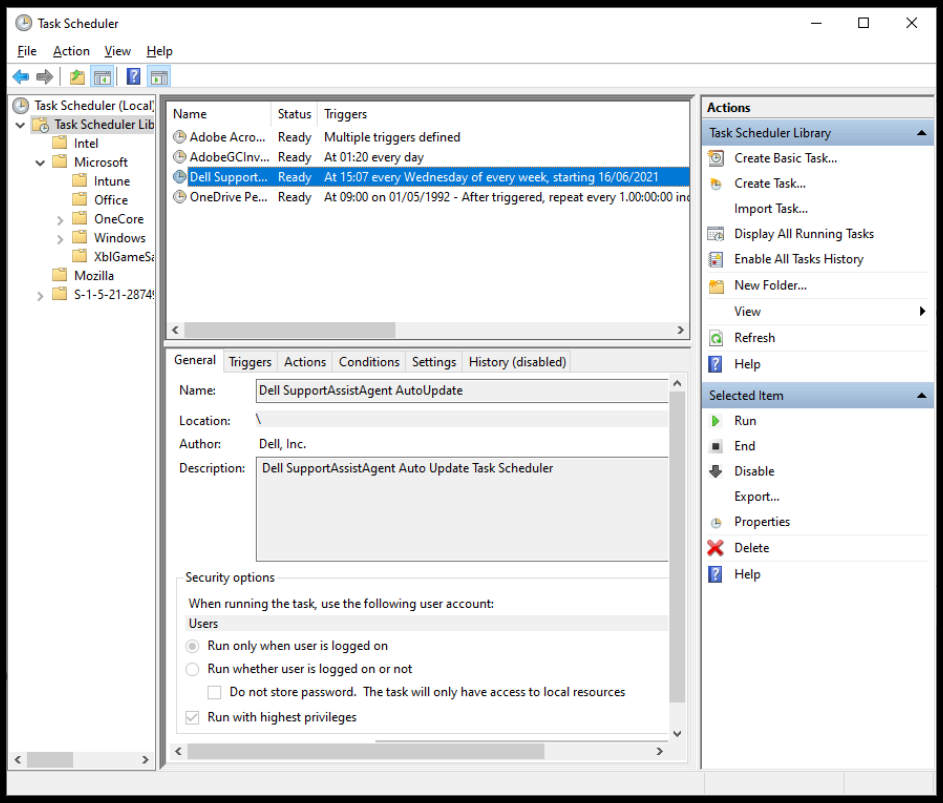
The text above reads, you can use Disk Clean Up to free up to 79.0 G B of disk space on C. The files to delete are listed below. The total amount of disk space you gain is 897 M B. The description is given below along with a clean up system files and a view files button. Ok and cancel button is at the bottom.

13.1.5 Task Scheduler

The **Task Scheduler** automates commands and scripts, with many Windows processes having predefined schedules. Tasks can be set to run once at a future date/time or on a recurring schedule. They can involve simple applications (including switches, if necessary), batch files, or scripts. Key features include:

- Triggers: Tasks can be triggered by events, such as user sign-in or the machine waking from sleep, not just by calendar dates/times.
- Multiple Actions: Each task can include multiple actions for complex automation.
- Logging: All task activity is logged so you can investigate failures.
- Organization: Tasks can be organized into folders for better management.

Figure 1. Task Scheduler showing a Dell Support auto-update task configured to run each week.



Description

The Task Scheduler Library is selected from the menu on the left. The main panel displays a list of tasks with columns for name, status, and triggers. The lower panel lists the general settings. The tab lists the name, location, author, and description. It further lists the security options. Task Scheduler Library and selected item are listed on the right.

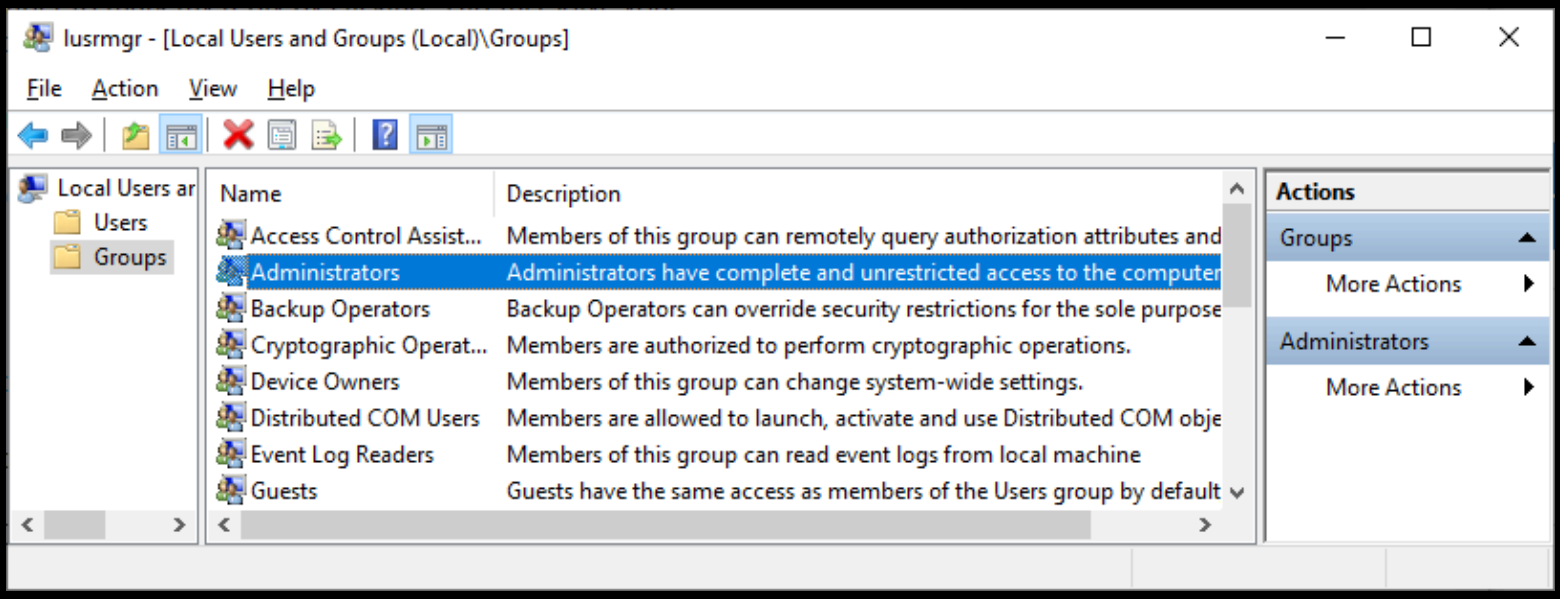
In addition to specifying the file or script path and trigger, you must enter the credentials under which the task will run. If the user account lacks sufficient permissions, the task will not execute.

13.1.6 Local Users and Groups Console

The **Local Users and Groups console** offers an advanced interface for managing user accounts, including creating, modifying, disabling, deleting, and resetting passwords.

Security groups allow you to group user accounts with similar permissions, like editing files in a shared folder. Default groups, such as Administrators, Users, and Guests, define account types available through the settings interface.

Figure 1. Local Users and Groups console showing default security groups. Adding a user account as a member of the Administrators group gives the account full privileges.



Screenshot courtesy of Microsoft.

Description

The left panel has a navigation tree with Users and Groups categories. The main panel lists various groups along with descriptions. The highlighted group is Administrators, which grants complete and unrestricted access to the computer. The right panel contains an Actions menu with options for managing groups and administrators.

Note:

Users, groups, and sharing/permissions are covered in more detail later in the course.

Using PowerShell

PowerShell can be used to perform the same tasks from the Local Users and Group Console. This is useful when developing scripts to create users and assign them to groups.

To add a new user account, use the `net user` command with the `/add` switch. The basic syntax and common switches include:

- `net user`: The command used to manage user accounts.
- `UserName`: Specifies the name of the user account you want to create or manage.
- `Password`: Specifies the initial password for the account.
- `/add`: Creates a new user account with the specified name and password.

Example usage:

- `net user UserName Password /add`

After creating the account, you can force the user to change their password at the next logon by using the `/logonpasswordchg` switch with `net user`:

Example usage:

- `net user UserName Password /logonpasswordchg:yes`

To place a user into an appropriate local group, you use the `net localgroup` command with the `/add` switch:

- `net localgroup`: The command used to manage local groups on the computer.
- `GroupName`: Specifies the local group you are modifying (for example, `Administrators`, `Backup Operators`).
- `UserName`: Specifies the user account you want to add to the group.
- `/add`: Adds the specified user to the specified local group.

Example usage:

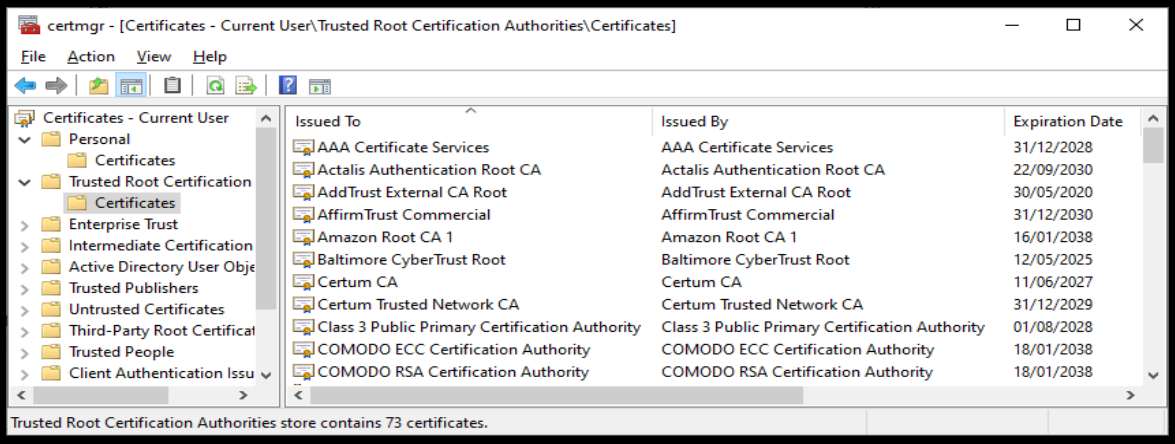
- `net localgroup GroupName UserName /add`

13.1.8 Certificate Manager

A digital certificate verifies the identity of a user, computer, or service, with validity guaranteed by the issuing certification authority (CA). The certificate manager console displays installed certificates and allows for requesting and importing new ones.

Key subfolders include:

- Personal Folder: Stores certificates issued to the user account, used for network authentication, data encryption, and digital signatures.
- Trusted Root Certification Authorities: Contains certificates from all trusted issuers, including Microsoft's CA root, local enterprise CAs, and third-party CAs, mostly managed via Windows Update.
- Third-party Root Certification Authorities: Contains trusted issuers from non-Microsoft or local enterprise providers. Figure 1. Using Certificate Manager to view certificates for the current user.



Description
The certificates folder under the head trusted root certification is selected from the menu on the left. The table lists the certificate issued to, issued by, and the expiration date.

Note:

Use **certmgr.msc** to manage certificates for the current user and **certlm.msc** for the computer certificate store.

Trusting an unsafe CA raises critical security vulnerabilities. For example, a rogue CA certificate might allow a website to masquerade as a legitimate bank or other service and trick the user into submitting a password because the browser

seems to trust the web server’s certificate. Use Certificate Manager to remove compromised certificates when necessary.

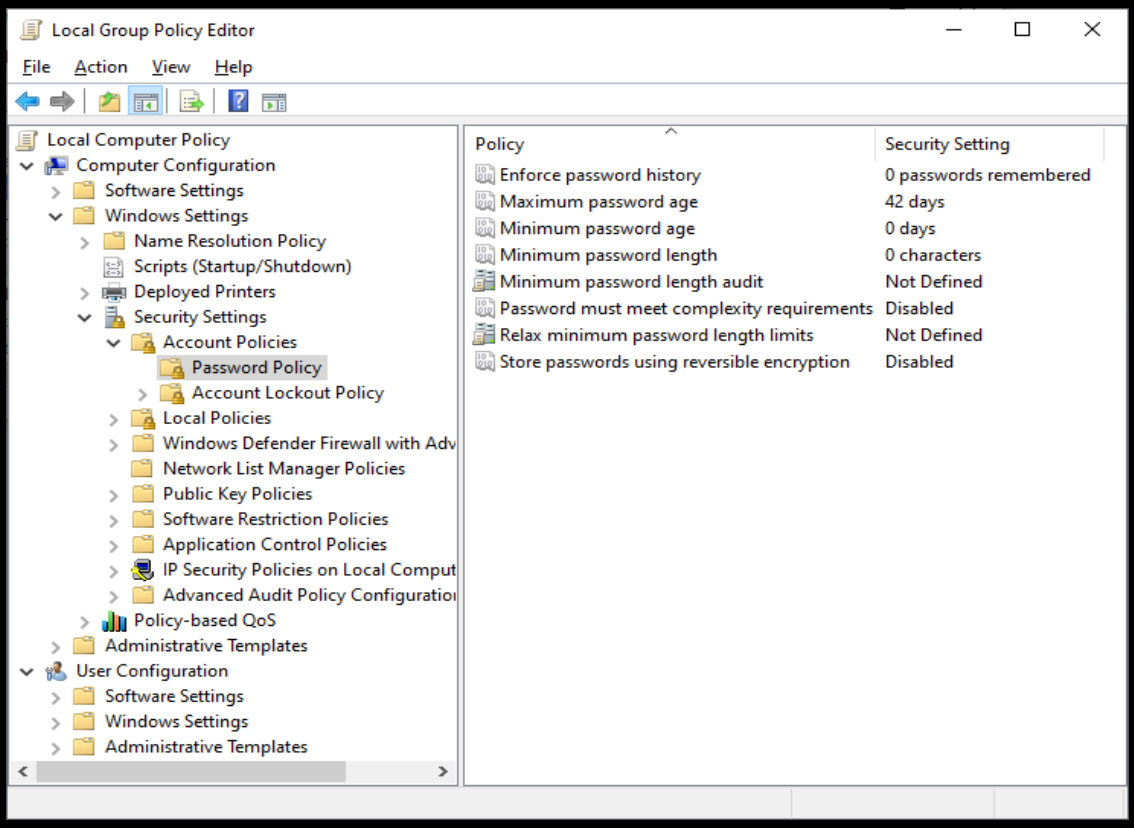
Note:

Third-party browsers often maintain a separate store for personal certificates and trusted root CAs.

13.1.9 Group Policy Editor

GUI tools like Settings and Control Panel modify user profiles and system configurations stored in the registry, but many registry settings aren't accessible through these tools. The Group Policy Editor offers a robust way to configure these Windows settings without directly editing the registry. Vendors can also create administrative templates to configure third-party software via policies.

Figure 1. Using Group Policy Editor to view the local password policy.



Screenshot courtesy of Microsoft.

Description

The password policy folder under the folders account policies and security settings is selected from the menu on the left. The table lists the policy and security setting.

In large networks, group policy efficiently applies settings across multiple computers, avoiding manual configuration. Policies are typically set using an enabled/disabled/not defined toggle, though some require discrete values. It's crucial to read each policy carefully to understand the effects of enabling, disabling, or leaving it not defined.

Note:

Use the Local Security Policy editor (secpol.msc) to modify security settings specifically.

13.1.10 Registry Editor

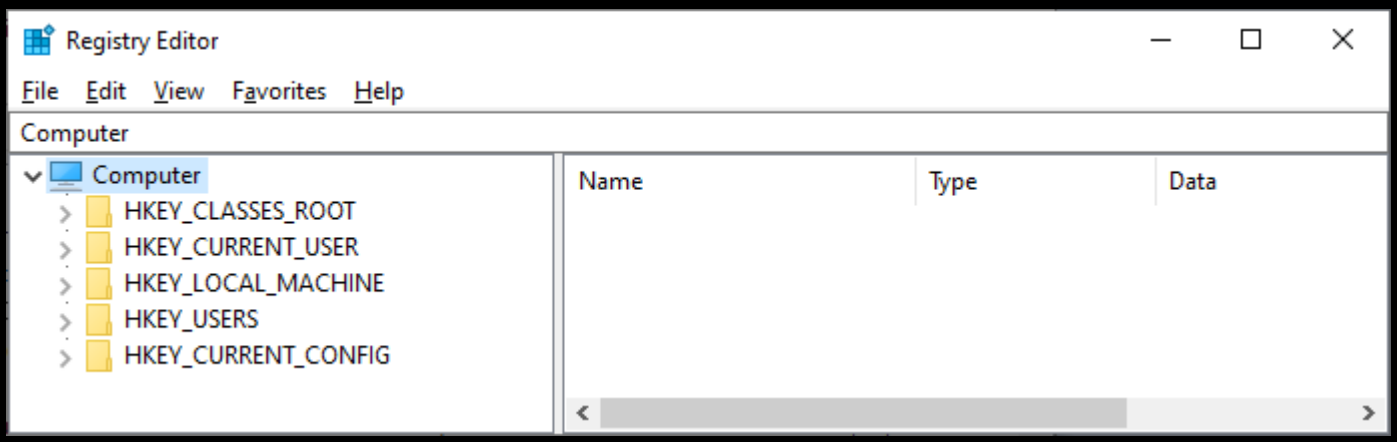
The Windows registry is a remotely accessible database for storing configuration information for the OS, devices, and applications. Use the Registry Editor (regedit.msc) to view or edit the registry.

Registry Keys

The **Registry** is organized into five root keys containing computer and user databases:

- HKEY_LOCAL_MACHINE (HKLM): Manages system-wide settings.
- HKEY_USERS (HKU): Contains settings for individual user profiles, like desktop personalization.
- HKEY_CURRENT_USER (HKCU): A subset of HKEY_USERS with settings for the logged-in user.
- HKEY_CLASSES_ROOT (HKCR): Contains information about registered applications, file associations, and OLE object classes, determining which application opens a file type.
- HKEY_CURRENT_CONFIG (HKCC): Reflects the current hardware profile used at startup, dynamically built at boot time.

Figure 1. Registry root keys



Screenshot courtesy of Microsoft.

Description

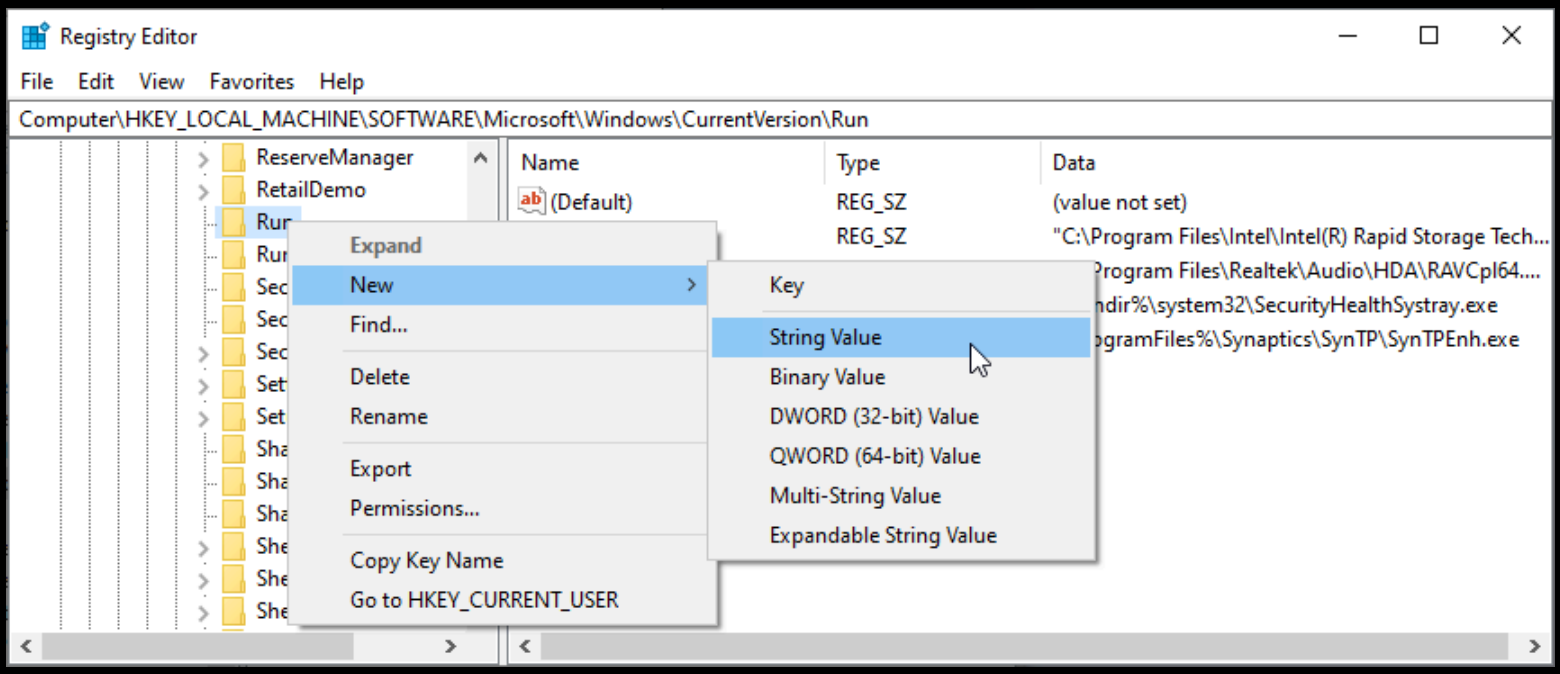
The computer on the left menu is highlighted. A blank table with heads name, type, and data is at the center.

The registry database is stored in binary files called hives, consisting of a main file, a .LOG file (transaction log), and a .SAV file (setup copy). The system **hive** also has an .ALT backup file. Most files are in the C:\Windows\System32\Config folder, while each user profile's hive (NTUSER.DAT) is in the user's profile folder.

Editing the Registry

Root keys contain subkeys and data items called value entries, similar to folders and files. A value entry includes the name, data type (such as string or binary), and the value itself. Use the **Find** tool to search for keys or values.

Figure 2. Editing the registry



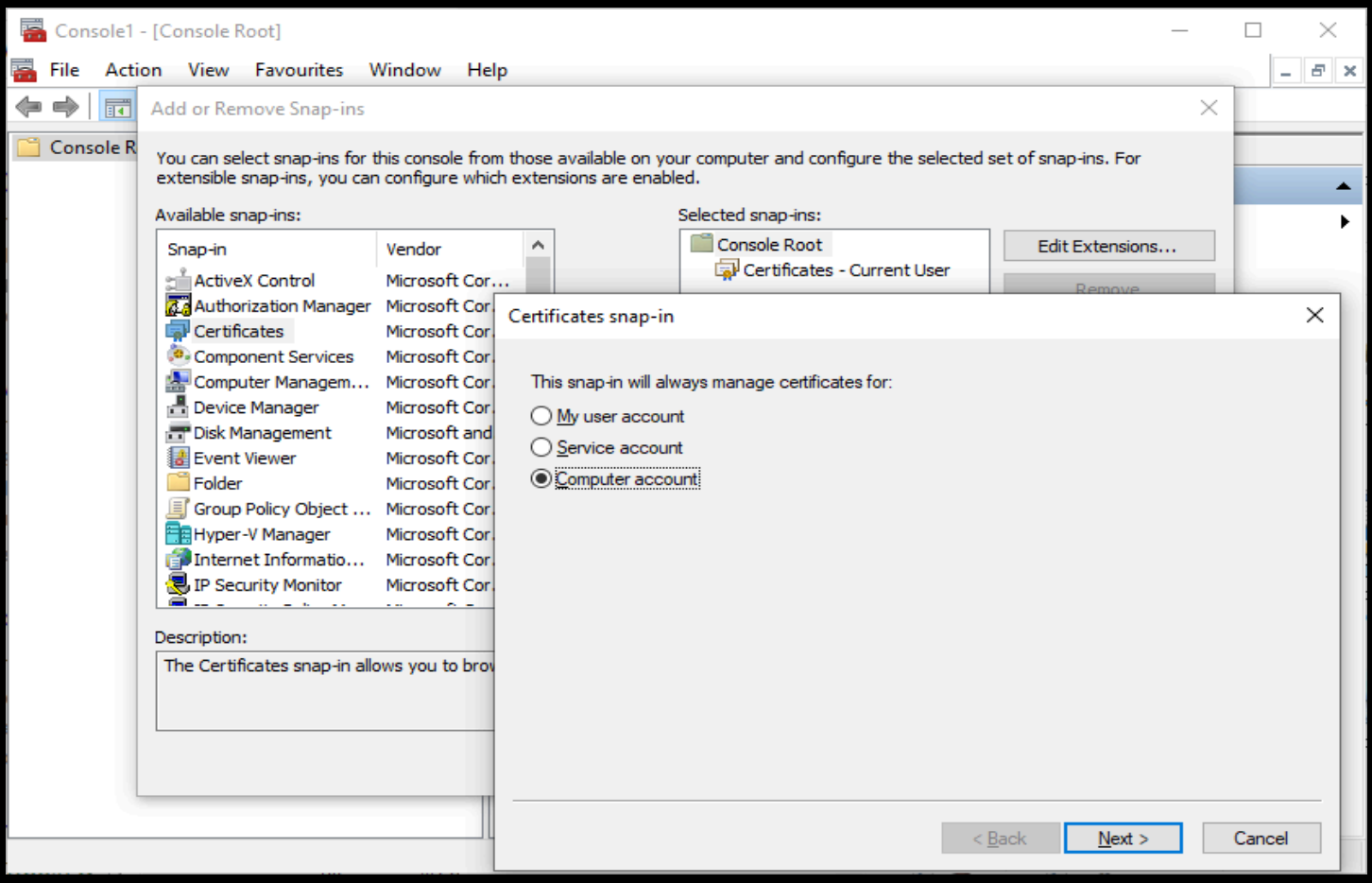
Screenshot courtesy of Microsoft.

To copy registry portions to other computers, select File > Export Registry File. The exported file can be merged into another registry by double-clicking it or calling it from a script.

13.1.11 Custom Microsoft Management Consoles

A Microsoft Management Console (MMC) is a container for snap-ins like Device Manager, Disk Management, Group Policy Editor, and Certificate Manager. Use the `mmc` command to customize and create a console with your chosen snap-ins. Save the console as an MSC file in the Administrative Tools folder.

Figure 1. Adding a snap-in to a custom console



Screenshot courtesy of Microsoft.

Description

The window background lists various available snap-ins, selected snap-ins, and description. The Certificates Snap-in dialog box is open, offering three options: My user account, Service account, and Computer account, with Computer account selected. Back, Next, and Cancel buttons are at the bottom.

Note:

Most MMC snap-ins can manage both local and remote computers on the network.

13.2.1 Command Prompt

You can execute any command from the **Run** dialog, but for a series of commands or viewing output, use the command shell. The **command prompt** processes legacy commands from early Windows versions.

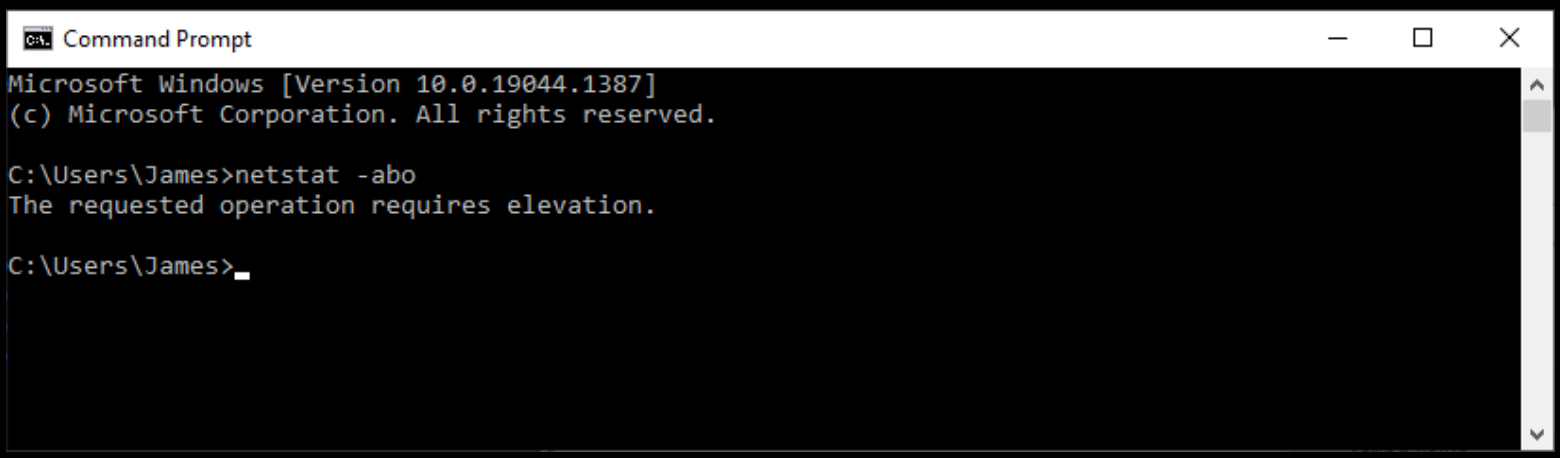
Note:

You can also run the legacy commands at a modern Windows PowerShell prompt. In Windows 11, the command interface is redesigned as the Windows Terminal.

Administrative Command Prompt

Some commands require elevated privileges. If a command needs elevation, you'll see "The requested operation requires elevation." To run as administrator, right-click the Command Prompt shortcut, select "**Run as administrator**," and confirm the UAC prompt. Alternatively, type cmd the Instant Search box and press **CTRL+SHIFT+ENTER**. The title bar will show "Administrator: Command Prompt," and the default folder will be C:\Windows\System32 rather than C:\Users*Username*.

Figure 1. Trying to run a command that requires elevation



Screenshot courtesy of Microsoft.

Note:

This method can also open other utilities like Explorer or Notepad with administrative privileges.

Command Syntax

Enter commands at the prompt (>) using the command name, switches, and arguments with proper syntax. Press ENTER to execute the command. Required and optional arguments and switches are listed in the command syntax. Switches are usually preceded by a forward slash. If an argument includes a space, enclose it in quotes. Use cls to clear the screen if needed.

Some commands, like nslookup or telnet , work in interactive mode. This means when you start the command, it opens the program, and the prompt will only accept inputs related to that program. To leave the program, use the exit or quit command, or press **CTRL+C**. If you're not in an interactive command, using exit will close the Command Prompt window.

Getting Help

The command prompt includes a basic help system. Type help and then press **ENTER** at the command prompt to see available commands or type help Command for syntax and switches used for the command. Use the /? switch for command-specific help, e.g., netstat /? displays help on the netstat command.

13.2.2 Navigation Commands

The string before the > in the command prompt indicates the current working **directory**. Commands apply to this directory's contents unless an absolute or relative path is specified as an argument.

Note:

Windows uses backslashes for directories, but it also accepts forward slashes in both Explorer and the command prompt. In Linux, directories are always delimited by forward slashes.

Listing Files and Directories

Use the **dir command** to list files and subdirectories in the current directory or a specified path.

- **Order Files:** Use /o:x to sort files, where x can be:
  - n for name
  - s for size
  - e for extension
  - d for date
- **Set Date Field:** Use /t:x to specify the date field, where x can be:
  - c for created
  - a for last accessed
  - w for last modified
- **Display Attributes:** Use /a:x to show files with specific attributes, where x can be:
  - r for Read-only
  - h for hidden
  - s for system
  - a for archive

Use wildcard characters for unspecified characters. A question mark ? represents a single unspecified character. For example, dir ????????.log lists all .log files with eight-character names.

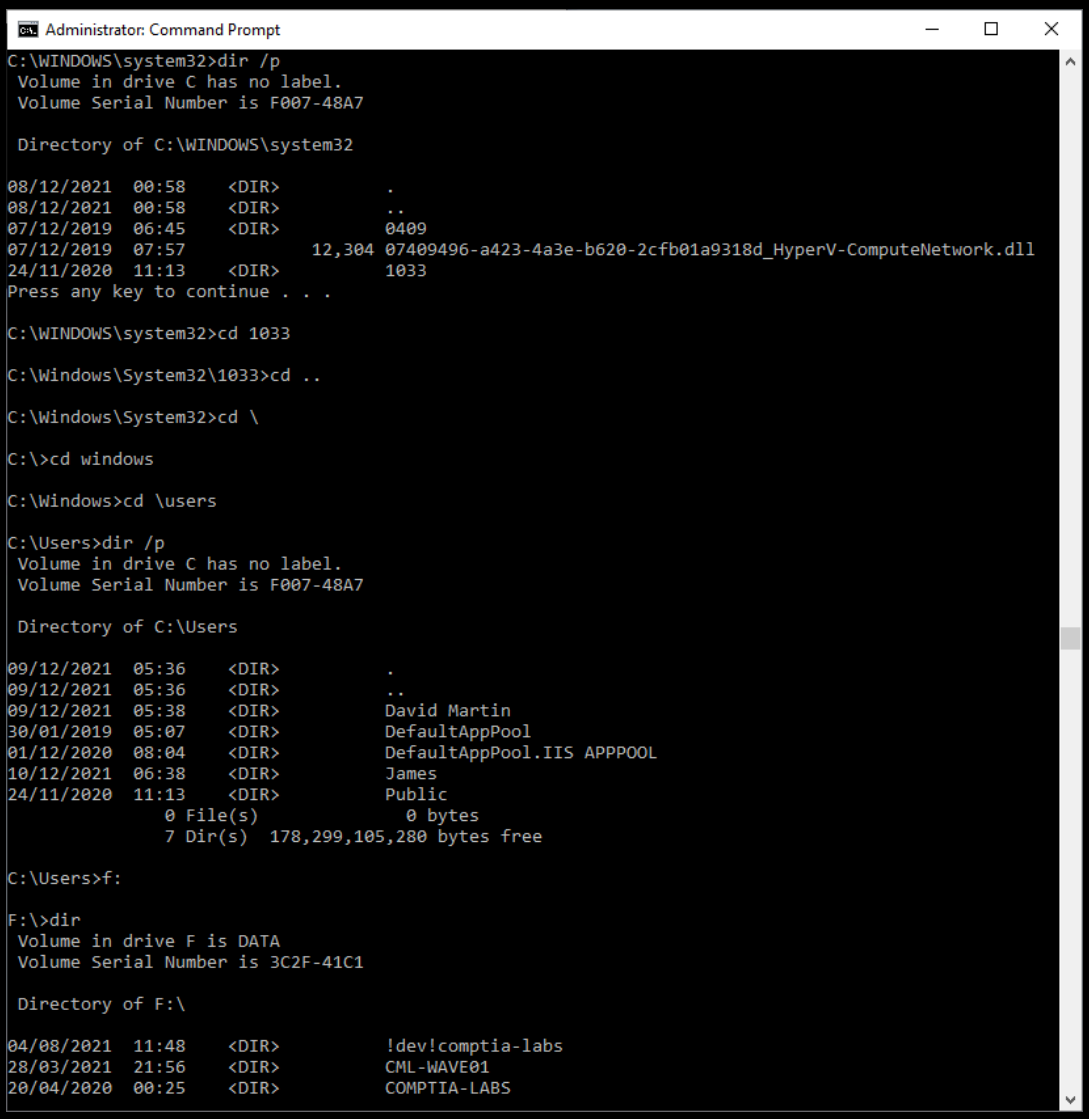
Changing the Current Directory

Use the **cd command** to change the working directory. Enter the full path to switch directories, such as cd C:\Users\David.

Here are some shortcuts:

- To move from C:\Users\David to C:\Users\David\Documents, type: cd Documents
- To move up to the parent directory from C:\Users\David\Documents, type: cd ..
- To change to the root directory from C:\Users\David, type: cd \
- To switch from C:\Users to C:\Windows, type: cd \Windows

Navigating directories with the cd command



Changing the Current Drive

The active, or in focus, drive is managed separately from the directory. To switch drives, enter the drive letter followed by a colon and press **ENTER**. For example, typing D: switches to the D drive, and the prompt will update to D:\, indicating that D is now the default drive.

13.2.3 File Management Commands

The **move command** and **copy command** allow you to transfer files within a single directory. They use a three-part syntax:command Source Destination, where Source specifies the drive, path, and file name to be moved or copied, and Destination specifies the drive and path for the new location.

Copying Directory Structures

The **robocopy command**, or "robust copy," is another file copy utility. Microsoft recommends using robocopy over xcopy for better handling of long file names and NTFS attributes.

The command includes various switches for enhanced functionality:

- **/xf**: Excludes files that match the specified names or paths.
- **/xd**: Excludes directories that match the specified names or paths.
- **/S**: Copies subdirectories, excluding empty ones.
- **/E**: Copies all subdirectories, including empty ones.
- **/L**: Lists the files and directories that would be copied, without actually copying them.

Check the command help for additional switches and syntax to tailor the command to your specific needs.

Note:

You can also use robocopy to move files with the /mov switch.

Creating a Directory

To create a directory, use the md or mkdir command. For example, type md Data to create a directory named Data in the current directory. To create a directory named *Docs* within a directory called *Data* on the A drive, while the current path is C:, type md A:\Data\Docs.

Note:

Folder and file names cannot include reserved characters: \ / : * ? " < > |

Removing a Directory

To delete an empty directory, use *rd Directory* or **rmdir** *Directory*. If the directory contains files or subdirectories, use the /s switch to remove them. The /q switch can be used to suppress confirmation messages for quiet mode.

13.2.5 Disk Management Commands

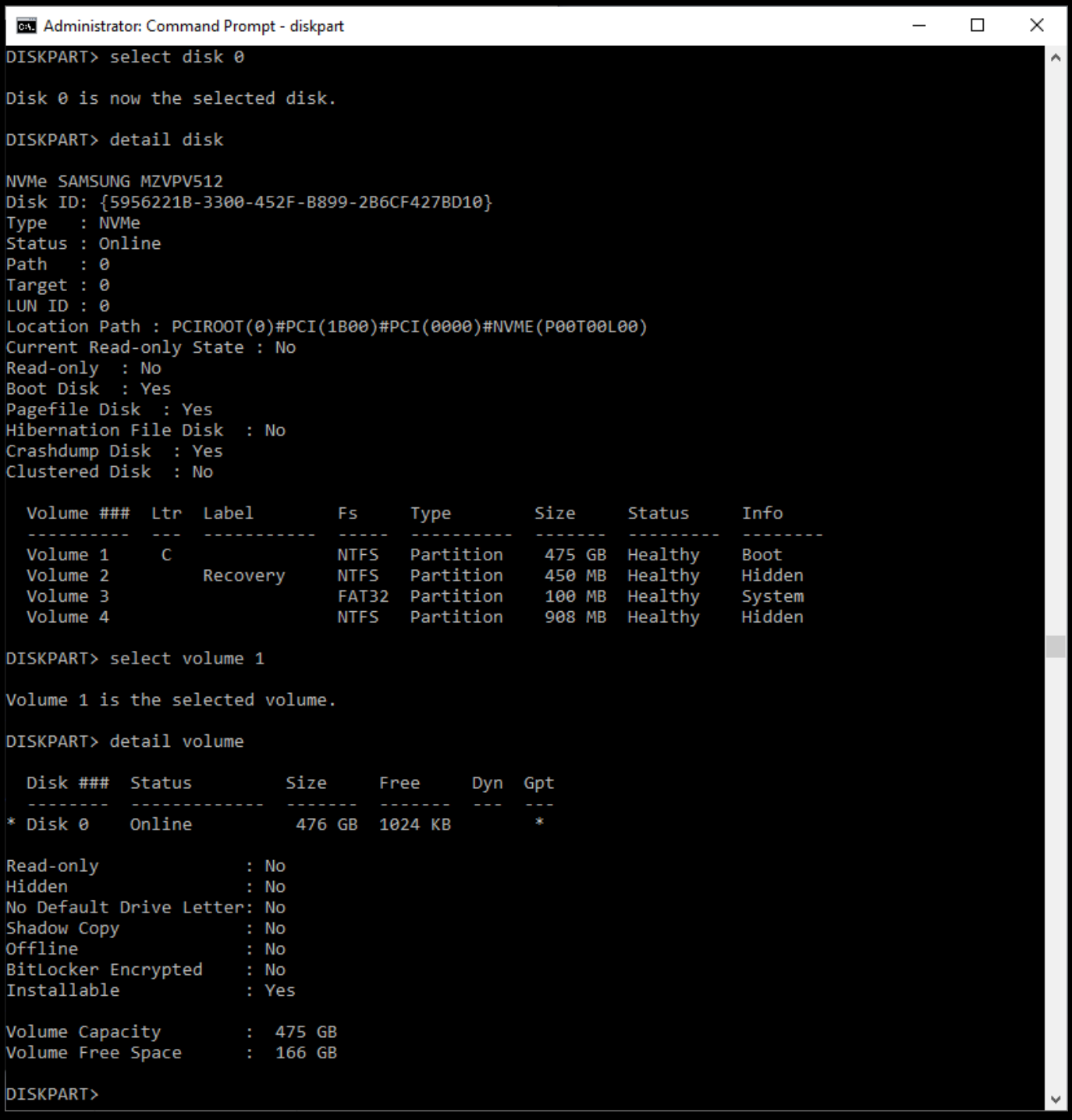
The Disk Management snap-in is easy to use, but there are some circumstances where you may need to manage volumes at a command prompt.

The diskpart Command

The **diskpart command** serves as the command-line interface for the Disk Management tool. While it offers many options, here's a basic process for inspecting disks and partitions:

1. Run the diskpart utility, then type select disk 0 (or the desired disk number).
2. Enter detail disk to view disk configuration. Healthy partitions should be reported; if none are found, the partition table might be corrupted.
3. Type select partition 0 or select volume 0 (or the desired partition/volume number).
4. Use detail partition or detail volume for more information. You can then use commands like assign (to change the drive letter), delete (to remove the volume), or extend .
5. Type exit to quit diskpart.

Figure 1. The diskpart program showing a hard disk partition structure



Screenshot courtesy of Microsoft.

Note:

Unlike the Disk Management tool, diskpart allows destructive actions, such as deleting system or boot volumes, so use it with caution.

The format Command

The **format command** creates a new file system on a drive, deleting all existing data. The basic command is format **drive navigation input** X: /fs:SYS, where *X* is the drive letter and *SYS* is the file system type (e.g., NTFS, FAT32, EXFAT). By default, it scans for bad sectors, which can be skipped using the/q switch. Refer to online help for additional switches.

Note:

Both standard and quick formats remove file references in the volume boot record, but do not erase the actual data. Existing files can be overwritten by new files, but data recovery is possible with third-party tools. A secure format utility prevents recovery by overwriting each sector with zeros, often using multiple passes.

The chkdsk Command

The **chkdsk command** scans the file system and disk sectors for faults and attempts to repair detected problems. A version called autochk runs automatically if file system errors are detected at boot.

There are three ways to use chkdsk :

- chkdsk X : (where X is the drive letter but no switch is used) runs in read-only mode, reporting any errors that need repair.
- chkdsk X : /f attempts to fix file system errors.
- chkdsk X : /r fixes file system errors and tries to recover bad sectors, prompting you to save recoverable data as filennnn.chk files in the root directory.

Check Disk cannot fix open files, so you may need to schedule the scan for the next system restart.

Note:

chkdsk /f and chkdsk /r can take a long time to complete. It's not recommended to cancel a scan. Consider running a read-only scan first.

13.2.6 System Management Commands

The **shutdown command** is used to safely power off, restart, hibernate, or log out of the system. For a complete list of options and their descriptions, use shutdown /?, which displays a help menu with all available parameters. This is a best practice for understanding and troubleshooting command usage.

- **Shutdown** (shutdown /s)**:** Closes all programs and services before turning off the computer. Users should save open files first but will be prompted to save unsaved changes. Use shutdown /t nn to delay shutdown by nn seconds (default is 30 seconds). Abort a shutdown with shutdown /a (if done quickly).
- **Hibernate** (shutdown /h)**:** Saves the current session to disk before powering off.
- **Log off** (shutdown /l)**:** Closes programs and services under the user account, leaving the computer running.

Windows Resource Protection safeguards system files and registry keys from damage or misuse. The **sfc command** utility (sfc) allows you to manually verify and restore system files from cache if they are corrupt or damaged. For a full list of options, use sfc /? to display the help menu.

Use sfc from an administrative command prompt in these modes:

- sfc /scannow : Runs an immediate scan.
- sfc /scanonce : Schedules a scan for the next computer restart.
- sfc /scanboot : Schedules a scan at every boot.

Note:

The WINSxS folder stores multiple versions of system and shared program files, ensuring the correct ones are available for operations and updates without needing external media (like CD or USBs) to restore or update files. This can result in significant disk space usage.

Reporting the Windows Version

The **winver command** provides Windows version information, useful for support. For additional details about the command, use winver /? .

Key details provided by winver:

- **Windows 10 or 11:** Identifies the OS as a client version, distinct from Windows Server.
- **Version:**Indicates a feature update, shown as a year/month code representing the time of release (e.g., 1607 for July 2016, 21H1 for early 2021).

- **OS Build:** A two-part number; the first part shows the brand and feature update, while the second part (rev) indicates quality updates or patches. The rev number can be used to find changes and known issues associated with the update in the Microsoft Knowledge Base (support.microsoft.com).

Note:

The About settings page offers more detailed information, including edition and license details.

Verifying User Identity

The **whoami command** is a utility that displays the current user's username and domain information, verifying the identity and access level of the logged-in user. For a full list of options, use whoami /? .

To use whoami, open the Command Prompt or PowerShell, type whoami , and press **Enter**. The output shows the username in the format DOMAIN\Username, indicating the domain or computer name for local accounts. The command can be extended with switches for more detailed information, such as whoami /groups to list security groups the user belongs to, or whoami /priv to display user privileges. These features assist in troubleshooting permission issues and verifying user rights for specific tasks.

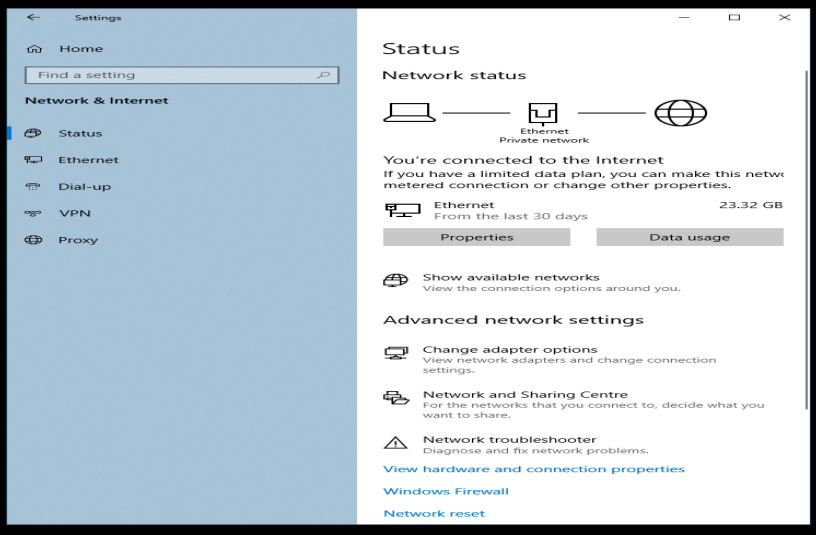
13.3.1 Windows Network Connection Types

A computer joins a local network by connecting the network adapter—or **network interface card**—to a switch or wireless access point. For proper end-user device configuration, the card settings should be configured to match the capabilities of the network appliance.

Establish a Wired Network Connection

Almost all **wired** network connections are based on some type of Ethernet. The adapter's media type must match that of the switch it is connected to. Most use copper wire cable with RJ45 jacks, though installations in some corporate networks may use fiber optic cabling and connector types. The adapter and switch must also use the same Ethernet settings. These are usually set to autonegotiate, and a link will be established as soon as the cable is plugged in.

Under Windows, each wired adapter is assigned a name. The first adapter is labeled `Ethernet`. Additional adapters are identified as `Ethernet2`, `Ethernet3`, and so on. A new name can be applied if necessary. If any Ethernet settings do need to be configured manually, locate the adapter in **Device Manager**, right-click and select **Properties**, and then update settings using the **Advanced** tab. You can also access adapter options via the status page in **Network & Internet** settings. Figure 1. Windows 10 Network & Internet Settings app



Description

The menu on the left has a find a setting field at the top followed by options Status, Ethernet, Dial-up, V P N, and Proxy under the head Network and Internet. A network diagram with the Ethernet Private network is on the right. The data

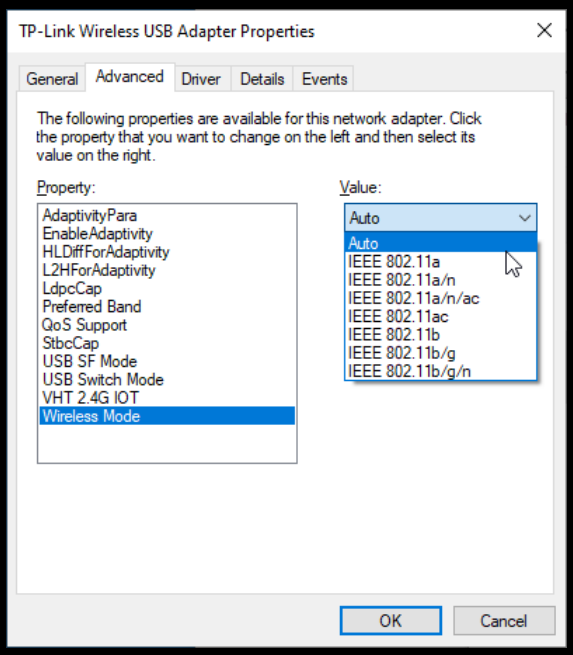
usage for Ethernet is listed as 23.32 G B over the last 30 days. Properties and Data usage buttons are below. Show available networks option is below the buttons. The advanced network settings include change adapter options, network and sharing center, and network troubleshooter. The link below reads, view hardware and connection properties, windows firewall, and network reset.

Establish a Wireless Network Connection

To **establish a wireless network connection**, select the network status icon in the notification area, and select from the list of displayed networks. If the access point is set to broadcast the network name or service set ID (SSID), then the network will appear in the list of available networks. The bars show the strength of the signal, and the lock icon indicates whether the network uses encryption. To connect, select the network, and then enter the required credentials. If you choose the **Connect automatically** option, Windows will use the network without prompting whenever it is in range.

If SSID broadcast is suppressed, input WLAN settings manually. From the Network & Internet page, select Wi-Fi ⇨ Manage known networks ⇨ Add a new network.

Wi-Fi properties for the adapter are configured via Device Manager. The most important setting on a wireless card is support for the 802.11 standard supported by the access point. Most cards are set to support any standard available. This means that a card that supports 802.11n will also be able to connect to 802.11g and 802.11b networks. You can also adjust parameters such as roaming aggressiveness and transmit power to address connection issues. Figure 2. Wireless network adapter properties in Device Manager.



Screenshot courtesy of Microsoft.

Description

The Wireless Mode property is selected. A dropdown menu with options such as Auto, I E E E 802 dot 11 a, I E E E 802 dot 11 a slash n, I E E E 802 dot 11 a slash n slash ac, I E E E 802 dot 11 ac, I E E E 802 dot 11 b, I E E E 802 dot 11 b slash g, and I E E E 802 dot 11 b slash g slash n. Ok and Cancel buttons are visible at the bottom.

13.3.2 IP Addressing Schemes

Device Manager properties are for the adapter's low-level network link (Ethernet or Wi-Fi). To connect to a network, the logical adapter must have a valid **client network configuration**. Each adapter must be configured with client software and allocated an appropriate IP address and **network-mask** (subnet mask).

Internet Protocol Addressing Scheme

An **Internet Protocol** addressing scheme uses these values:

- In IPv4, the 32-bit address is combined with a 32-bit subnet mask, both of which are typically entered in dotted decimal notation. The mask distinguishes the logical network from the host portions within the IP address. For example, the address 192.168.1.100 and mask 255.255.255.0 mean that the host is using the address portion .100 on the logical network 192.168.1.0. The subnet mask ensures that devices on the same network can communicate directly, while devices on different networks require a router.

- In IPv6, the address is 128 bits long and the interface address portion is always the last 64 bits. Network prefixes are used to identify logical networks within the first 64 bits.

All hosts on the same local network, or wired LAN, must use addresses from within the same range. Hosts with addresses in different ranges can only be contacted by forwarding the packet via a router. Each host must be configured with the IP address of a local router. This is referred to as the default gateway.

Note:

The router interface is usually assigned the first available value. For example, if the IP address scheme is 192.168.1.0/24, the first available host address is 192.168.1.1.

Typically, a host is also configured with the addresses of **domain name system** (DNS) servers that can resolve requests for name (e.g., www.example.com) to IP addresses, making identification of hosts and services simpler.

On a home network, the router is usually configured to forward DNS queries, so the gateway and primary DNS server parameters for client PCs will usually be set to the same value. As well as DNS servers, the host might be configured with a **domain suffix** to identify its fully qualified domain name (FQDN) on the local network. For example, if attached to a network identified as ad.company.example, the FQDN of PC1 will be PC1.ad.company.example.

Static versus Dynamic Configuration

These IP values can be assigned **statically or dynamically**. Configuring large numbers of hosts with valid static addressing parameters is a complex management task. Each host is manually assigned an IP address, subnet mask, gateway, and DNS server. While this provides precise control, it is time-consuming and error-prone for large networks. Most hosts are configured to obtain an address automatically, using a service called the **Dynamic Host Configuration Protocol (DHCP)**. DHCP simplifies management by automatically assigning valid IP parameters to hosts, ensuring they can communicate on the network without manual configuration.

13.3.3 Windows Client Configuration

The IP configuration for each adapter interface is often set using the GUI Properties dialog accessed via Network & Internet settings or the Network Connections applet (`ncpa.cpl`). By default, the following clients, protocols, and services are installed on Ethernet and Wi-Fi adapters:

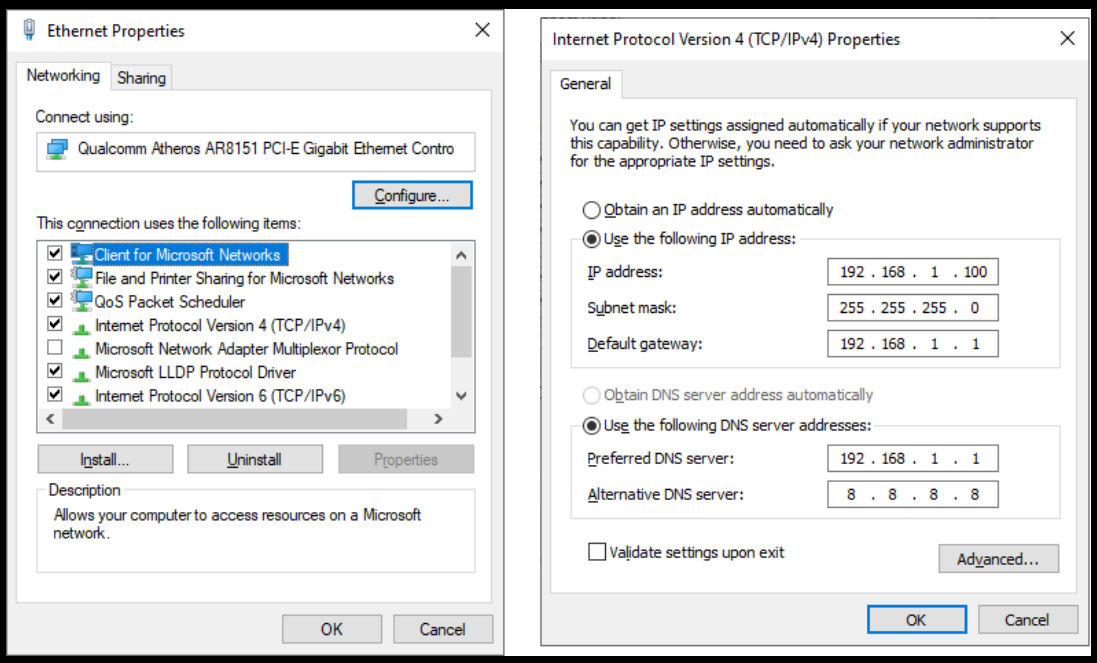
- Client for Microsoft Networks and File and Print Sharing for Microsoft Networks software.
- **Internet Protocol**—Both IP version 4 and IP version 6 will be installed. The network adapter automatically uses the appropriate version of the protocol depending on the network it is connected to.
- **Link-layer Topology Discovery**—This protocol provides network mapping and discovery functions for networks without dedicated name servers.

The IP properties will default to **Obtain an IP address automatically**, which uses a DHCP server. To configure a static address, double-click the IP properties item.

Note:

Windows prefers IPv6 if available which can be configured via the Registry or through group policy.

Figure 1. Ethernet Properties dialog (left) and Internet Protocol Version 4 (TCP/IPv4) Properties dialog (right).

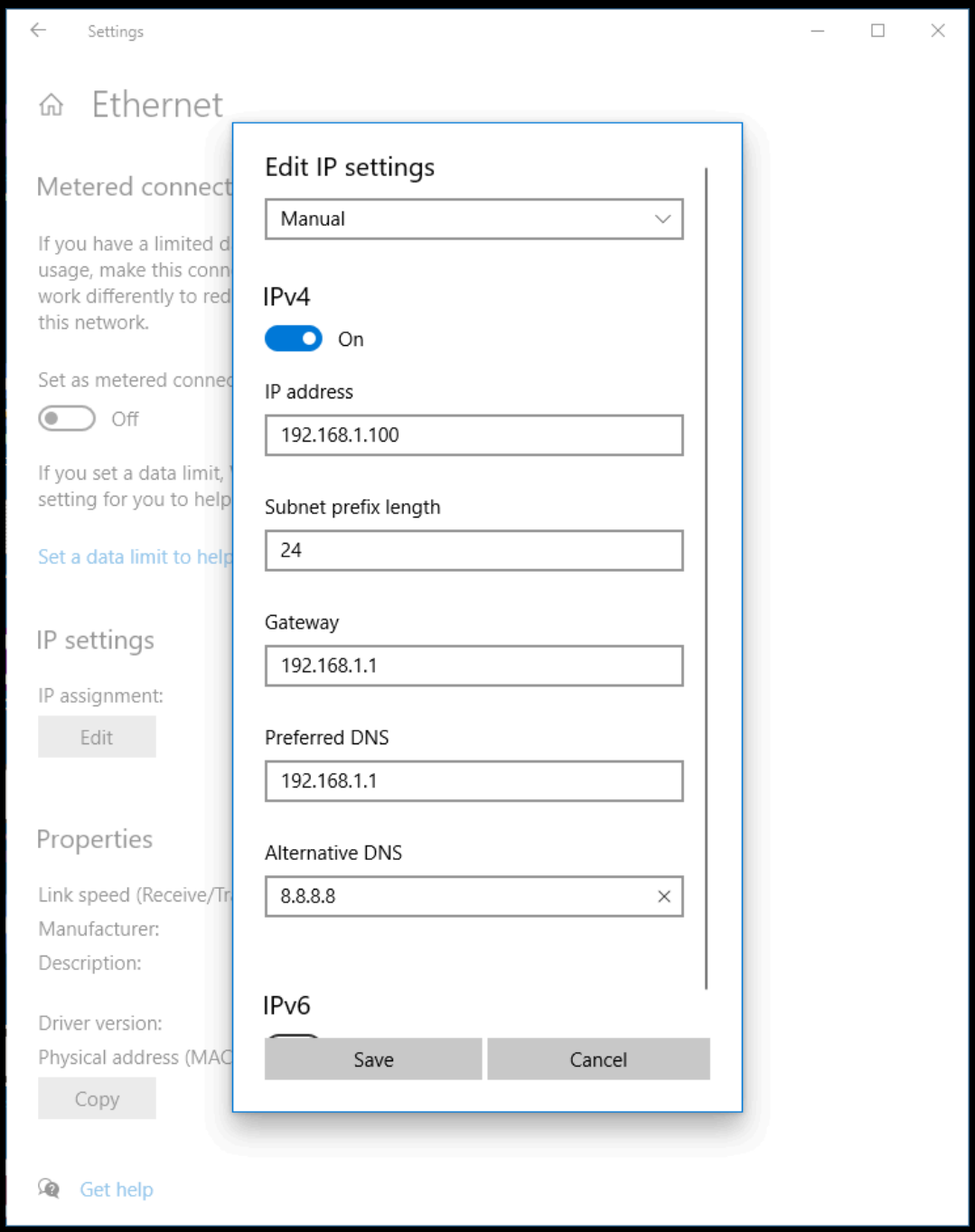


Description

The Ethernet Properties window has the networking tab selected. The connect using option is at the top followed by a configure button. The item used by the connection are listed at the bottom. The install, uninstall, and properties button are at the bottom. The description below is followed by the ok and cancel button. The Internet Protocol Version 4 (T C P slash I P v 4) Properties window shows the general tab. The I P address, subnet mask, and default gateway are listed under the head use the following I D address. The preferred D N S server and the alternative D N S server are listed under the head, use the following D N S server addresses. An advanced button at the bottom is followed by ok and cancel buttons below them.

You can also adjust the IP configuration via the settings app. In this dialog, you need to enter the mask as a prefix length in bits. A 255.255.255.0 mask is 24 bits.

Figure 2. Using Network & Internet settings to configure static addressing



Screenshot courtesy of Microsoft.

Description

The configuration is set to Manual and the I P v 4 toggle is switched on. The I P address is 192 dot 168 dot 1 dot 100, the Subnet prefix length is 24, and the Gateway is 192 dot 168 dot 1 dot 1. The Preferred D N S is 192 dot 168 dot 1 dot 1 and the Alternative D N S is 8 dot 8 dot 8 dot 8. The options Save and Cancel are visible at the bottom.

Using PowerShell

Network configurations can be established using PowerShell.

To configure a static IPv4 address on a network interface, you can use the `netsh interface ip set address` command. Common elements include:

- `netsh interface ip set address`: Configures IP address settings for a specific network interface.
- `name="InterfaceName"`: Specifies the name of the network interface you want to configure (for example, `"Ethernet"`).
- `static`: Indicates that you are assigning a static IP configuration (as opposed to using DHCP).
- `IPAddress`: The static IPv4 address to assign to the interface.
- `SubnetMask`: The subnet mask for the IP address.
- `DefaultGateway`: The default gateway for the interface (If no gateway is being set use `0.0.0.0`).

Example usage:

- `netsh interface ip set address name="Ethernet" static 192.168.0.5 255.255.255.0 192.168.0.1`

To configure DNS servers for a network interface, you can use the `netsh interface ip set dns` and `netsh interface ip add dns` commands. Common elements include:

- `netsh interface ip set dns`: Sets the primary DNS server for a specific network interface.
- `netsh interface ip add dns`: Adds an additional (secondary or tertiary) DNS server for the interface.
- `name="InterfaceName"`: Specifies the network interface whose DNS settings you are configuring.
- `static`: Indicates that you are assigning a static DNS server address.
- `DNSServerAddress`: The IP address of the DNS server.
- `primary`: Indicates that the specified DNS server is the primary DNS server for the interface.

- `index=Number`: Specifies the position/order of the DNS server (for example, `index=2` to set it as the second DNS server).

Example usage:

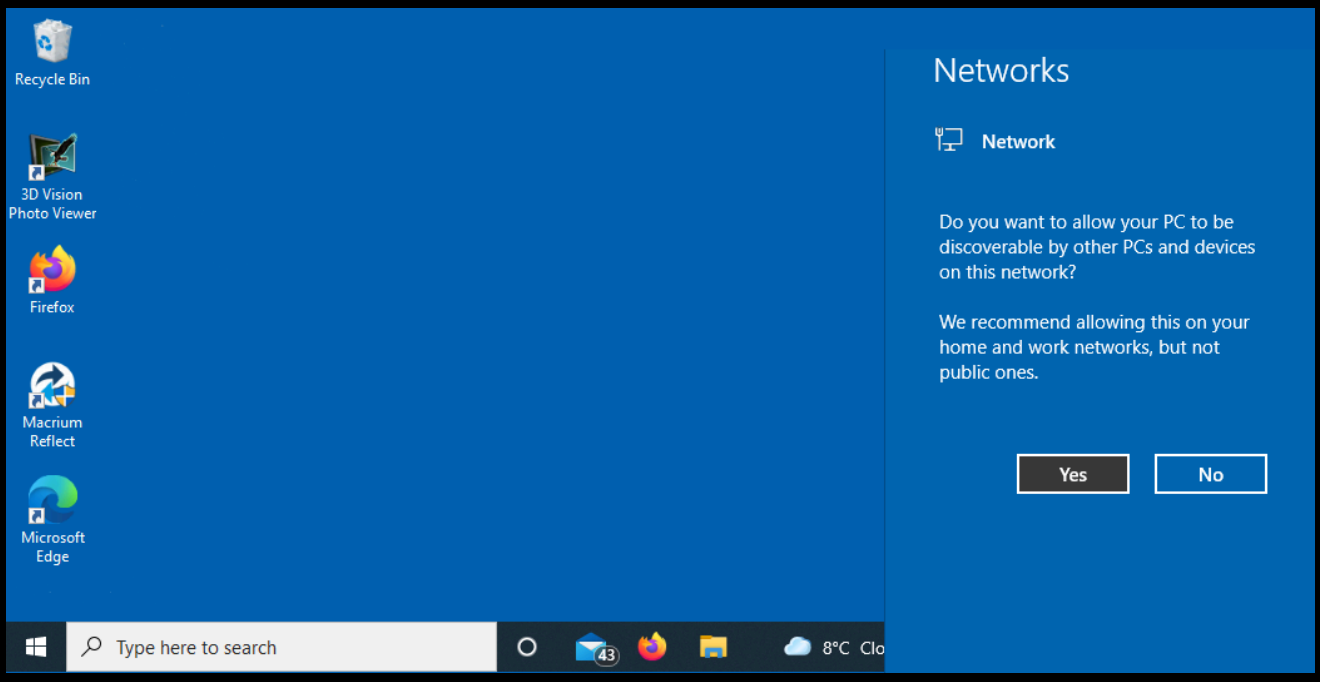
- `netsh interface ip set dns name="InterfaceName" static 10.23.88.32 primary`
- `netsh interface ip add dns name="InterfaceName" 10.23.40.32 index=2`

13.3.4 Network Location

Each network connection is governed by the **local OS firewall settings** imposed by Windows Defender Firewall.

When you connect to a new network, the **network location awareness** service prompts you to set the network profile type. If the network profile type is set as Private, the PC is discoverable and may be used for folder or printer sharing. This is only advisable when connecting to a trusted network. If the network is set as Public, Windows Firewall is configured to block all access and make the host undiscoverable.

Figure 1. Set Network Location prompt



Description

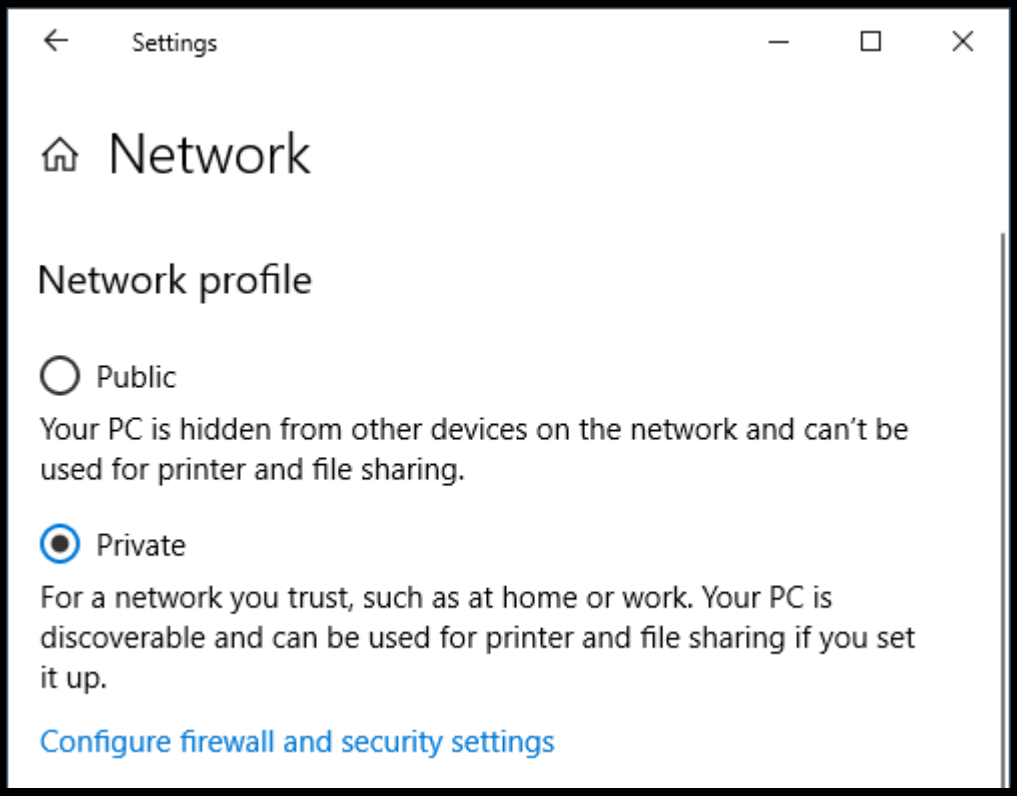
The desktop background is blue with icons for Recycle Bin, 3 D Vision Photo Viewer, Firefox, Macrium Reflect, and Microsoft Edge. The taskbar shows a search bar, system icons, and weather information displaying 8 degrees Celsius. The prompt on the right asks, Do you want to allow your P C to be discoverable by other P Cs and devices on this network? We recommends allowing this on your home and work networks, but not public ones. Below are two buttons: Yes and No.

Note:

There is also a Domain profile. You cannot choose this option, but if the computer is joined to a domain, then the firewall policy will be configured via Group Policy.

Use Network & Internet settings to change the location defined for a network.

Figure 2. Using Network & Internet settings to change the network profile



Description

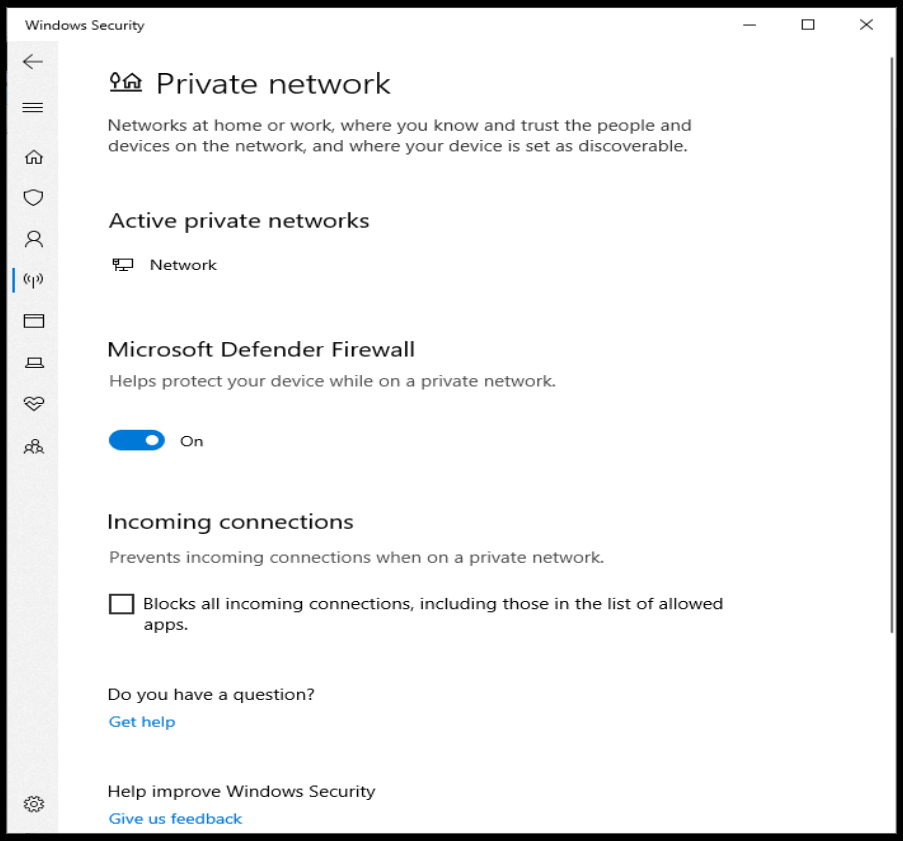
The user can choose between Public, which hides the P C from other devices and disables printer and file sharing, or Private, which allows discovery and sharing on trusted networks. The Private option is selected. A link at the bottom reads Configure firewall and security settings.

With network discovery enabled, other computers and devices can be accessed via the **Network object in File Explorer**. Windows uses a system called universal naming convention (UNC) syntax to address network hosts and resources. The syntax for a UNC **network path** is `\\ Host\Path` , where *Host* is the hostname, FQDN, or IP address of the server and *Path* is a shared folder or file path.

13.3.5 Windows Defender Firewall Configuration

You can turn the firewall on or off and access the configuration applets shown via the **Firewall & network protection** page in the Windows Defender Security Center or via the Windows Defender Firewall applet in Control Panel. You can also choose to block all incoming connections.

Figure 1. Setting the firewall state via the Windows Security Center

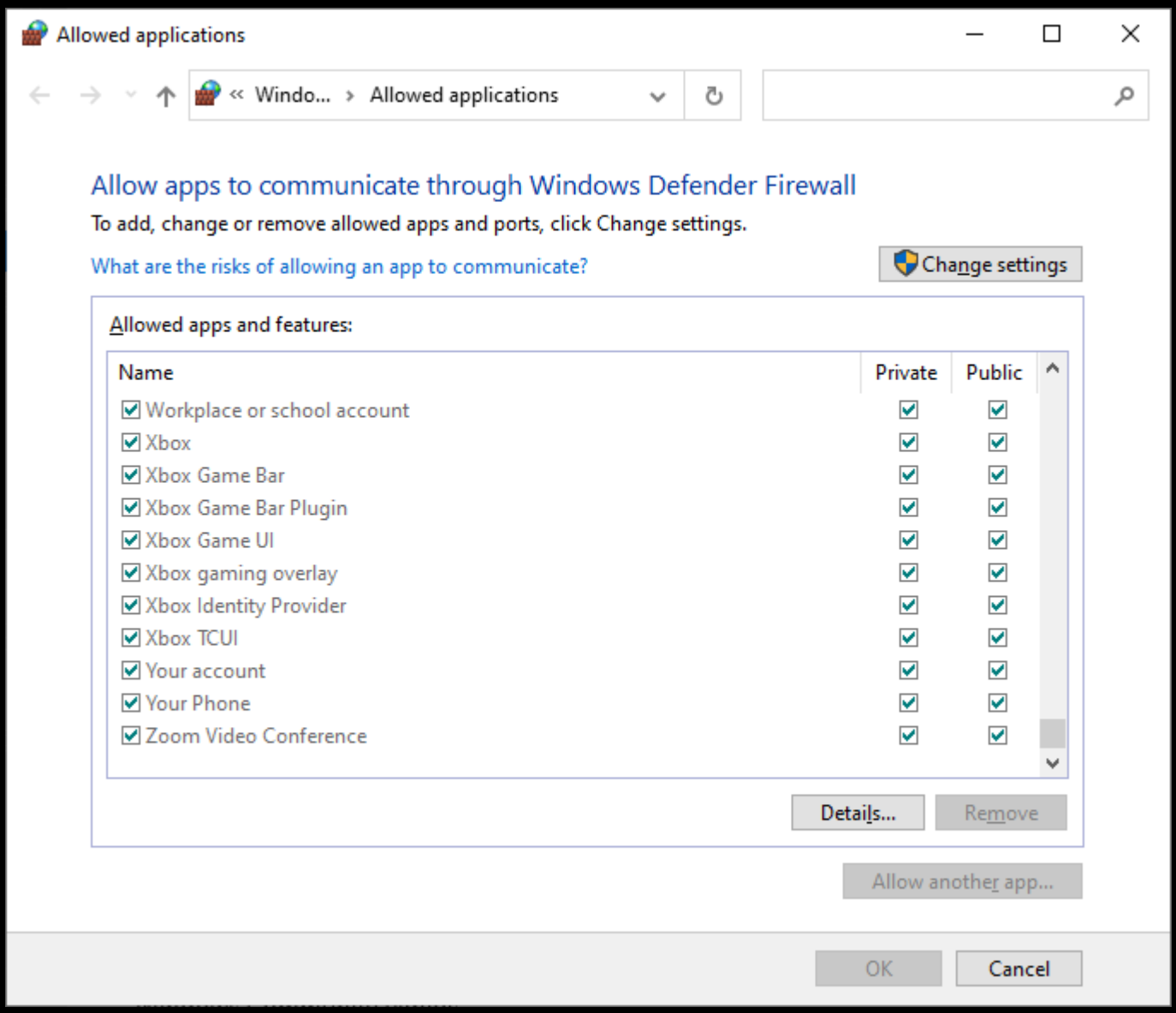


Description

It describes private networks as trusted environments where the device is set as discoverable. The head active private networks reads, network. The Microsoft Defender Firewall toggle is switched on. The Incoming connections section has a checkbox to block all incoming connections, including those in the list of allowed apps. Below are links for Get help and Give us feedback.

To allow or block programs (configure exceptions), from the **Windows Firewall** status page, select **Allow an app through the firewall**. Check the box for either or both network profile types or use **Allow another program** to locate its executable file and add it to the list.

Figure 2. Windows Firewall Allowed Applications



Description

The screen reads, allow apps to communicate through windows defender firewall. The change settings button is followed by a link that reads, what are the risks of allowing an app to communicate? The table below lists the name of the allowed apps and features and has checkboxes under the head private and public. The details and remove buttons are at the bottom. The allow another app button is below it. Ok and cancel buttons are further below them.

13.3.6 VPN and WWAN Connection Types

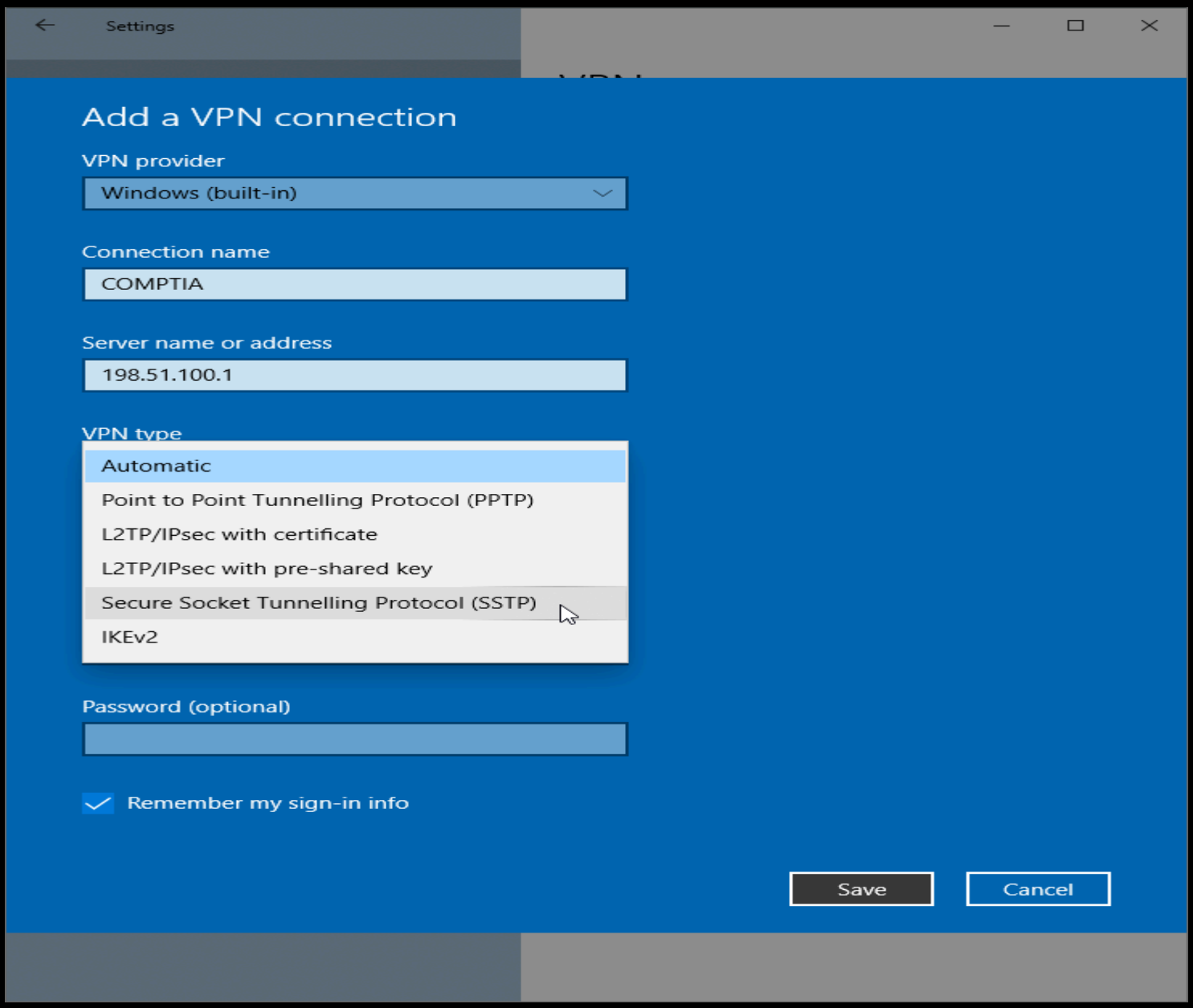
Wired and wireless adapters connect to local networks, but there are other network types too. Many corporate networks allow devices to connect remotely, to support home workers, field workers, branch offices, partners, suppliers, and customers. Also, a user might need or prefer to use a cellular adapter for Internet access.

Establish a Virtual Private Network Connection

A **virtual private network** connects the components and resources of two (private) networks over another (public) network. A VPN is a "tunnel" through the Internet (or any other public network). It uses special connection protocols and encryption technology to ensure that the tunnel is secure and that the user is properly authenticated. Once the connection has been established the remote computer becomes part of the local network (though it is still restricted by the bandwidth available over the WAN link).

Windows supports several VPN types. If the VPN type is supported, you can configure a connection using the Windows client from Network & Internet settings. Some VPNs might require the use of third-party client software.

Figure 1. Configuring a new VPN connection



Description

The V P N provider is set to Windows Built hyphen in. The Connection name is COMPTIA and the Server name or address is 192 dot 51 dot 100 dot 1. The V P N type dropdown is open, displaying options such as Automatic, Point to

Point Tunneling Protocol, L 2 T P slash I P sec with certificate, L 2 T P slash I P sec with pre-shared key, Secure Socket Tunneling Protocol (S S T P), and I K E v 2. Automatic is selected. The password field below is blank. A check box to remember my sign-in info is ticked. The Save and Cancel buttons are at the bottom.

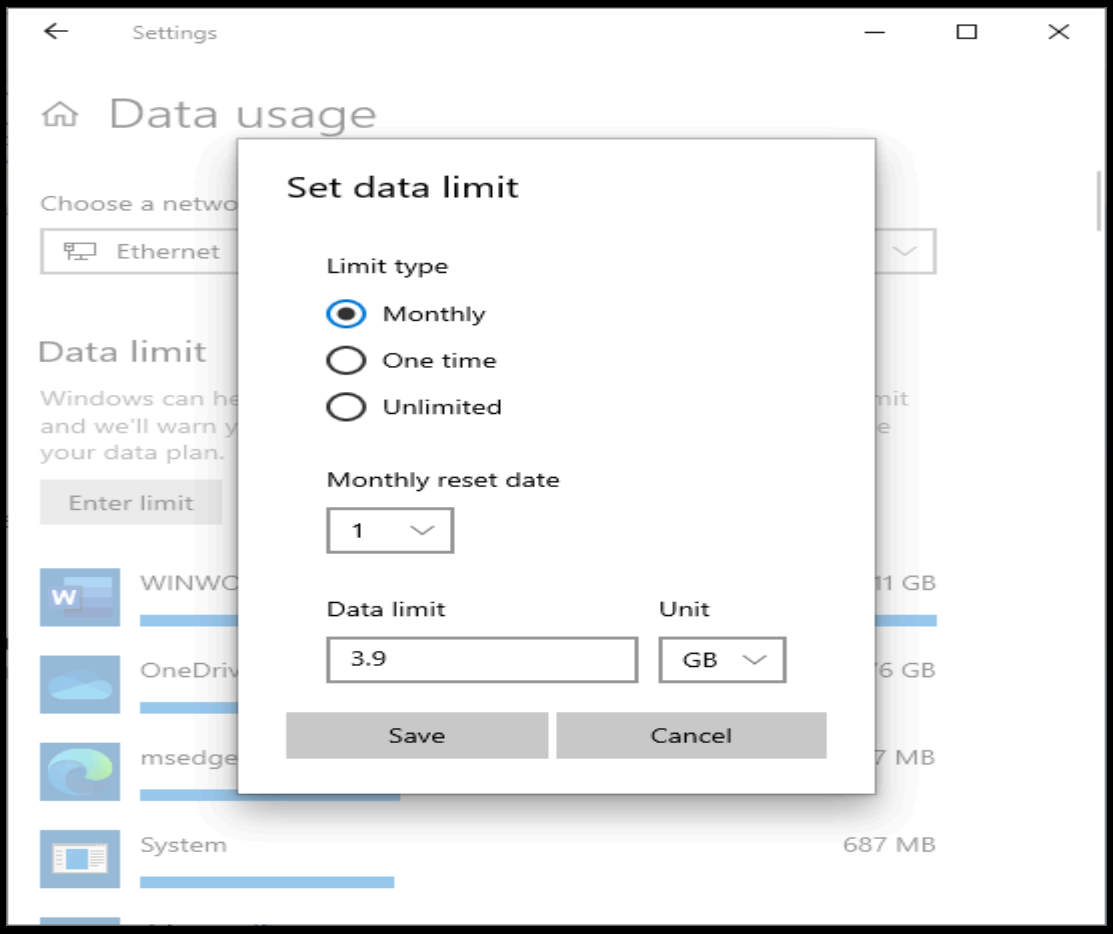
Subsequently, the network connection will be available via the network status icon. Right-click the icon and select the VPN connection icon to **Connect** or **Disconnect** or modify the connection's Properties.

Establish a Wireless Wide Area Network Connection

Wireless wide area network refers to using a cellular adapter to connect to the Internet via a provider's network. The bandwidth depends on the technologies supported by the adapter and by the local cell tower (3G, 4G, or 5G, for instance).

The WWAN adapter can be fitted as a USB device or as an internal adapter. For GSM and 4G or 5G services, the adapter must also be fitted with a subscriber identity module (SIM) card issued by the network provider. You can enable or disable the connection using the network status icon and configure it via Network & Internet settings.

Cellular providers can impose high charges if the subscriber's data allowance is exceeded. You can define the network type as **metered connection** and set a data limit within Windows to avoid the risk of exceeding the provider's cap. You can also monitor data usage by each app. Figure 2. Configuring a data limit for a metered network.



Description

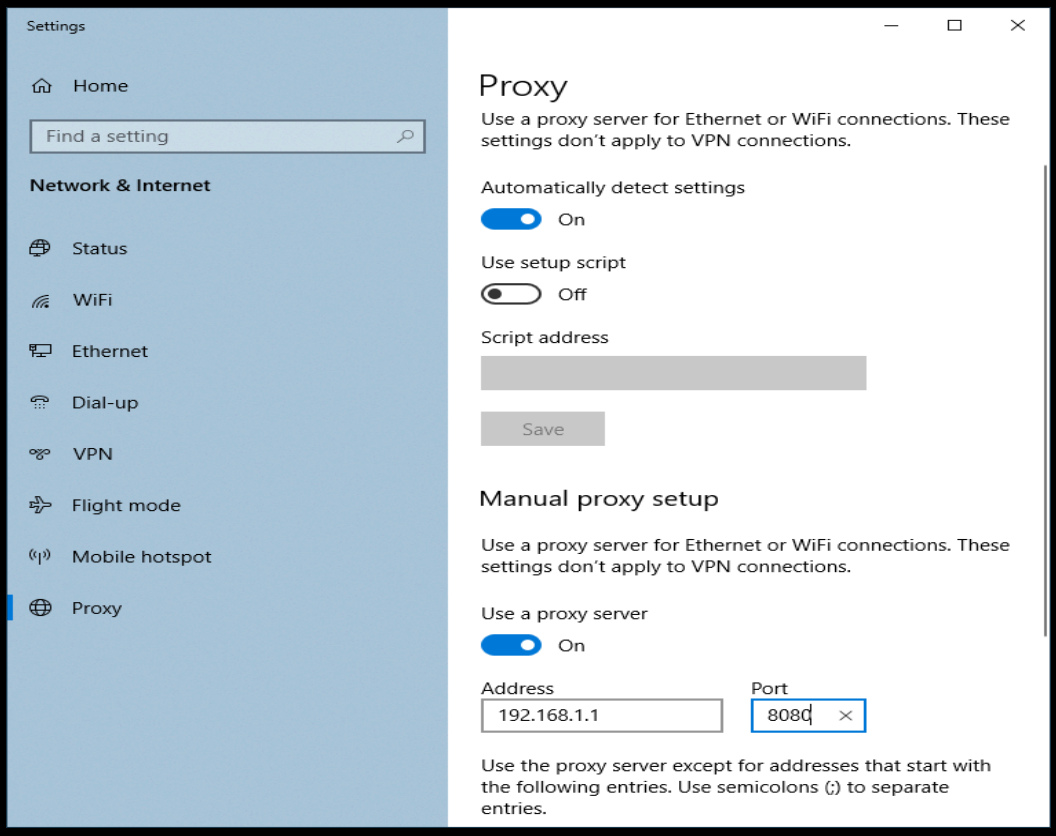
The options include limit types, Monthly, One time, and Unlimited. Monthly is selected. The monthly reset date is set to 1. The data limit is 3.9 and the unit is G B. The save and cancel buttons are at the bottom.

13.3.8 Proxy Settings

Some networks use a proxy to provide network connectivity. A **proxy server** can improve both performance and security. Client PCs pass Internet requests to the proxy server, which forwards them to the Internet. The proxy may also cache pages and content that is requested by multiple clients, reducing bandwidth.

An intercepting or transparent proxy does not require any client configuration and some proxies are autoconfiguring. If neither of these cases apply, each client must be configured with the IP address and TCP port to use to forward traffic via the proxy. These **proxy settings** are configured via Network & Internet settings.

Figure 1. Use the Settings app to apply a manual proxy setup



Screenshot courtesy of Microsoft.

Description

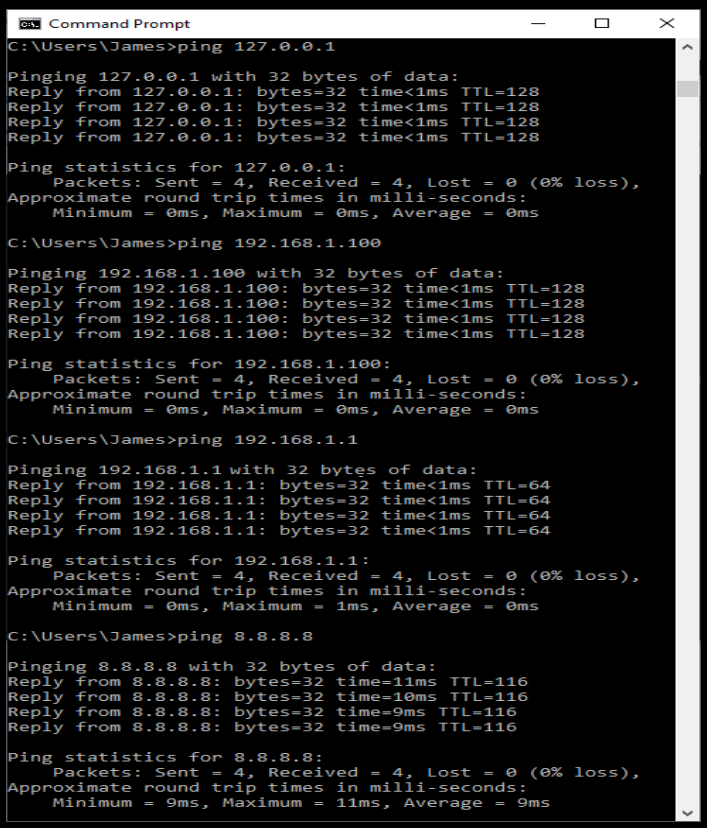
The menu on the left has a find a setting field at the top followed by options Status, Wi-Fi, Ethernet, Dial-up, V P N, Flight mode, Mobile hotspot, and Proxy under the head Network and Internet. The main panel has head Proxy followed by the text, use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to V P N connections. Automatically detect settings: A toggle switch is set to On. Use setup script: A toggle switch is set to Off. Under the manual proxy setup, use a proxy server is on. The fields for Address and Port are displayed, with the values 192.168.1.1 and 8080, respectively.

14.1.3 Troubleshoot Local Network Connectivity

If the link and IP configuration both seem to be correct, the problem may not lie with the local machine but somewhere in the overall network topology. You can test connections to servers such as file shares, printers, or email by trying to use them. One drawback of this method is that there could be some sort of application fault rather than a network fault. Therefore, it is useful to have a low-level test of basic connectivity that does not have any dependencies other than a working link and IP configuration.

The ping command utility is a command-line diagnostic tool used to test whether a host can communicate with another host on the same network or on a remote network. The following steps outline the procedures for verifying a computer's configuration and for testing router connections:

1. Ping the loopback address to verify TCP/IP is installed and loaded correctly (`ping 127.0.0.1`)—the loopback address is a reserved IP address used for testing purposes.
2. Ping the IP address of your workstation to verify it was added correctly and to check for possible duplicate IP addresses.
3. Ping the IP address of the default gateway to verify it is up and running and that you can communicate with a host on the local network.
4. Ping the IP address of a remote host to verify you can communicate through the router.
   Figure 1. Troubleshooting with ping

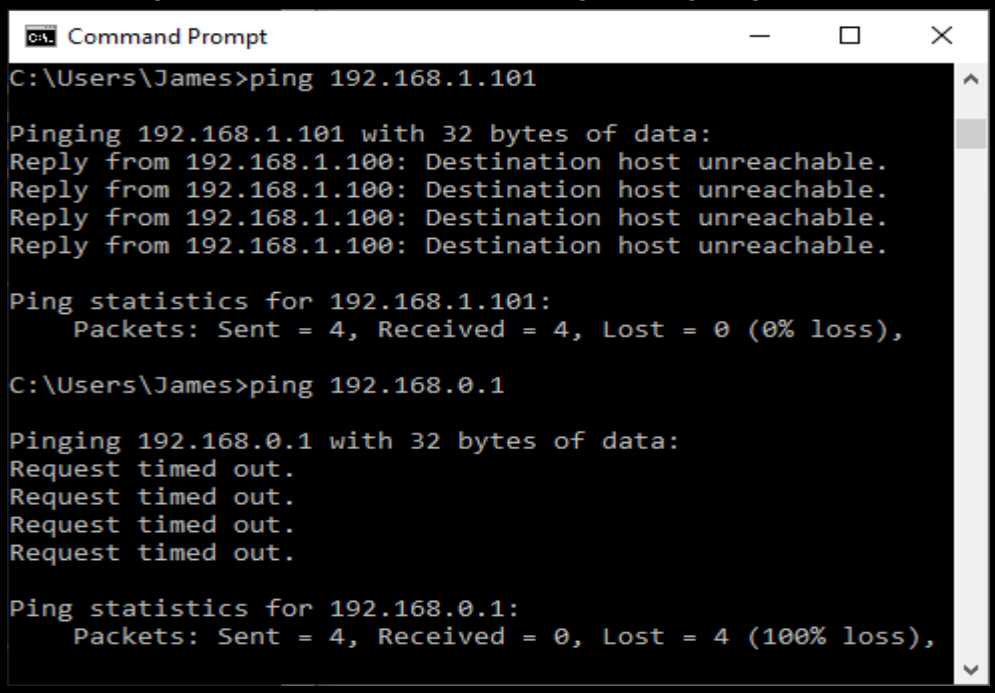


If ping is successful, it responds with the message **Reply from IP Address** and the time it takes for the host's response to arrive. The millisecond (ms) measures of round-trip time (RTT) can be used to diagnose latency problems on a link.

If ping is unsuccessful, one of three messages are commonly received:

- **Reply from *SenderIP* Destination unreachable**- If both hosts are supposed to be on the same local network segment, this means that the sending host gets no response to Address Resolution Protocol (ARP) probes. ARP is used to locate the hardware or media access control (MAC) address of the interface that owns an IP address. The most likely cause is that the destination host is disconnected or configured as non-discoverable. If you can confirm that the host is up, this could indicate some sort of IP misconfiguration, such as duplicate addresses or an incorrect subnet mask.
- **Reply from *GatewayIP* Destination unreachable**- The gateway router has no forwarding information for that IP address. This indicates some misconfiguration of the router or destination network.

- **No reply (Request timed out)**- The probe was sent to a remote host or network via the gateway, but no response was received. The most likely cause is that the destination host is down or configured not to respond. Figure 2. Examples of error messages using ping



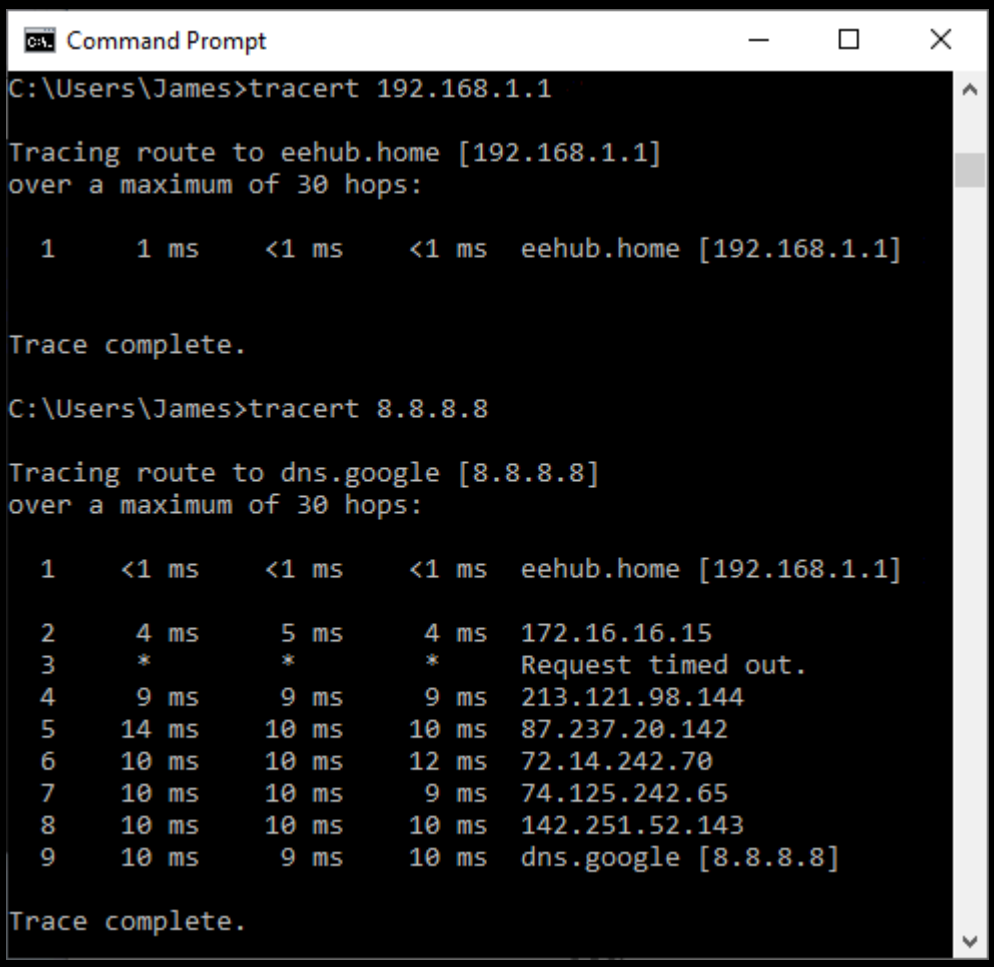
5. Note:
   The ping command in Windows will only send four packets for the connectivity text by default. To use ping with an unlimited number of packets, use the *ping -t* command. To stop the ping test, simply depress CTRL + C.

   You can also ping DNS names (`ping comptia.org`, for example) or FQDNs (`ping sales.comptia.org`, for instance). This will not work if a DNS server is unavailable. You can also force the DNS query to use IPv4 or IPv6 by using the -4 or -6 switches, respectively.

14.1.5 Troubleshoot Remote Network Connectivity

When a packet is forwarded to a remote network, each router in the path to the network counts as one hop. The path taken by a packet can be used to diagnose routing issues. The tracert command (pronounced trace route) line utility is used to trace the path a packet of information takes to get to its target. The command can take an IP address or FQDN as an argument.

Figure 1. Using tracert in Windows



Screenshot courtesy of Microsoft.

If the host cannot be located, the command will eventually timeout, but it will return every router that was attempted. The output shows the number of hops (when a packet is transferred from one router to another), the ingress interface of the router or host (that is, the interface from which the router receives the probe), and the time taken to respond to each probe in milliseconds (ms). If no acknowledgment is received within the timeout period, an asterisk is shown against the probe.

As an alternative to tracert, the pathping command performs a trace and then pings each hop router a given number of times for a given period to determine the round-trip time (RTT) and measure link latency more accurately. The output also shows packet loss at each hop.

If there is a routing issue, check that the local router’s Internet connection status is OK. If the router is connected, locate your ISP's service status page or support helpline to verify that there are no wider network issues or DNS problems that might make your Internet connection unavailable. If there are no ISP-wide issues, try restarting the router.

A+ Core 1 and Core 2 CertMaster Perform 15.0

14.1.6 Troubleshoot Name Resolution

If you cannot identify a problem with basic connectivity, you should start to suspect a problem at a higher layer of processing. There are three main additional "layers" where network services fail:

- **Security**- A firewall or other security software or hardware might be blocking the connection or proxy settings might be misconfigured.
- **Name resolution**- If a service such as DNS is not working, you will be able to connect to servers by IP address but not by name.
- **Application/OS**- The software underpinning the service might have failed. If the OS has failed, there might not be any sort of connectivity to the host server. If the server can be contacted, but not a specific service, the service process might have crashed.

When troubleshooting Internet access or unavailable local network resources, such as file shares, network printers, and email, try to establish the scope of the problem. If you can connect to these services using a different host, the problem should lie with the first client. If other hosts cannot connect, the problem lies with the application server or print device or with network infrastructure between the clients and the server.

If you identify or suspect a problem with name resolution, you can troubleshoot DNS with the nslookup command , either interactively or from the command prompt:

```
nslookup -Option Host Server
```

Host can be either a host name/FQDN or an IP address. *Server* is the DNS server to query; the default DNS server is used if this argument is omitted. -*Option* specifies a nslookup sub-command. Typically, a sub-command is used to query a particular DNS record type. For example, the following command queries Google's public DNS servers (8.8.8.8) for information about comptia.org's mail records:

```
nslookup -type=mx comptia.org 8.8.8.8
```

Figure 1. Using nslookup to query the mail server configured for the comptia.org domain name using Google's public DNS servers (8.8.8.8)

```
C:\Users\Admin>nslookup -type=mx comptia.org 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
comptia.org     MX preference = 10, mail exchanger = comptia-org.mail.protection.outlook.com

C:\Users\Admin>nslookup -type=ns comptia.org 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
comptia.org     nameserver = ns2.comptia.org
comptia.org     nameserver = ns1.comptia.org

C:\Users\Admin>nslookup -type=mx comptia.org ns1.comptia.org
Server:  UnKnown
Address:  209.117.62.56

comptia.org     MX preference = 10, mail exchanger = comptia-org.mail.protection.outlook.com

C:\Users\Admin>
```

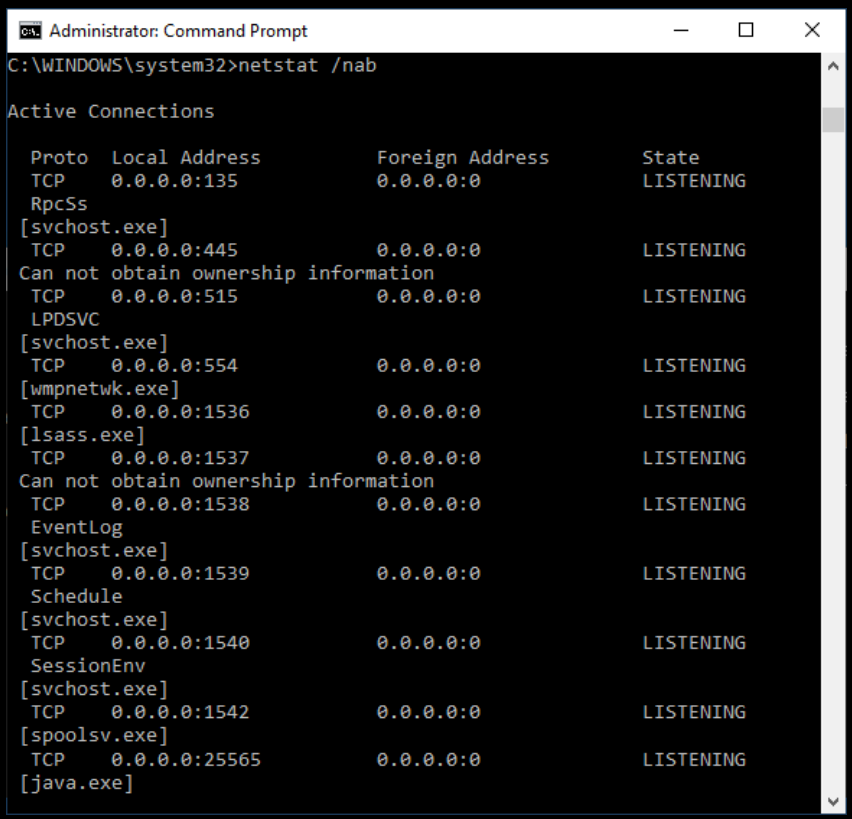
If you query a different name server, you can compare the results to those returned by your own name server. This might highlight configuration problems.

14.1.7 Troubleshoot Network Ports

The netstat command can be used to investigate open ports and connections on the local host. In a troubleshooting context, you can use this tool to verify whether file sharing or email ports are open on a server and whether other clients are connecting to them.

When used without switches, `netstat` lists active and listening TCP ports. An active port is connected to a foreign address, while a listening port is waiting for a connection. The following represent some of the main switches that can be used:

- `-a` includes UDP ports in the listening state.
- `-b` shows the process that has opened the port. Alternatively, use the `-o` switch to list the process ID (PID) rather than the process name. These switches can only be used from an administrative command prompt.
- `-n` displays ports and addresses in numerical format. Skipping name resolution speeds up each query.
- `-e` and `-s` can be used to report Ethernet and protocol statistics respectively. Figure 1. Listening connections and the processes that opened each port with netstat.



Screenshot courtesy of Microsoft.

14.2.1 Remote Desktop Tools

With remote desktop, the target PC runs a graphical terminal server to accept connections from clients. This allows a user to work at the desktop of a different computer over the network.

Remote desktop is often configured for laptop users working from home with a slow link. Having gained access to the corporate network (via the Internet using a VPN, for example) they could then establish a remote desktop connection to a PC in the office. A technician can also use a remote desktop access tool to configure or troubleshoot a computer.

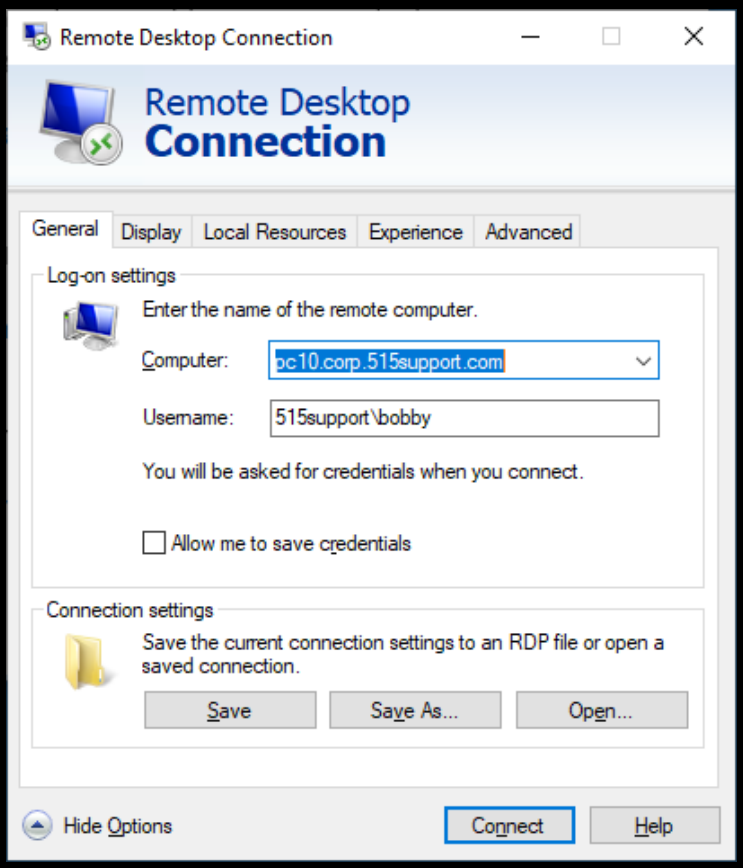
When allowing remote access to a host or network, you must assess and resolve security considerations:

- Remote access permissions should be granted to accounts selectively using least privilege principles.
- The connection must use encryption to be made secure against snooping. Users must have a means of confirming that they are connecting to a legitimate server to mitigate the risk of evil twin-type attacks. The server can be installed with a digital certificate to identify it securely.
- The server software supporting the connection must be safe from vulnerabilities, especially when the server port is accessible over the Internet.

Remote Desktop Protocol

Windows uses the **Remote Desktop Protocol (RDP)** to implement terminal server and client functionality. To connect to a server via Remote Desktop, open the **Remote Desktop Connection** shortcut or run `mstsc.exe` . Enter the server's IP address or fully qualified domain name (FQDN). Choose whether to trust the server connection, inspecting any certificate presented, if necessary.

Figure 1. Remote Desktop Connection client (mstsc.exe)



Description

The interface is open to the General tab, displaying fields for computer and username under the Log-on settings section. Below these fields, there is a checkbox labeled Allow me to save credentials, which is unchecked. In the Connection settings section, options are available to Save the current connection settings to an R D P file or open a saved connection. There are three buttons: Save, Save As, and Open. At the bottom, there are two prominent buttons labeled Connect and Help. The Hide Options button is displayed in the lower left corner.

You also need to define credentials for the remote host. To specify a domain account, use the format `Domain\Username`. To use a local account, use either `.\ Username` or `Host\Username`. RDP authentication and session data is always encrypted. This means that a malicious user with access to the same network cannot intercept credentials, interfere, or capture anything transmitted during the session.

Note:

A limitation of RDP on Windows is that only one person can be signed in at any one time. Starting an RDP session will lock the local desktop. If a local user logs in, the remote user will be disconnected.

There are versions of the mstsc client software for Linux, macOS, iOS, and Android, so you can use devices running those operating systems to connect to an RDP server running on a Windows machine.

Virtual Network Computing

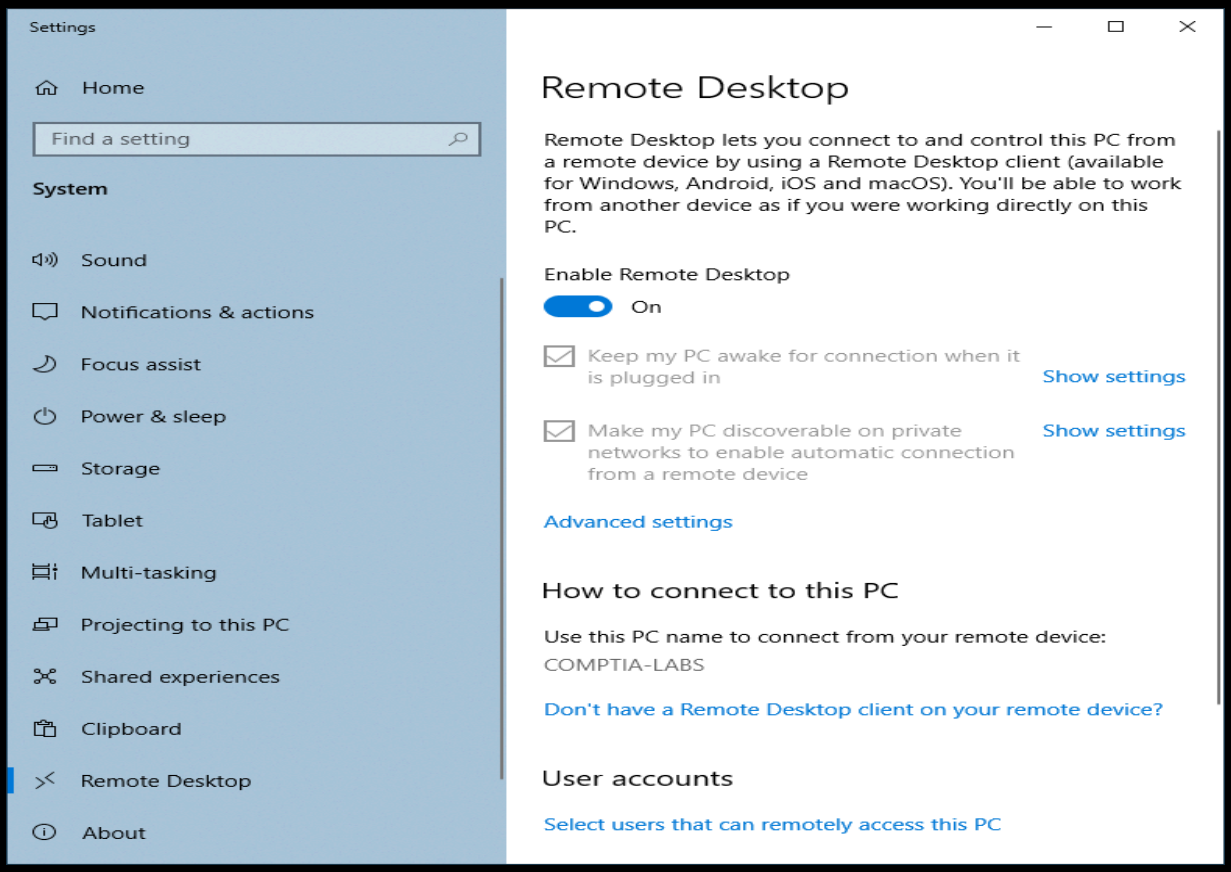
There are alternatives to using RDP for remote access. For example, in macOS, you can use the Screen Sharing feature for remote desktop functionality. Screen Sharing is based on the **Virtual Network Computing (VNC)** protocol. You can use any VNC client to connect to a Screen Sharing server.

VNC itself is a freeware product with similar functionality to RDP. It works over TCP port 5900. Not all versions of VNC support connection security. macOS Screen Sharing is encrypted.

14.2.2 RDP Server and Security Settings

A Remote Desktop server is not enabled by default. To change remote access settings, open the **Remote Desktop** page in the **Settings** app.

Figure 1. Configuring Remote Desktop server settings



Description

The menu on the left has a find a setting field at the top followed by options Display, Sound, Notifications and actions, Focus assist, Power and sleep, Storage, Tablet, Muti-tasking, Projecting to this PC, Shared experiences, clipboard, remote desktop, about under the head System. The right panel displays the title Remote Desktop and a description explaining that Remote Desktop allows connection to and control of the P C from another device using a Remote Desktop client available for Windows, Android, i O S, and mac O S. Below the description, there is a toggle switch labeled Enable Remote Desktop, which is set to On. Additional options include a checkbox labeled Keep my P C

awake for connections when it is plugged in, followed by a link to Show settings. Another checkbox labeled Make my P C discoverable on private networks to enable automatic connection, also followed by a link to Show settings. There is a link to Advanced settings under these options. The section How to connect to this P C provides instructions and displays the name of the computer as COMP T I A dash LABS. Below this, there is a link asking, Don't have a Remote Desktop client on your remote device. The final section, User accounts, includes a link labeled Select users that can remotely access this P C.

Use the **Select users** link to define which accounts are permitted to connect remotely. Users in the local administrators' group are allowed to connect by default. You can select users from the local accounts database or from the domain that the machine is joined to.

Under **Advanced settings**, you can choose between allowing older RDP clients to connect and requiring RDP clients that support Network Level Authentication (NLA). NLA protects the RDP server against denial-of-service attacks. Without NLA, the system configures a desktop before the user logs on. A malicious user can create multiple pending connections to try to crash the system. NLA authenticates the user before committing any resources to the session.

If Remote Desktop is used to connect to a server that has been compromised by malware, the credentials of the user account used to make the connection become highly vulnerable. RDP Restricted Admin (RDPRA) Mode and Remote Credential Guard are means of mitigating this risk. You can read more about these technologies at docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard.

The Remote Desktop server runs on TCP port 3389 by default but can be changed to another port.

Note:

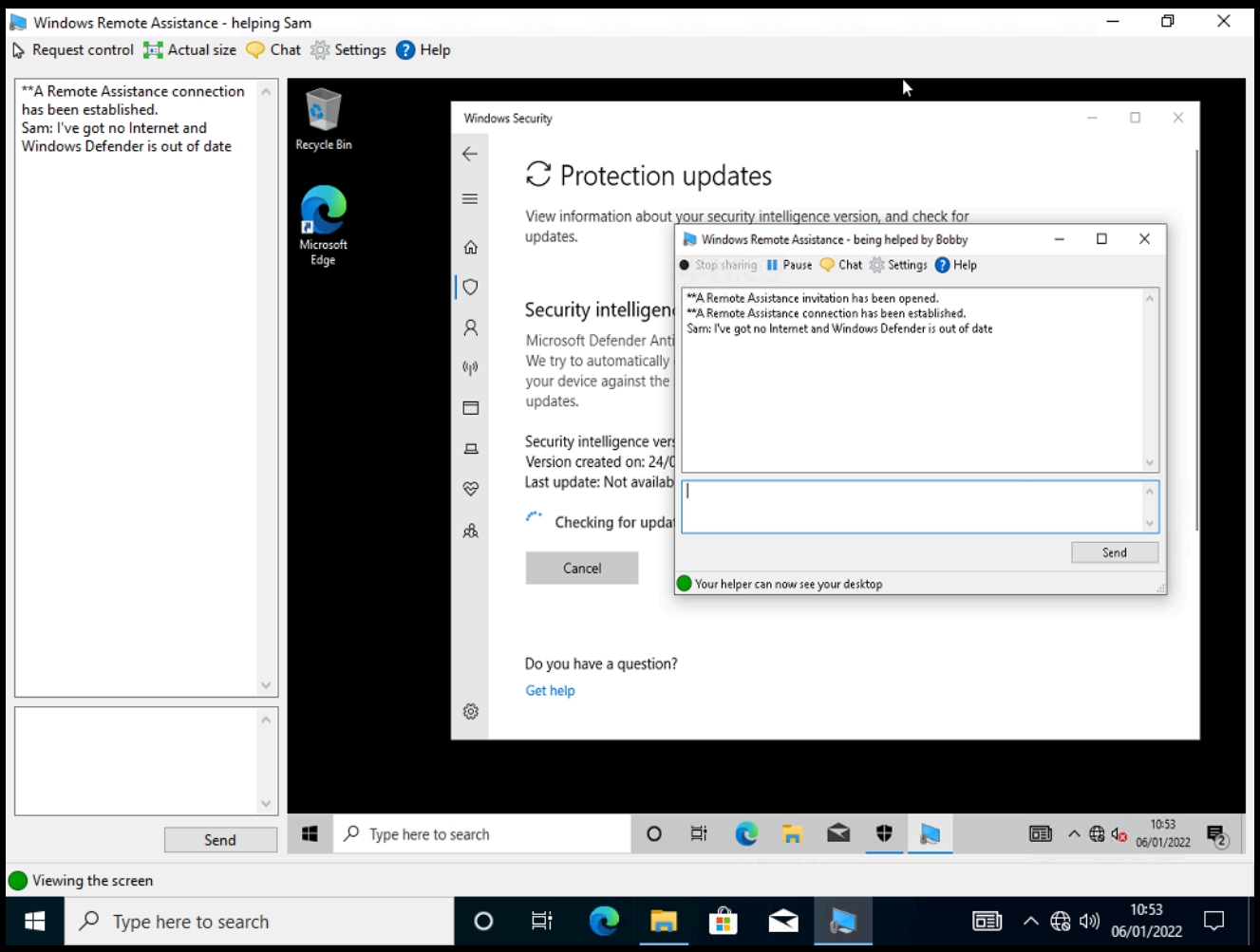
Windows Home editions do not include the Remote Desktop server, so you cannot connect to them, but they do include the client, so you can connect to other computers from them.

There are also open-source implementations of RDP, such as XRDP. You can use XRDP to run an RDP server on a Linux host.

14.2.3 Microsoft Remote Assistance

Remote Assistance allows a user to ask for help from a technician or co-worker via an invitation file protected by a passcode. The helper can open the file to connect over RDP and join the session with the user. There is a chat feature, and the helper can request control of the desktop.

Figure 1. Using Remote Assistance



Description

At the top of the session window, there is a toolbar with options like Request Control, Actual size, Chat, Settings, and Help. The session displays the remote user's screen, which is open to the Windows Security application in the

Protection Updates section. A chat window overlay titled Windows Remote Assistance - helping Sam is active in the foreground. The chat box reads, A remote assistance invitation has been opened. A remote assistance connection has been established. Sam: I've got no internet and windows defender is out of date. There is an empty text input field at the bottom of the chat window, followed by a Send button. The local system's taskbar is visible at the bottom, showing common Windows icons like Start, File Explorer, and various application shortcuts.

Remote Assistance assigns a port dynamically from the ephemeral range (49152 to 65535). This makes it difficult to configure a firewall securely to allow the connection. Windows 10 feature updates introduced the **Quick Assist** feature (CTRL +WINDOWS +Q) as an alternative to msra.exe. Quick Assist works over the encrypted HTTPS port TCP/443. The helper must be signed in with a Microsoft account to offer assistance. The helper generates the passcode to provide to the sharer.

Note:

Neither Remote Assistance nor Quick Assist allows the helper to perform tasks that require UAC consent in the default configuration. Either the Secure Desktop feature of UAC must be disabled, or UAC notifications need to be turned off or set to a lower level, weakening the security configuration.

14.2.5 WinRM

WinRM is Microsoft's implementation of the WS-Management protocol. It allows systems to exchange and access management information across a network. Being a Simple Object Access Protocol (SOAP) based program it relies on HTTP/HTTPS connections to communicate between the systems. The administrator can use the WinRM console to execute management commands on the system remotely. All current versions of Windows already include the WinRM application. It is used as one method to forward logs to a remote system for log collection and analysis.

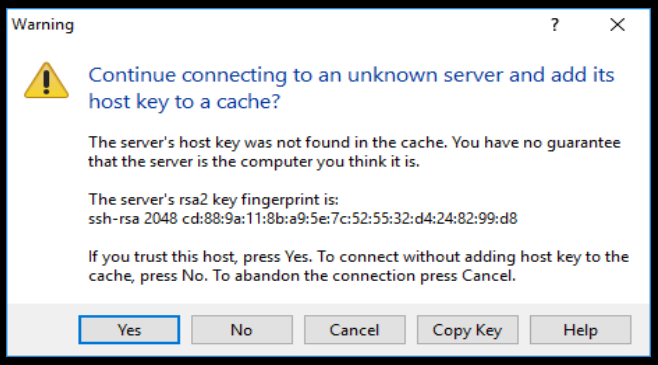
Security concerns about the use of WinRM include the ability for remote attackers to execute their own commands against the network device. Additional concerns of traffic being passed in clear text format when using HTTP are unfounded since WinRM utilizes Kerberos to encrypt the traffic before passing it through the HTTP connection.

14.2.6 Secure Shell

Secure shell is also a remote access protocol, but it connects to a command interpreter rather than a desktop window manager. SSH uses TCP port 22 (by default). SSH uses encryption to protect each session. There are numerous commercial and open-source SSH products available for all the major OS platforms.

Each SSH server is configured with a public/private encryption key pair, identified by a host key fingerprint. Clients use the host key fingerprint to verify that they are attempting to connect to a trusted server and mitigate the risk of on-path attacks. A mapping of host names to SSH server keys can be kept manually by each SSH client, or there are various enterprise software products designed for SSH key management.

Figure 1. Confirming the SSH server's host key



Below, it explains that The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is. The server's R S A 2 key fingerprint is shown as S S H dash R S A 2048 c d colon 88 colon 9 a colon 11 colon 8 b colon a 9 colon 5 e colon 7c colon 52 colon 55 colon 32 colon d 4 colon 24 colon 82 colon 99 colon d 8. The dialog offers instructions stating that if you trust this host, you can press Yes. To connect without adding the host key to the cache, press No, and to abandon the connection, press Cancel. There are five buttons at the bottom labeled Yes, No, Cancel, Copy Key, and Help.

The server's host key pair is used to set up an encrypted channel so that the client can submit authentication credentials securely. SSH allows various methods for the client to authenticate to the server. Each of these methods can be enabled or disabled as required on the server. Two commonly implemented methods are as follows:

- **Password authentication**- The client submits a username and password that are verified by the SSH server either against a local user database or using an authentication server.
- **Public key authentication**- The server is configured with a list of the public keys of authorized user accounts. The client requests authentication using one of these keys, and the server generates a challenge with the user's public key. The client must use the matching private key it holds to decrypt the challenge and complete the

authentication process.

Note:

Monitoring for and removing compromised client public keys is a critical security task. Many recent attacks on web servers have exploited poor SSH key management.

14.2.7 Desktop Management and Remote Monitoring Tools

Network visibility refers to the challenge of ensuring that every host communicating on the network is authorized to be there and is running in a secure configuration. It is impractical for a technician to regularly locate and visit each device, so visibility depends on remote monitoring and management technologies.

There are two general classes of tools that provide this type of enterprise desktop monitoring and remote access:

- **Remote monitoring and management (RMM)** tools are principally designed for use by managed service providers (MSPs). An MSP is an outsourcing company that specializes in handling all IT support for their clients. An RMM tool will be able to distinguish client accounts and provide support for recording and reporting billable support activity.
- **Desktop management**/mobile-device management (MDM) software suites are designed for deployment by a single organization and focus primarily on access control and authorization.

Given those distinctions, these tools have many features in common. In general terms, any given suite might offer a mix of the following functionality:

- Locally installed agent to report status, log, and inventory information to a management server and provide integration with support ticket/help desk systems. Most suites will support both desktop (Windows/Linux/macOS) and mobile (iOS/Android) hosts.
- Agent that also performs **endpoint detection and response** security scanning.
- Automated “push” deployment of upgrades, updates, security-scanner definitions, apps, and scripts plus management of license compliance.
- Remote network boot capability, often referred to as wake on LAN (WOL), plus ability to enter system firmware setup and deploy firmware updates and OS installs.
- Access control to prevent hosts that do not meet OS version/update or other health policies from connecting to the network.
- Live chat and remote desktop and/or remote shell connection to hosts.

A software agent depends on the OS to be running to communicate with the management server. The management suite can also be configured to take advantage of a hardware controller, such as Intel vPro or AMD PRO, to implement out-of-band (OOB) management and power on a machine remotely.

14.2.8 Simple Protocol for Independent Computing Environments (SPICE)

The Simple Protocol for Independent Computing Environments provides a remote display system to monitor and interact with virtual machine environments from across the Internet. The server and client relationship is used for the protocol by allowing the server to monitor and interact with each client. Security of the machines is provided through various authentication options such as Kerberos. It also provides for a secure TLS mode which enables encryption of the traffic transmitted between the server and client machines.

14.2.9 Other Remote Access Tools

Enterprise monitoring suites are designed for environments with large numbers of desktops, and the cost can be prohibitive when managing just a few machines. Other protocols and software tools are available for accepting incoming connections to non-Windows devices and can be more suitable for the management of SOHO networks.

Screen-sharing Software

There are many third-party alternatives to the sort of **screen sharing** and remote-control functionality implemented by MSRA/Quick Assist. Examples include TeamViewer and LogMeIn. Like Quick Assist, these products are designed to work over HTTPS (TCP/443) across the Internet, which is secure because the connection is encrypted and is easier to implement as it does not require special firewall rules.

Some tools require the app to be installed locally, while others can be executed non-persistently. The user can grant access to an assistant or technician by giving them a PIN code generated by the local software installation.

Users must be made aware of the potential for threat actors to use social engineering to persuade them to allow access. When used in a corporate environment, there should be a specific out-of-band verification method for users to confirm they are being contacted by an authorized technician.

Video-conferencing Software

Most **video conferencing** or web-conferencing software, such as Microsoft Teams or Zoom, includes a screen-share client, and some also allow participants to be granted control of the share. The share can be configured as a single window or the whole desktop. The share will have the privileges of the signed-in user, so these apps cannot be used to perform any administrator-level configuration, but they are useful for demonstrating a task to a user or reproducing a support issue by observing the user.

File Transfer Software

Setting up a network file share can be relatively complex. You need to select a file-sharing protocol that all the connecting hosts can use and that allows configuring permissions on the share and provisioning user accounts that both the server and client recognize. Consequently, OS vendors have developed other types of file transfer software:

- **AirDrop**—Supported by Apple iOS and macOS, this uses Bluetooth to establish a Wi-Fi Direct connection between the devices for the duration of the file transfer. The connection is secured by the Bluetooth pairing mechanism and Wi-Fi encryption.

- **Nearby Sharing**—Microsoft's version of AirDrop. Nearby Sharing was introduced in Windows 10 (1803).
- **Nearby Share**—Bluetooth-enabled sharing for Android devices.

Although the products have security mechanisms, there is always the potential for misuse of this kind of file transfer feature. Users accepting connections from any source could receive unsolicited transfer requests. It is best to only accept requests from known contacts. The products can be subject to security vulnerabilities that allow unsolicited transfers.

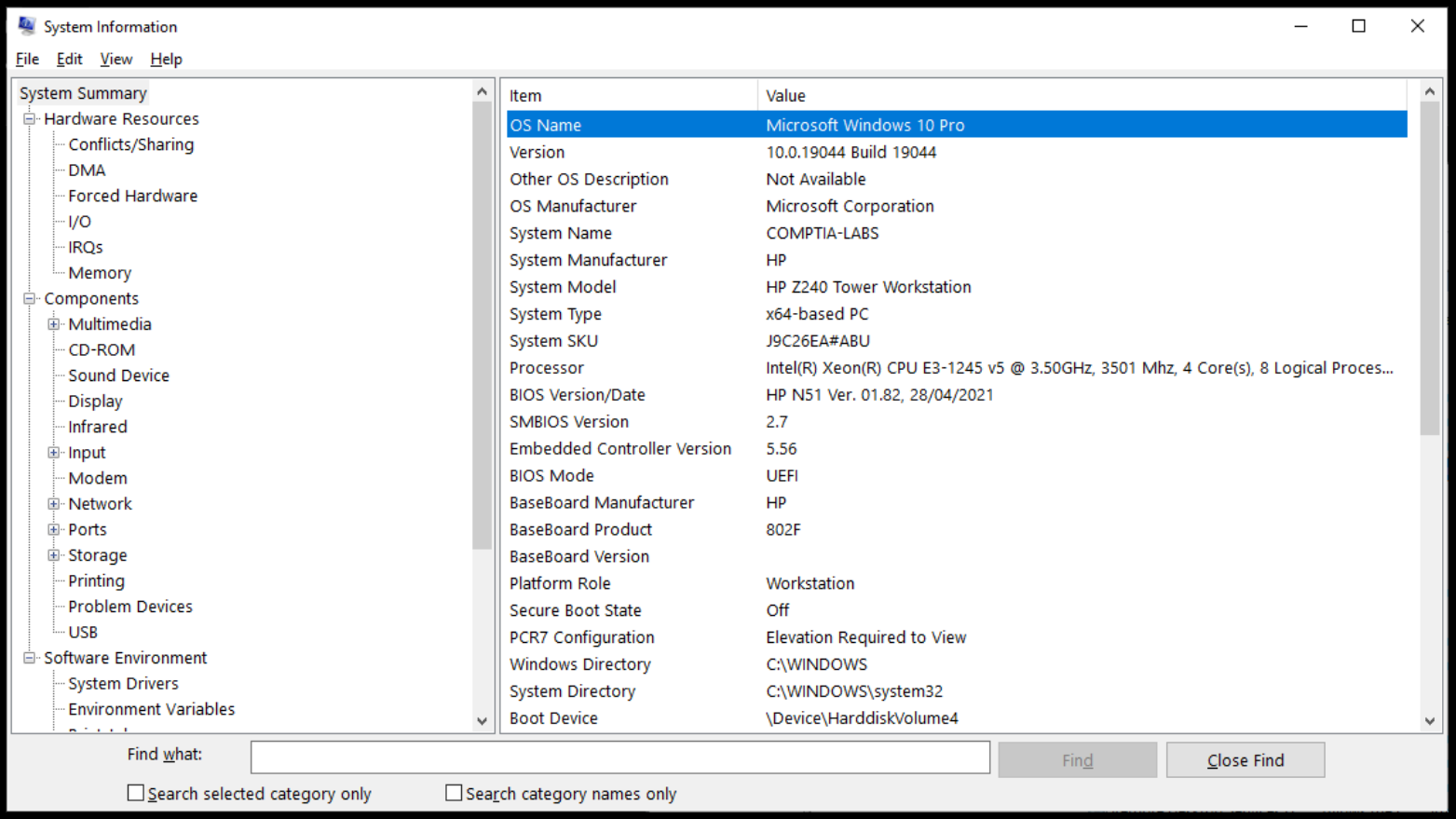
Virtual Private Networks

Where remote desktop or SSH establishes a connection to a single host over the network, a virtual private network (VPN) establishes a tunneled link that joins your local computer to a remote network. The VPN could be used as an additional layer of security. For example, you could establish a VPN link and then use a remote desktop to connect to a host on the private network. This avoids having to open remote desktop ports on the network's firewall.

14.3.1 System Information

The **System Information tool (msinfo32.exe)** generates a comprehensive report on the system's hardware and software components. It provides an inventory of system resources, firmware and OS versions, driver file locations, environment variables, and network status.

Figure 1. System Information report



Description

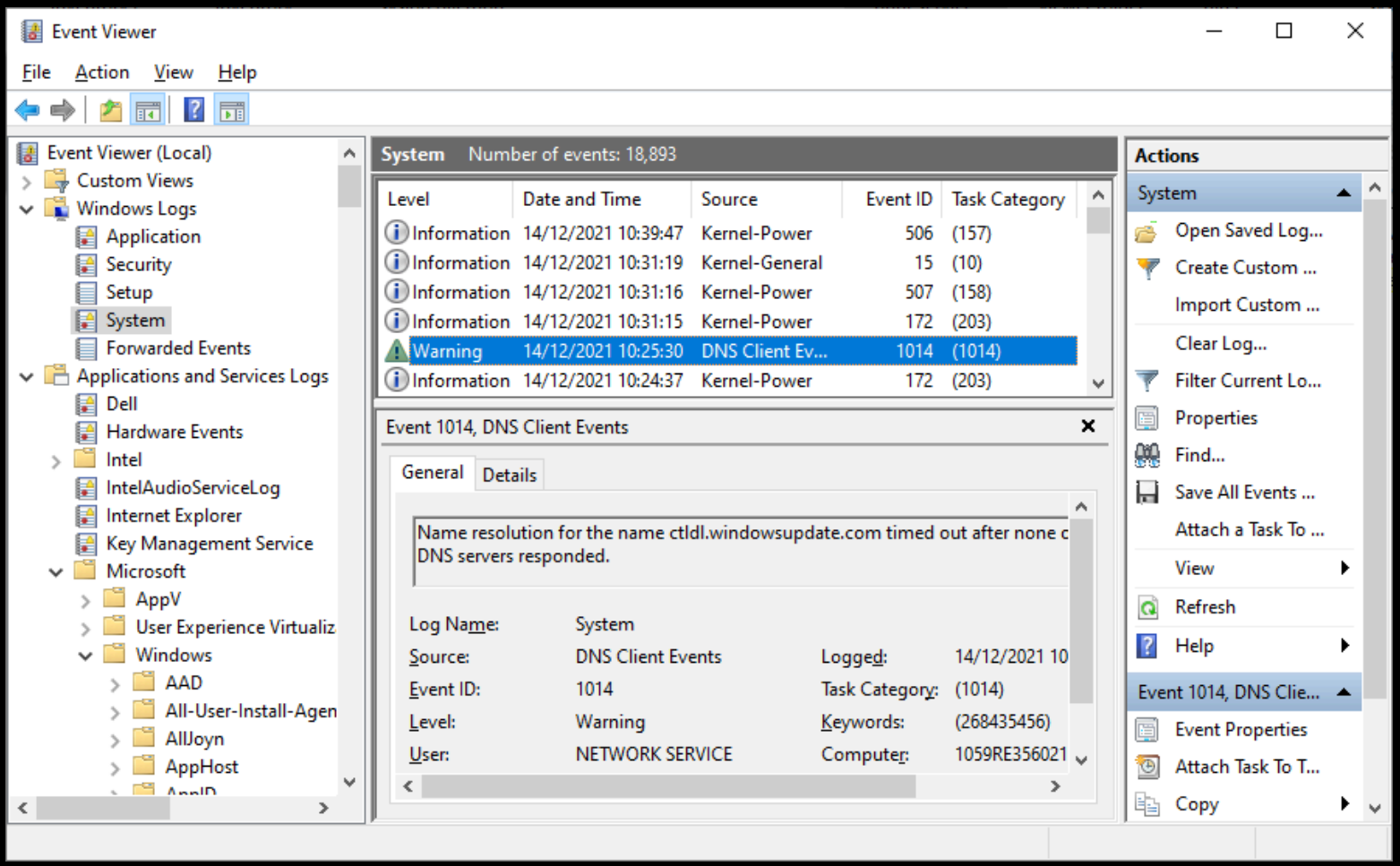
The system summary menu is on the left. A table on the right displays the item and its value. The item OS name with the value Microsoft Windows 10 Pro is selected. A field to find what is at the bottom. Checkboxes for search selected category only and search category names only are below the find what field. The find and close find buttons are on the right.

14.3.2 Event Viewer

When Windows detects a problem, it generates an error message to aid troubleshooting. You can look up these messages using the Microsoft Knowledge Base (support.microsoft.com) or third-party support sites.

Event Viewer (eventvwr.msc) is a management console snap-in for viewing and managing logs on a Windows host. The default page summarizes system status, displaying recent errors and warnings. The left pane categorizes log files.

Figure 1. Reviewing the System log in Windows 10 Event Viewer management console



Screenshot courtesy of Microsoft.

Description

The left pane shows a hierarchical navigation tree with options like Custom Views, Windows Logs, and Applications and Services Logs. The middle section lists events, including their level, date and time, source, event I D, and task category. The bottom pane provides detailed information about the selected event, including a warning message about a D N S query timeout. The right-hand pane includes action options.

Default Log Files

The Windows Logs folder contains four main log files:

- System Log: Records events affecting the core OS, such as service load failures, hardware conflicts, driver load failures, and network issues.
- Application Log: Contains information on non-core processes, utilities, and some third-party apps, like app installers write events to the Application log.
- Security Log: Holds audit data for the system.
- Setup Log: Records installation events.

Each log file has a default maximum size (usually about 20 MB), adjustable via **Properties**. You can set the overwrite option to overwrite, do not overwrite, or archive (close the current file and start a new one).

Note:

Monitor log preservation carefully, as archive logs can grow large if unmonitored.

Additional logs under **Applications and Services Logs** are useful for troubleshooting specific Windows features, services, or third-party applications.

Event Sources and Severity Levels

Each event is generated by a source application and assigned an ID and severity level:

- **Critical**: Highest priority issues, often indicating a halted or unresponsive process.
- **Error**: Less severe issues to investigate after resolving critical ones.
- **Warning**: Conditions that could lead to errors or critical issues if not addressed, like low disk space.
- **Information**: Noteworthy operations or states that don't require action.
- **Audit Success/Failure**: Security log events indicating successful actions, like user authentication, or failures, like incorrect password entries.

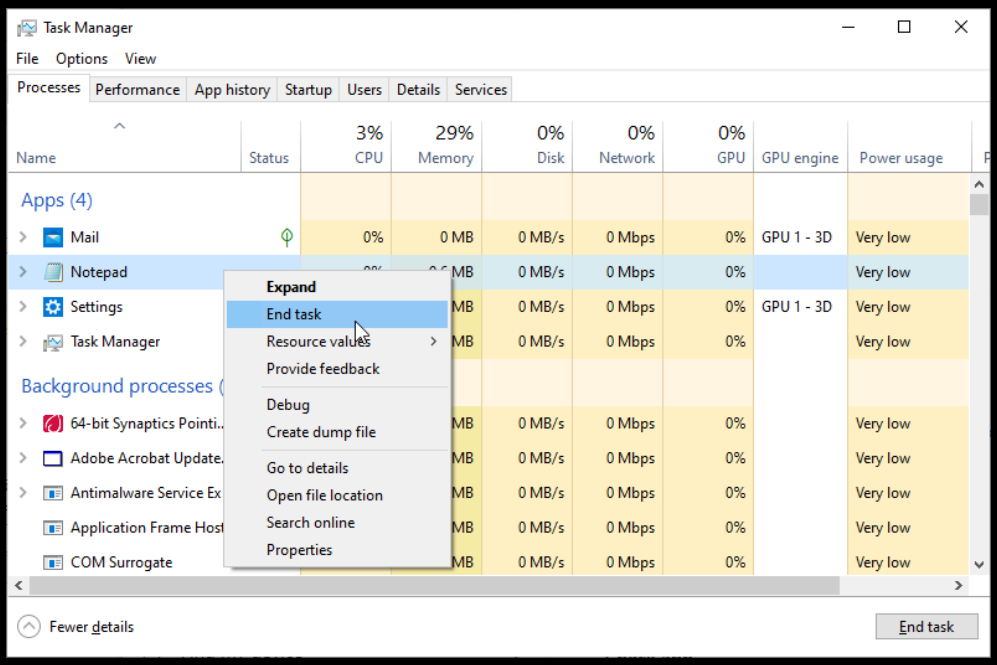
Double-click an event for a full description and more information.

14.3.3 Task Manager Process Monitoring

Task Manager monitors your PC's key resources. Open it by pressing **CTRL+SHIFT+ESC**, right-clicking the taskbar or Start, or pressing **CTRL+ALT+DEL** and selecting Task Manager.

If it starts in summary mode, click "Show details" to expand it. On the **Processes** tab, expand each app or background **process** to view sub-processes and resource usage.

Figure 1. Windows 10 Task Manager—Processes tab



Screenshot courtesy of Microsoft.

Description

The Processes tab is active, showing a list of running applications and background processes. Applications such as Mail, Notepad, Settings, and Task Manager are listed under Apps, with columns displaying metrics like C P U usage, memory, disk activity, network activity, G P U, G P U engine, and power usage. The Notepad application is highlighted, and a context menu is open, offering options such as Expand, End Task, Resource Values, Provide Feedback, Debug, Create dump file, Go to details, Open File Location, Search Online, and Properties. At the bottom, the End Task button is below.

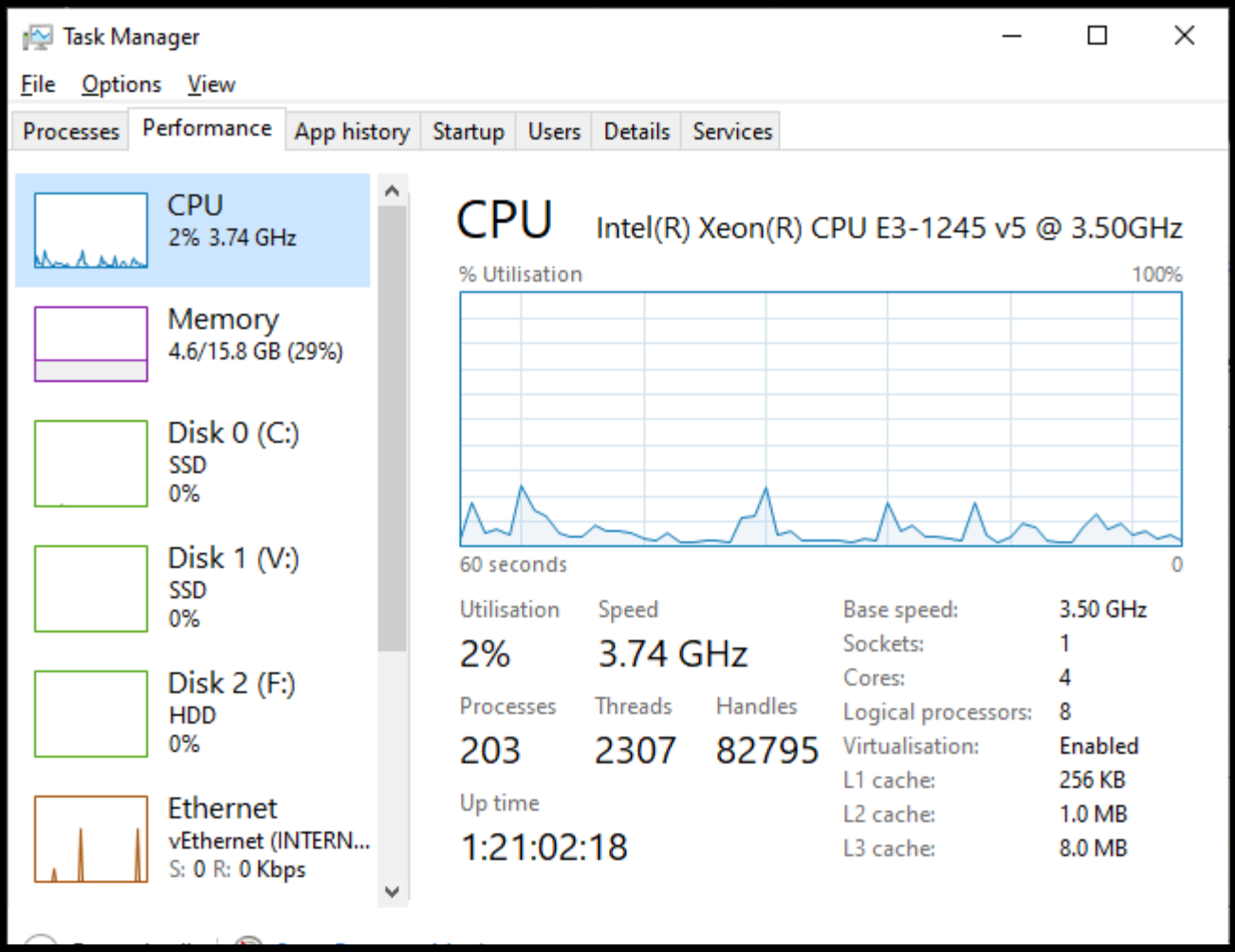
The shortcut menu for a process lets you end a task or search for information about the process online. For more details, use the **Details** tab to identify services associated with each process.

To prioritize tasks, right-click a process and select an option from the **Set Priority** submenu. For instance, setting a Voice over IP application's priority to **Above normal** may improve call quality by allocating more CPU resources to it.

14.3.4 Task Manager Performance Monitoring

The **Performance** tab offers detailed information about the CPU, memory, disk, network, and graphics processing unit (GPU) subsystems. The **App History** tab displays usage information for Windows Store apps.

Figure 1. Performance tab in Task Manager showing CPU utilization



Screenshot courtesy of Microsoft.

Description

The left panel lists system components, including C P U, Memory, Disk 0 (C colon), Disk 1 (V colon), Disk 2 (F colon), and Ethernet. The C P U section is selected, displaying real-time usage statistics for an Intel (R) X e o n C P U E 3 dash 1 2 4 5 v 5 at 3 dot 5 0 Gigahertz. The main pane includes a graph depicting C P U utilization over time, currently at 2 percent. Additional details include Base Speed (3.74 Gigahertz), Processes (203), Threads (2307), Handles (82795), and Uptime (1 day, 21 hours, 2 minutes, and 18 seconds). The other details are available on the right. At the bottom, a link labeled Open Resource Monitor is available for further analysis.

Disk Monitoring

The Disk pages display type, capacity, and statistics for active time, response time, and read/write speeds.

Note:

Utilization is measured across all disk devices. For instance, 50% utilization might mean one disk is at 100% while another is inactive.

High disk utilization and slow response times can cause poor system performance, potentially due to slow HDD technology, excessive paging, file/cache corruption, or faulty devices with bad sectors/blocks.

Network Monitoring

The **Ethernet** or **Wi-Fi** tab displays send and receive throughput for the active network adapter, along with the IP address and MAC address. For active wireless adapters, it also shows the SSID, connection type (802.11 standard), and signal strength.

14.3.5 CPU and GPU Monitoring

The **CPU** page shows the number of cores and logical processors (HyperThreading), whether the system is multisocket, and whether virtualization is enabled. The statistics show overall utilization, system uptime, and a count of the number of processes, threads, and handles. Higher numbers indicate more activity. Each process can run operations in multiple threads and can open handles to files, registry keys, network pipes, and so on.

High peak values for utilization are nothing to worry about, but sustained periods of high utilization mean that you should consider adding more resources to the system (or run fewer processes!).

The GPU page is shown if the system has a dedicated graphics adapter. It reports the amount of graphics memory available and utilization statistics.

14.3.6 Memory Monitoring

The **Memory** page reports which slots have modules installed and the speed. The usage statistics are broken down as follows:

- **In use** refers to system (RAM) usage only.
- **Committed** reports the amount of memory requested and the total of system plus paged memory available. Paged memory refers to data that is written to a disk pagefile.
- **Cached** refers to fetching frequently used files into memory pre-emptively to speed up access.
- **Paged pool** and **non-paged pool** refer to OS kernel and driver usage of memory. Paged usage is processes that can be moved to the pagefile, while non-paged is processes that cannot be paged.

High physical memory utilization up to the amount of system RAM isn't necessarily a sign of poor performance as it's good to make full use of the resource. High pagefile utilization is more problematic.

14.3.7 Disk and Network Monitoring

Disk Monitoring

The **Disk** pages report the type and capacity plus statistics for active time, response time, and read/write speeds.

Note:

Note that utilization is measured across all disk devices. For example, 50% utilization could mean one disk working at 100% and the other seeing no activity.

High disk utilization and slow response times are common causes of poor overall system performance issues. This could be a result of slow HDD technology, excessive paging activity, file/cache corruption, or a faulty device with bad sectors/blocks.

Network Monitoring

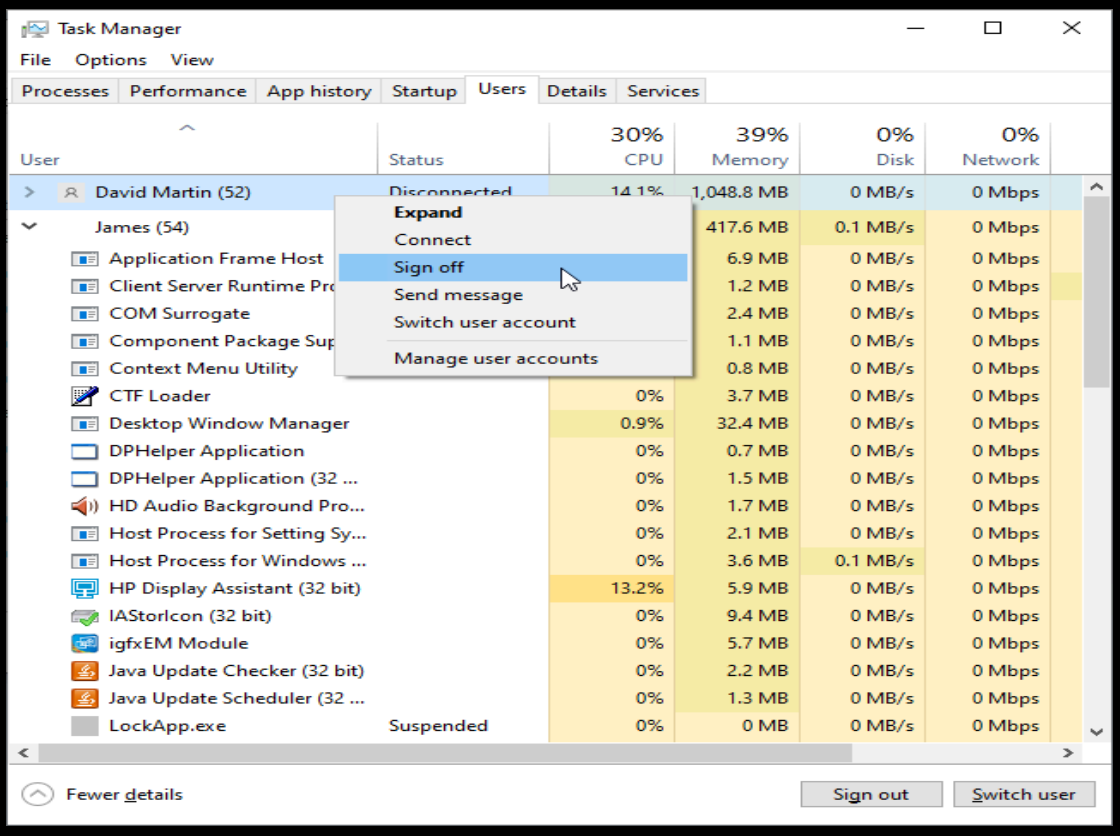
The **Ethernet** or **Wi-Fi** tab reports send and receive throughput for the active network adapter plus the IP address and hardware (MAC) interface address. If a wireless adapter is active, the SSID, connection type (802.11 standard), and signal strength are also shown.

14.3.8 Task Manager User Monitoring

The **Users** tab in Task Manager lets you:

- View all logged-in users.
- Send messages to users.
- Sign out users.
- See each user's running processes.
- Monitor resource usage (CPU, memory, disk) per user.

Figure 1. Using Task Manager to manage users



Screenshot courtesy of Microsoft.

Description

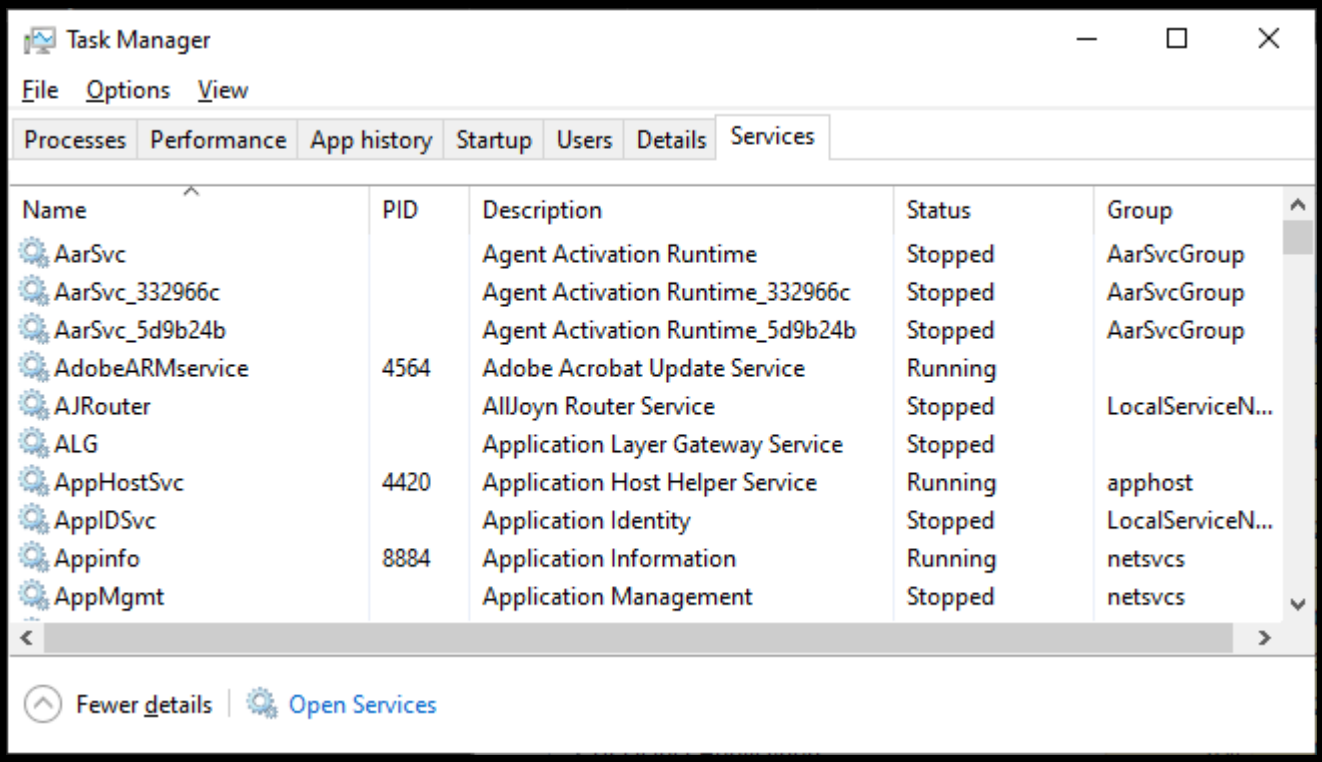
The tab shows a list of active users along with their resource usage. The user David Martin is highlighted, with a context menu open that provides options such as Expand, Connect, Sign Off, Send Message, Switch User Account, and Manage User Accounts. Sign Off is selected. The columns display information like Status, C P U usage, Memory usage, Disk activity, and Network activity. At the bottom, buttons labeled Sign Out and Switch User are visible, providing quick access to these actions.

14.3.9 Startup Processes and Services Console

The **Startup** tab allows you to disable programs set to run at startup from the Startup folder or registry. Right-click the headers to view the **startup type** and each item's impact on boot times.

The **Services** tab tracks all background services, which run without any user interaction. These services support Windows functions like logon, network browsing, and file indexing. Services can be installed by Windows or other applications like antivirus, database, or backup software.

Figure 1. Monitoring service status using Task Manager



Description

The tab lists services along with columns displaying their Name, P I D (Process I D), Description, Status, and Group. At the bottom, a link labeled Open Services is visible. The interface also has options to show more or fewer details.

Use the "Open Services" button in Task Manager to access the **Services console**, where you can disable nonessential services for better performance or security. Set services to Manual to prevent startup execution or **Disabled** to stop them entirely, but be cautious of dependencies.

If issues occur, ensure dependent services are running, and consider restarting services as a first troubleshooting step.

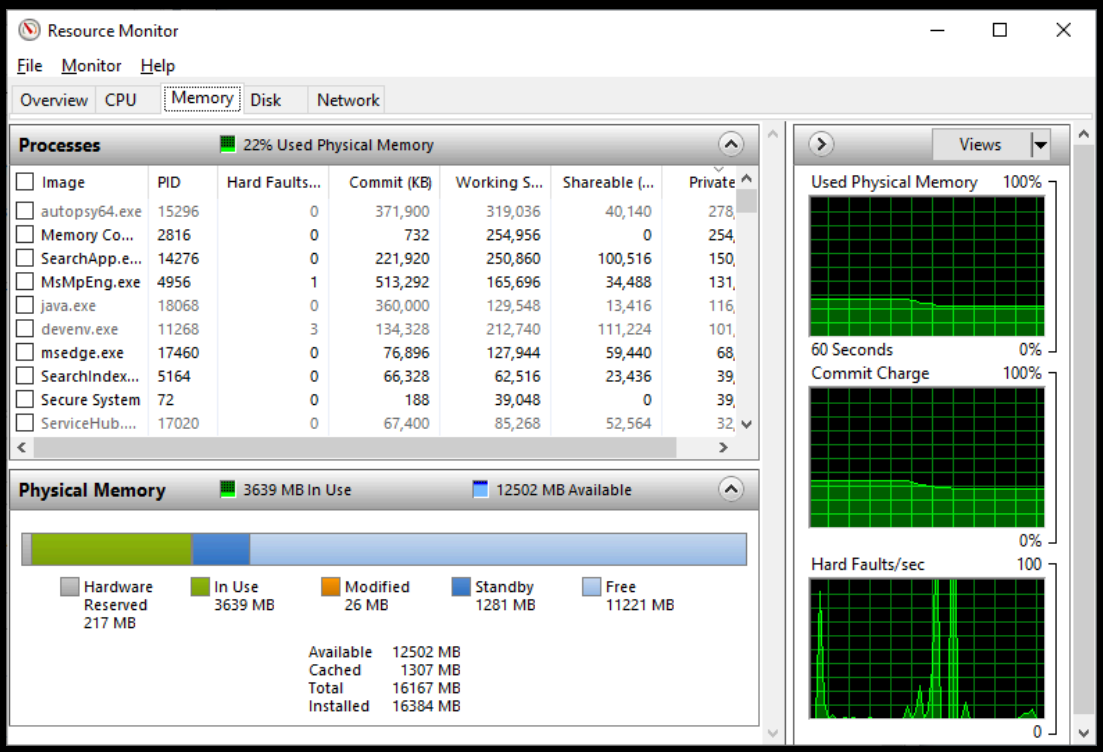
14.3.11 Resource Monitor and Performance Monitor

Task Manager can be used to assess key system statistics quickly, but there are other tools for more detailed performance monitoring.

Resource Monitor

Resource Monitor (resmon.exe) offers advanced snapshot monitoring beyond Task Manager, displaying resource performance graphs and key statistics like threads initiated by a process and hard page faults per second. A continuous rise in these numbers may signal a problem.

Figure 1. Viewing system memory utilization in Resource Monitor



Screenshot courtesy of Microsoft.

Description

The top section lists processes with columns showing details such as Process Name, P I D (Process I D), Hard Faults Per Second, Commit in kilobytes, Working Set in kilobytes, Shareable in kilobytes, and Private in kilobytes. The bottom section features the Physical Memory overview, highlighting categories such as Hardware Reserved, In Use, Modified, Standby, and Free, with a total memory usage summary. On the right, graphs display real-time data for Used Physical Memory, Commit Charge, and Hard Faults Per Second.

Performance Monitor

Windows **Performance Monitor** (perfmon.exe) offers real-time system resource charts and logs data for long-term analysis. These charts and logs are more detailed than the Performance tab of Task Manager. By monitoring resources at various times, you can identify system bottlenecks causing issues, such as application freezes. These may result from a slow processor, hard disk, or network link. Performance Monitor helps determine which component upgrades are critical.

You can create log files, known as Data Collector Sets, to record performance data over time, establishing a system baseline for long-term analysis. There are two log types:

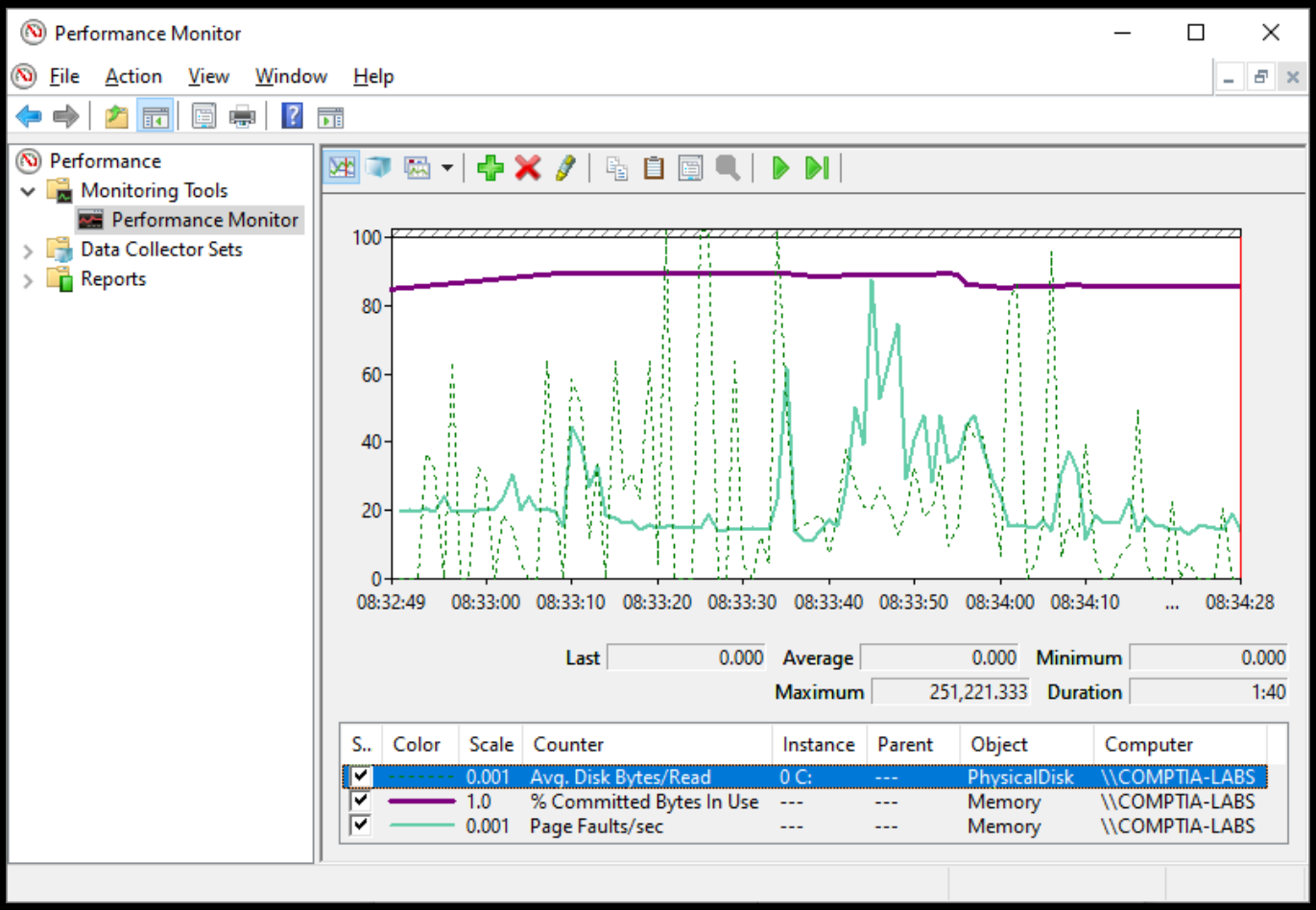
- **Counter Logs:** Collect statistics on resources like memory, disk, and processor to assess system health and performance.
- **Trace Logs:** Gather detailed service statistics, offering detailed reports on resource behavior. They extend the capabilities of the Event Viewer by logging data that would otherwise be inaccessible.

Saved logs can be analyzed in Performance Monitor from the Reports folder or exported to other programs for further examination.

14.3.12 Performance Counters

To configure a counter log in Performance Monitor, choose the resources to monitor. Resources like memory and disks are grouped into objects. Objects contain counters that represent various performance statistics, and multiple instances of the same object type can exist. For example, disk performance is measured using the **Physical Disk Object**, with the **Average Queue Length** as a useful counter. If there are two disks, you can view three instances: disk 0, disk 1, and disks Total.

Figure 1. Using Performance Monitor to record three counters from the PhysicalDisk and Memory objects



Description

The window displays a line graph representing system performance data over time. The graph tracks metrics such as average disk bytes read, committed bytes in use, and page faults per second shown in different colors to distinguish each counter. The fields below the graph list data for last, average, minimum, maximum, and duration. Below the graph, a table provides details for each performance counter, including columns like Color, Scale, Counter, Instance, Parent, Object, and Computer.

Some of the most used counters are listed here:

Object	Counter	Description
Processor	% Processor Time	Measures non-idle thread execution time and should be low in general. Sustained values over 85% may indicate a bottleneck.
	% Privileged Time % User Time	High processor time (over 85% for sustained periods) can be analyzed by comparing these. A significantly higher privileged time suggests the CPU may be underpowered (it can barely run Windows core processes efficiently).
Physical Disk	% Disk Time	The percentage of time the selected disk drive is occupied with read or write requests serves as a strong indicator of disk activity. If this average exceeds 85% for an extended period, it may indicate a disk problem.
	Average Disk Queue Length	Shows outstanding disk requests. Taken with the preceding counter, this gives a better indicator of disk problems. For example, high values alongside high disk time suggest disk problems.
Memory	Available Bytes	The amount of available memory should not be below 10% of the total RAM. Continuous decline may indicate a memory leak (a process that allocates memory but does not release it again).

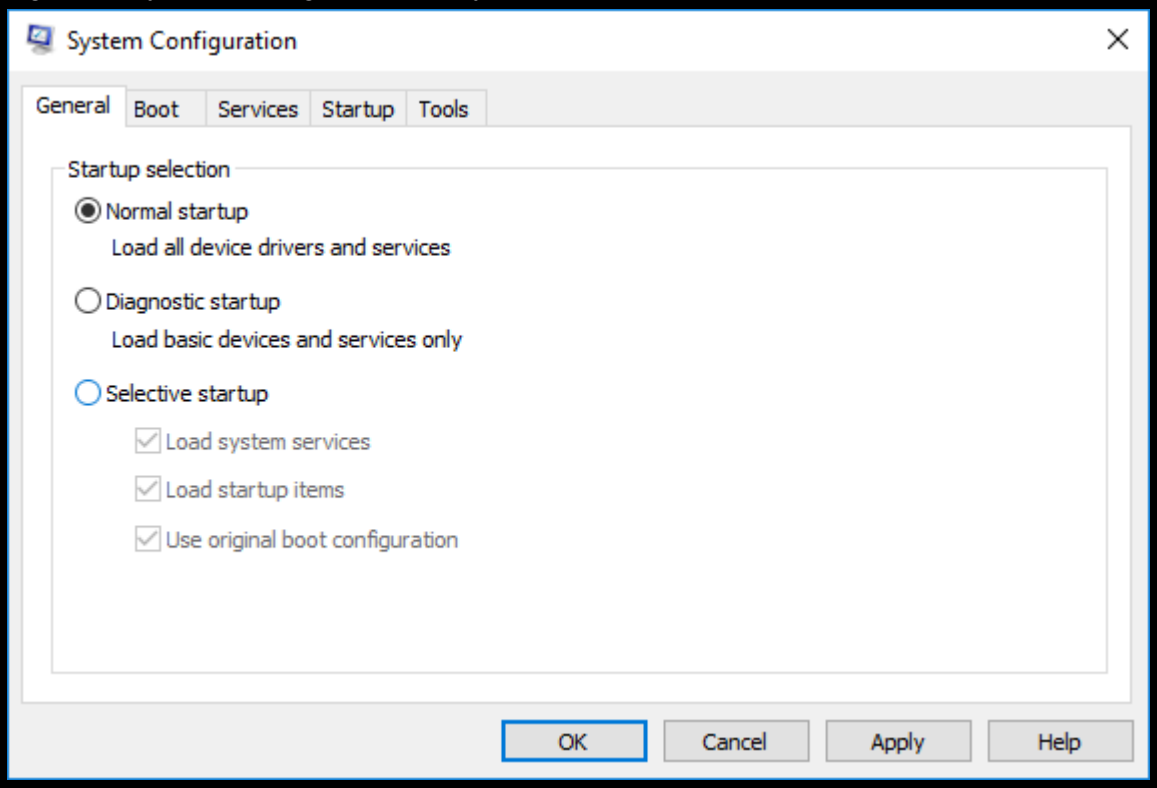
	Pages/sec	The number of pages read from or written to disk to resolve hard page faults indicates your system's use of the paging file. This is acceptable unless it becomes excessive (averaging above 50). It's advisable to check the paging file's usage by examining the paging object itself.
Paging File	% Usage	The percentage of the pagefile in use indicates its utilization. If your 1000 MB paging file averages 50% usage, adding around 500 MB of memory could be beneficial. Remember, excessive paging can degrade disk performance, as paging is disk-intensive.

Counters are interrelated and should be analyzed together. For example, low memory can slow the disk due to excessive paging. Always consider counters in context to identify performance issues.

14.3.13 System Configuration Utility

The **System Configuration Utility** modifies settings affecting how the computer boots and loads Windows. It's primarily used for diagnostic testing rather than permanent changes, which are typically made using tools like Services. The utility can be accessed by searching for System Configuration from the search menu or by running msconfig.exe from the Run menu.

- **General Tab:** Configure startup mode:
  - **Normal:** Standard startup.
  - **Diagnostic:** Basic startup for troubleshooting.
  - **Selective:** Choose specific boot sequence components.
- Figure 1. System Configuration Utility—General tab

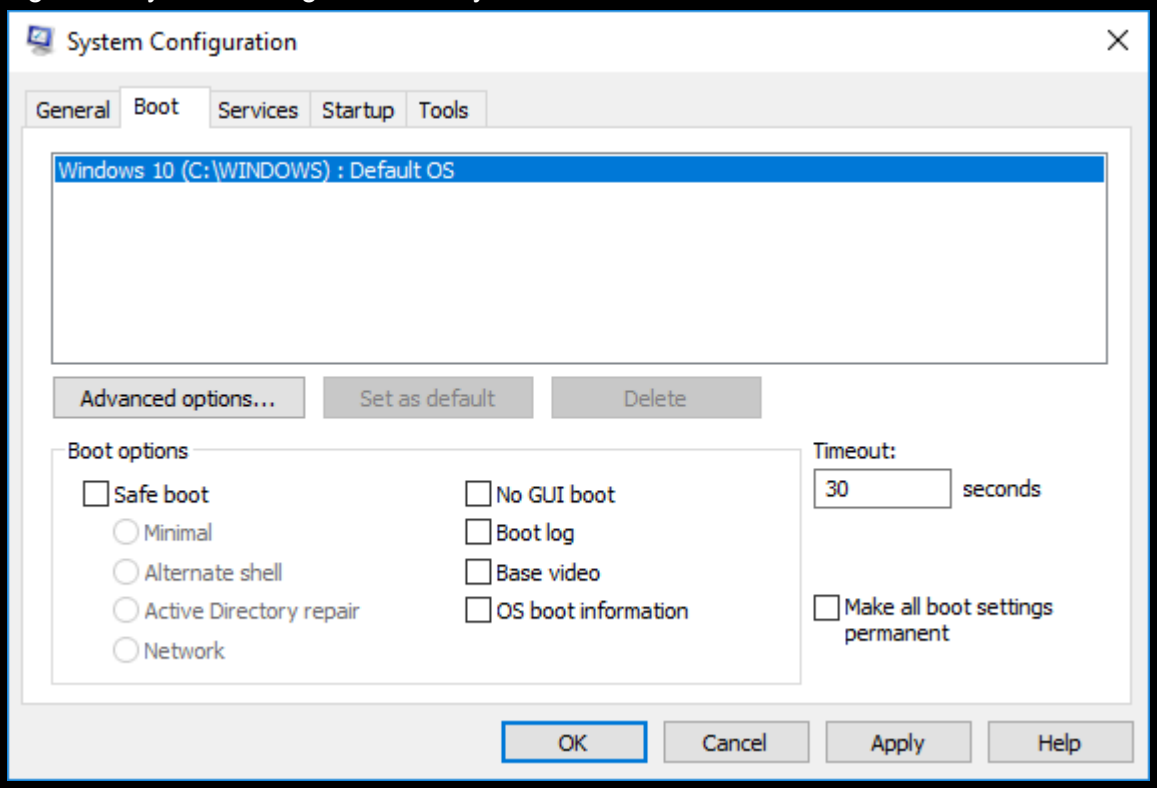


Screenshot courtesy of Microsoft.

Description
The tab displays options for Startup Selection, allowing users to choose between three modes: Normal Startup

– Loads all device drivers and services. Diagnostic Startup – Loads basic devices and services only. Selective Startup – Allows the user to customize startup options by selecting or deselecting options such as Load System Services, Load Startup Items, and Use Original Boot Configuration. At the bottom of the window, buttons labeled OK, Cancel, Apply, and Help provide controls for confirming or discarding changes.

- **Boot Tab:** Adjust Boot Configuration Data settings:
    - Change the default OS and add boot options like Safe Mode.
    - Set the timeout for the boot options menu.
    - Use the bcdedit command to add boot paths.
    - Note: Ensure Safe Boot or command prompt options aren't set permanently if troubleshooting.
- Figure 2. System Configuration Utility—Boot tab



Screenshot courtesy of Microsoft.

Description

The buttons for advanced options, set as default, and delete are below. The check boxes for different boot options are listed below. Timeout is set to 30 seconds. A check box to make all boot settings permanent is unchecked. Ok, Cancel, Apply, and Help buttons are at the bottom.

- **Services Tab:** Select services to run at startup, with the disable date shown for easier troubleshooting.
- **Tools Tab:** Access shortcuts to administrative utilities like System Information, Registry Editor, and Performance Monitor.

Note:

You can log boot events to a file saved at%SystemRoot%\ntblog.txt, which is not displayed in Event Viewer.

14.4.1 Boot Process

When a computer starts, the firmware runs a power-on self-test (POST) to verify that the system components are present and functioning correctly. It then identifies a boot device and passes control to the operating system's boot loader process.

With a legacy BIOS, the firmware scans the disk identified as the boot device and reads the master boot record (MBR) in the first sector of the disk. The MBR identifies the boot sector for the partition marked as active. The boot sector loads the boot manager, which for Windows is BOOTMGR.EXE. The boot manager reads information from the boot configuration data (BCD) file, which identifies operating systems installed on the computer. BOOTMGR and the BCD are normally installed to a hidden System Reserved partition.

Assuming there is only a single Windows installation, the boot manager loads the Windows boot loader WINLOAD.EXE stored in the system root folder on the boot partition.

Note:

If there is more than one OS installation, the boot manager shows a boot menu, allowing the user to select the installation to boot.

WINLOAD then continues the Windows boot process by loading the kernel (NTOSKRNL.EXE), the hardware abstraction layer (HAL.DLL), and boot device drivers. Control is then passed to the kernel, which initializes and starts loading the required processes. When complete, the WINLOGON process waits for the user to authenticate.

In UEFI boot mode, the initial part of the boot process is different. Following POST, the firmware reads the GUID partition table (GPT) on the boot device.

The GPT identifies the EFI System Partition. The EFI system partition contains the EFI boot manager and the BCD. Each Windows installation has a subfolder under \EFI\Microsoft\ that contains a BCD and BOOTMGFW.EFI.

BOOTMGFW.EFI reads the BCD to identify whether to show a boot menu and to find the location of WINLOAD.EFI. From this point, the Windows boot loader continues the boot process by loading the kernel, as described previously.

A+ Core 1 and Core 2 CertMaster Perform 15.0

14.4.2 Boot Recovery Tools

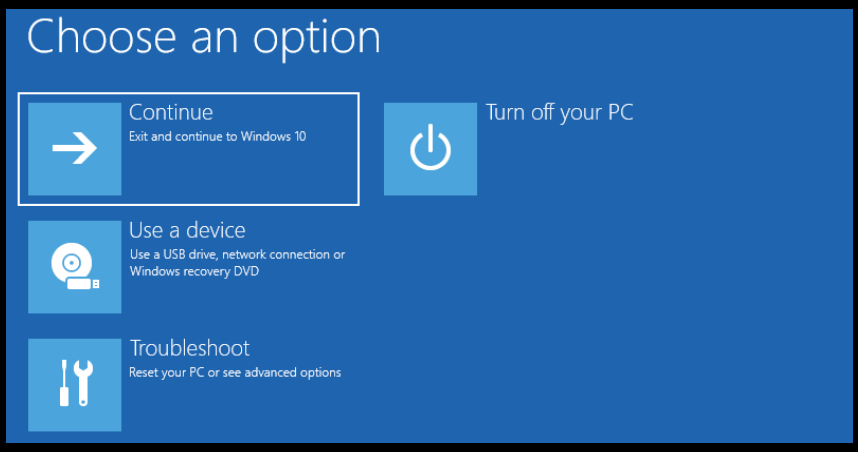
To troubleshoot boot issues, you need to use options and recovery tools to access an environment in which to run tests and attempt fixes.

Advanced Boot Options

The **Advanced Boot Options** menu allows the selection of different startup modes for troubleshooting. Startup options are displayed automatically if the system cannot start the OS. You can also invoke the menu manually. With BIOS boot, startup options are accessed by pressing **F8** before the OS loads. With UEFI, you need to reboot to show boot options. Hold the **SHIFT** key when selecting the **Restart** option from the **Power** menu on the lock screen—note that you don't have to sign in to view the power menu.

The Advanced Boot Options menu in Windows 11 can be accessed by going to Settings-> System -> Recovery->Advanced startup and clicking the Restart Now button.

Figure 1. Windows 10 startup options



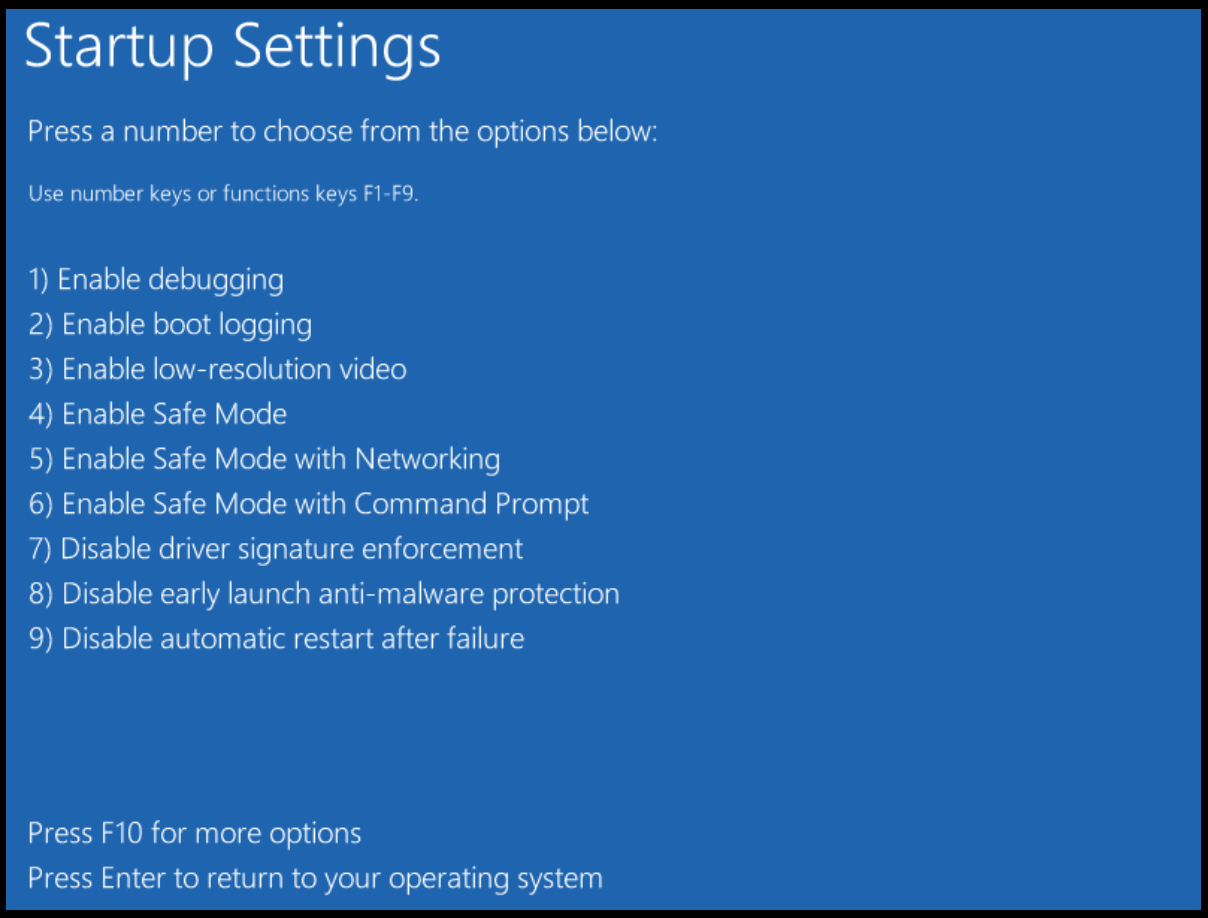
Screenshot courtesy of Microsoft.

Description

The options are as follows: Continue: Exit and continue to Windows 10. Turn off your PC. Use a device: Use a USB drive, network connection or Windows recovery DVD. Troubleshoot: Reset your PC or see advanced options.

Within startup options, from the first **Choose an option** screen, select Troubleshoot. From the next screen, select Advanced options. Select Startup Settings, and then on the next screen, select Restart.

Figure 2. Windows 10 Startup Settings



Screenshot courtesy of Microsoft.

Description

The text above reads, Press a number to choose from the options below. Use number keys or function keys F1 to F9. 1. Enable debugging. 2. Enable boot logging. 3. Enable low-resolution video. 4. Enable Safe Mode. 5. Enable Safe Mode with Networking. 6. Enable Safe Mode with Command Prompt. 7. Disable driver signature enforcement. 8.

Disable early launch anti-malware protection. 9. Disable automatic restart after failure. Press F10 for more options. Press Enter to return to your operating system.

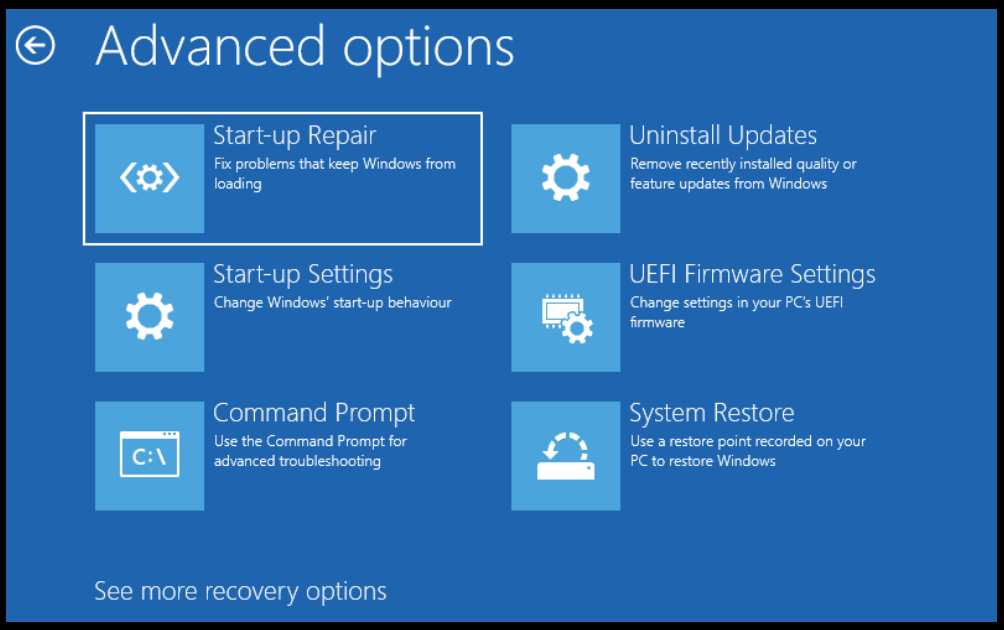
Press **F4** to select Safe Mode, or choose another option as necessary. **Safe Mode** loads only basic drivers and services required to start the system. This is a useful troubleshooting mode as it isolates reliability or performance problems to add-in drivers or application services and rules out having to fully reinstall Windows. It may also be a means of running analysis and recovery tools, such as chkdsk, System Restore, or antivirus utilities.

WinRE and Startup Repair

If you cannot boot the computer or access startup options from the local installation, you can try booting from the product media, a repair disk, or a recovery partition. You may have to access BIOS or UEFI setup to configure the recovery media as the priority boot device.

If you don't have the product media, you can make a system repair disk from Windows using the **Create a recovery drive** setting. You need to have done this before the computer starts failing to boot or create one using a working Windows installation.

Once in the recovery environment, select the Troubleshoot menu and then Advanced options. If the boot files are damaged, you can use the **Startup Repair** option to try to fix them. You can also launch System Restore or restore from an image backup, perform a refresh, or reset reinstallation of Windows from here. The last two options are to run a memory diagnostic and to drop into the **Windows Recovery Environment** command prompt, where you could run commands such as `diskpart`, `sfc`, `chkdsk`, `bootrec`, `bcdedit`, or `regedit` to try to repair the installation manually. Figure 3. Windows 10 Startup Troubleshooting—Advanced options



Screenshot courtesy of Microsoft.

Description

The options are listed as follows: Start-up Repair: Fix problems that keep Windows from loading. Uninstall Updates: Remove recently installed quality or feature updates from Windows. Start-up Settings: Change Windows' start-up behavior. UEFI Firmware Settings: Change settings in your PC's UEFI firmware. Command Prompt: Use the Command Prompt for advanced troubleshooting. System Restore: Use a restore point recorded on your PC to restore Windows.

14.4.4 System Restore

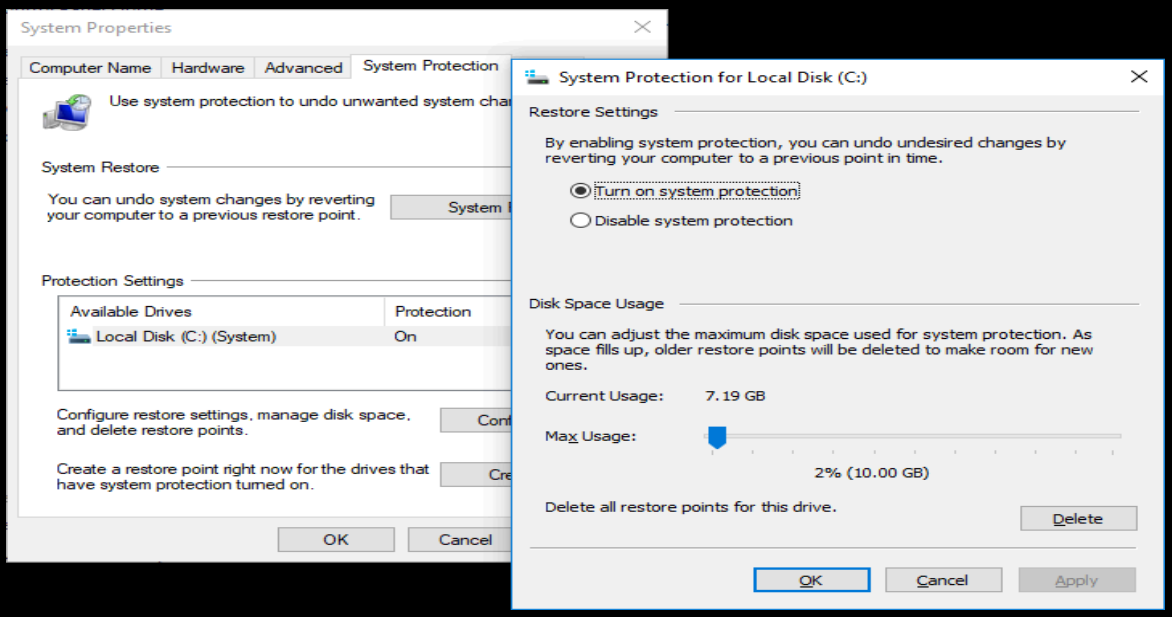
System Restore allows you to roll back from system configuration changes. System Restore allows for multiple restore points to be maintained (some are created automatically) and to roll back from changes to the whole registry and reverse program installations and updates.

System Restore does not restore (or delete) user data files.

Configuring System Protection

Use the **System Protection** tab (opened via the advanced **System** settings) to select which disk(s) to enable for system restore and configure how much disk capacity is used. The disk must be formatted with NTFS, have a minimum of 300 MB free space, and be over 1 GB in size.

Figure 1. Configuring System Protection in Windows 10



Description

The text under the head, restore settings reads, by enabling system protection, you can undo undesired changes by reverting your computer to a previous point in time. Radio buttons to turn on system protection and disable system

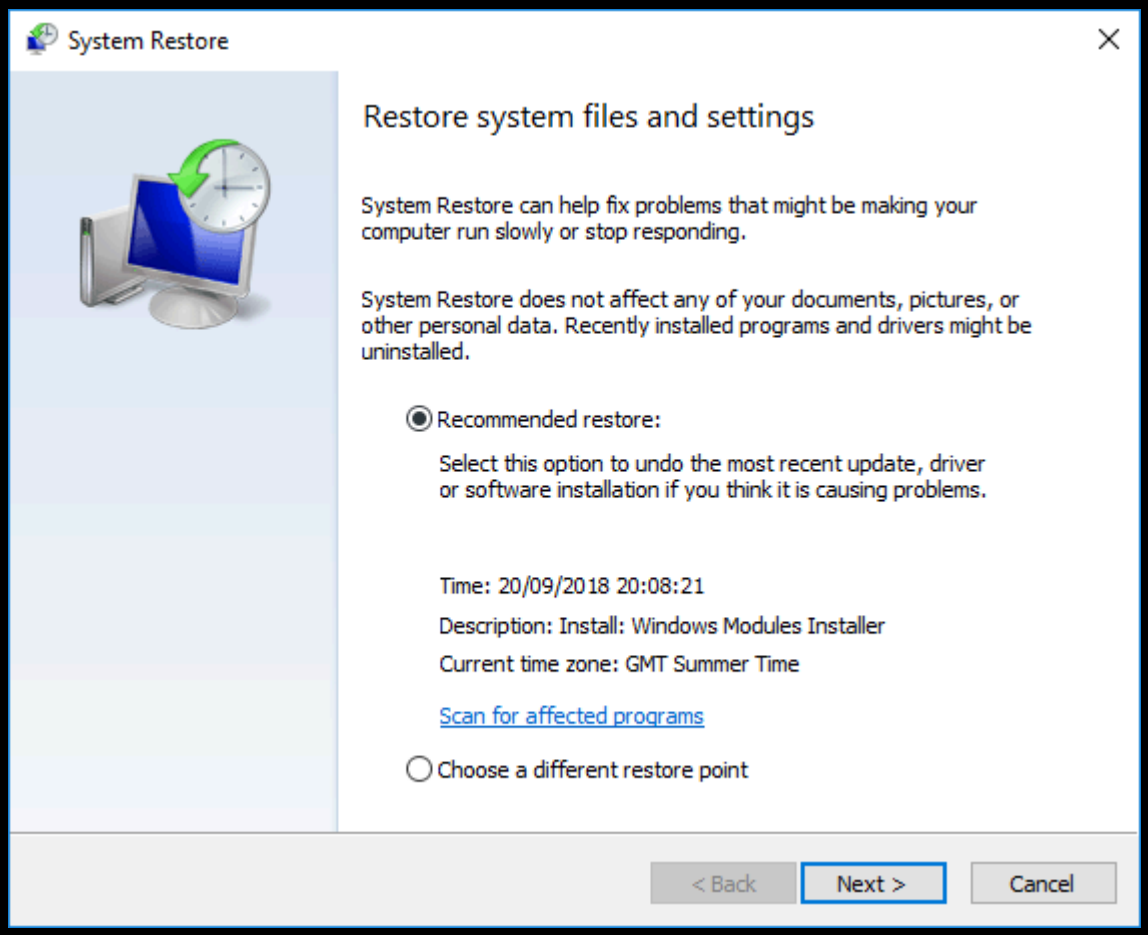
protection are given below. The disk space usage shows the current usage and max usage. The delete button is on the right. Ok, Cancel, and Apply buttons are at the bottom.

Restore points are created automatically in response to application and update installs. They are also created periodically by Task Scheduler. Windows will try to create one when it detects the PC is idle if no other restore points have been created in the last seven days. You can also create a restore point manually from this dialog.

Using System Restore

To restore the system, open the System Restore tool (`rstrui.exe`). You can also run System Restore by booting from the product disk or selecting **Repair Your Computer** from the recovery environment.

Figure 2. Using System Restore to apply a previous system configuration



Description

The head restore system files and settings has few lines for text followed by radio buttons for recommended restore along with the time, description, and current time zone. A link to scan for affected programs is at the bottom. Another radio button is to choose a different restore point. Back, Next, and Cancel buttons are at the bottom.

Note:

System Restore does not usually reset passwords (that is, passwords will remain as they were before you ran the restore tool), but System Restore does reset passwords to what they were at the time the restore point was created if you run it from the product disk.

Using PowerShell

System Restore and backups can be managed using PowerShell cmdlets.

The `Enable-ComputerRestore` cmdlet is used to turn on System Restore for a specific drive. Common elements include:

- `Enable-ComputerRestore`: Enables System Restore on one or more drives.
- `-Drive 'DriveLetter:\'`: Specifies the drive on which System Restore should be enabled.

Example usage:

- `Enable-ComputerRestore -Drive 'C:\'`

The `vssadmin resize shadowstorage` command is used to configure the amount of disk space allocated for Volume Shadow Copy which is used by System Restore and other backup technologies. Common switches include:

- `vssadmin resize shadowstorage`: Adjusts the size of the shadow copy storage area.
- `/on=DriveLetter:`: Specifies the drive where the shadow copy storage area is located.
- `/for=DriveLetter:`: Specifies the drive for which the shadow copies are being stored.
- `/maxsize=Value`: Sets the maximum size of the shadow copy storage. This can be specified as a percentage or as a specific size.

Example usage:

- `vssadmin resize shadowstorage /on=C: /for=C: /maxsize=5%`

The `Checkpoint-Computer` cmdlet is used to create a System Restore point. Common elements include:

- `Checkpoint-Computer`: Creates a restore point on the local computer.
- `-Description "Text"`: Provides a descriptive name for the restore point.
- `-RestorePointType "Type"`: Specifies the type of restore point being created. Options include:
    - `APPLICATION_INSTALL`: Used when installing an application so you can roll back if the installation causes problems.
    - `APPLICATION_UNINSTALL`: Used before uninstalling an application.
    - `MODIFY_SETTINGS`: Used before changing system or application settings (for example, registry edits or configuration changes).
    - `DEVICE_DRIVER_INSTALL`: Used when installing or updating device drivers.
    - `CANCELLED_OPERATION`: Indicates a restore point created for an operation that was later canceled.

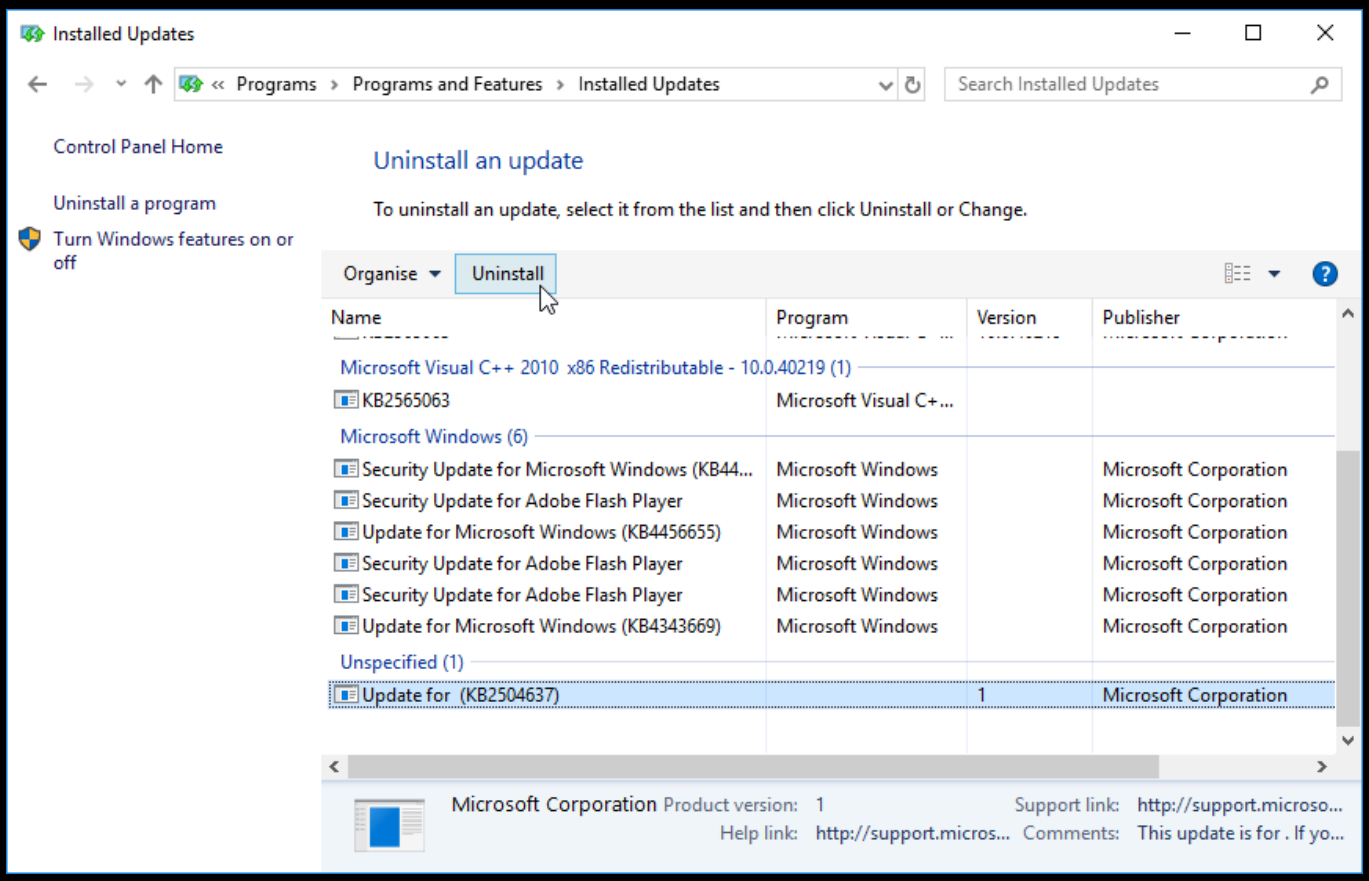
Example usage:

- `Checkpoint-Computer -Description "Before installing graphics driver update" -RestorePointType "DEVICE_DRIVER_INSTALL"`

14.4.6 Update and Driver Roll Back

If an update causes problems, you can try to uninstall it. You might be able to use System Restore to do this. Otherwise, open the **Programs and Features** applet and select **View installed updates**. Select the update, and then select the **Uninstall** button.

Figure 1. Using Programs and Features to uninstall an update



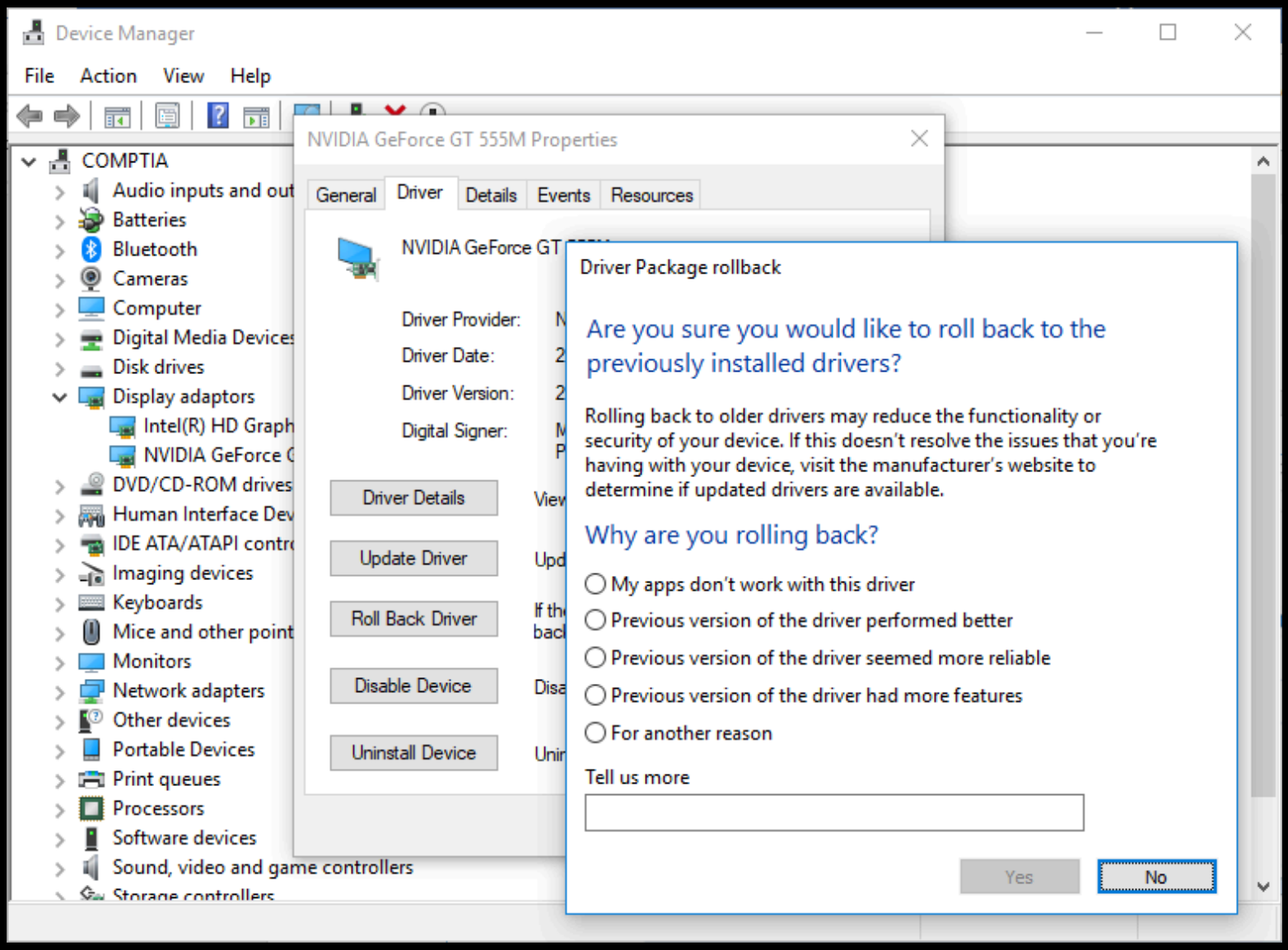
Description

The table lists the Name, Program, Version, and Publisher under the heads Microsoft Visual C plus plus 2010 x86 Redistributable and Microsoft Windows (6).

If you are experiencing problems with a device and you have recently updated the driver, Windows also provides a **Roll Back Updates Drivers** feature. A new driver may not work properly because it has not been fully tested, or it may not

work on your particular system. You can use **Device Manager** to revert to the previous driver. Right-click the device and select **Properties**. Select the **Driver** tab, and then select the **Roll Back Driver** button.

Figure 2. Using driver rollback via Device Manager



Description

The question at the top reads, are you sure you would like to roll back to the previously installed drivers. Rolling back to older drivers may reduce the functionality or security of your device. If this doesn't resolve the issues that you are having with your device, visit the manufacturer's website to determine if updated drivers are available. The question why are you rolling back is followed by radio buttons for the following: My apps don't work with this driver. Previous

version of the driver performed better. Previous version of the driver seemed more reliable. Previous version of the driver had more features. For another reason.

14.4.7 System Repair, Reinstall, and Reimage

If System Restore or Startup Repair does not work and you cannot boot to a logon, you will have to use a system repair tool or possibly a reinstall option and restore from data backup (presuming you have made one). The various versions of Windows use different system recovery tools and backup processes.

Creating and Using a Recovery Image

You can make a complete backup of the system configuration and data files as an **image**. This requires a backup device with sufficient capacity. The best compression ratio you can hope for is 2:1- so a 20 GB system will create a 10 GB image- but if the system contains a lot of files that are already heavily compressed, the ratio could be a lot lower. You also have to keep the image up-to-date or make a separate data backup.

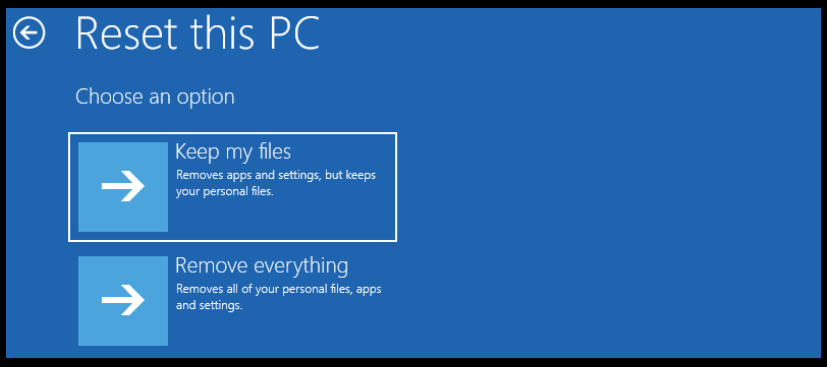
You create a system image using the **Backup and Restore** applet in **Control Panel**. Select the **Create a system image** link in the tasks pane.

To recover the system using the backup image, use the **Advanced Boot Option** or the **System Image Recovery** option off a repair disk or recovery environment.

Reinstalling Windows

If you do not have an up-to-date image, the last option is to reinstall Windows using the **Reset This PC** option in the recovery environment.

Figure 1. Windows 10 startup recovery



Description

The options are as follows: Keep my files: Remove apps and settings, but keeps your personal files. Remove everything: Removes all of your personal files, apps and settings.

Select **Keep my files** or **Remove everything** as appropriate. The **Keep my files** option can be used to repair the existing installation using either a local setup cache or by downloading the files from Microsoft's cloud servers. A reset recopies the system files and reverts all PC settings to the default, but it can preserve user personalization settings, data files, and apps installed via Windows Store. Desktop applications are removed.

The computer will restart, and you will be prompted to sign on using an administrator account to authorize the reinstallation. Select **Reset** to continue (or **Cancel** if you have changed your mind).

If you choose to remove everything, there is a further option to securely delete information from the drive. This will take several hours but is recommended if you are giving up ownership of the PC.

14.4.8 Troubleshoot Boot Issues

Assuming there is no underlying hardware issue, the general technique for troubleshooting **boot problems** is to determine the failure point, and therefore the missing or corrupt file. This can then be replaced, either from the source files or by using some sort of recovery disk.

Failure to Boot/Invalid Boot Disk

If the system firmware returns an error message such as **No boot device found** or **Invalid boot disk** , then the system has completely failed to boot. The most common cause of this error used to be leaving a floppy disk in the drive on a restart. A modern cause is for the system firmware to be set to use USB for boot. Check for any removable disks, and change the boot device priority/boot order if necessary. If this message occurs when booting from a hard disk or SSD, check the connections to the drive. If the error is transitory (for example, if the message occurs a few times and then the PC starts to boot OK), it could be a sign that the fixed disk is failing. On an older system, it could be that the system firmware is having trouble detecting the drive.

No OS Found

A **no OS found** type message can appear when a disk drive is identified as the boot device but does not report the location of the OS loader. This could indicate a faulty disk, so try running disk diagnostics (if available), and then use a recovery option to run `chkdsk` .

If the disk cannot be detected, enter system setup, and try modifying settings (or even resetting the default settings). If the disk's presence is reported by the system firmware but Windows still will not boot, use a startup repair tool to open a recovery mode command prompt, and use the `bootrec` tool to try to repair the drive's boot information.

- Enter bootrec /fixmbr to attempt repair of the MBR. Do not use this option if the disk uses GPT partitioning.

- Enter `bootrec /fixboot` to attempt repair of the boot sector.
- Enter `bootrec /rebuildbcd` to add missing Windows installations to the boot configuration database (BCD).

You could also use `diskpart` to ensure that the system partition is marked as active and that no other partitions have been marked as active.

Graphical Interface Fails to Load/Black Screen

If Windows appears to boot but does not display the sign-in screen or does not load the desktop following logon, the likely causes are corruption of drivers or other system files. If the system will boot to a GUI in Safe Mode, then replace the graphics adapter driver. If the system will not boot to a GUI at all, then the Windows installation will probably have to be repaired or recovered from backup. It is also possible that the boot configuration has been changed through `msconfig` and just needs to be set back.

Windows is also sporadically prone to black screen issues, where nothing appears on the screen. This will often occur during update installs, where the best course of action is to give the system time to complete the update. Look for signs of continuing disk activity and spinning dots appearing on the screen. If the system does not recover from a black screen, then try searching for any currently known issues on support and troubleshooting sites. You can use the key sequence **WINDOWS+CTRL+SHIFT+B** to test whether the system is responsive. There should be a beep and the display may reinitialize.

If the problem occurs frequently, use `chkdsk` and `sfc` to verify system file integrity. Also, consider either an update or rollback of the graphics adapter driver.

14.4.10 Troubleshoot Profile Issues

If Windows does boot, but only **slowly**, you need to try to identify what is happening to delay the process. You can enable verbose status messages during the Windows load sequence by configuring a system policy or applying a registry setting to enable **Display highly detailed status messages**.

Delays affecting the system prior to sign-in are caused by loading drivers and services. Quite often the culprit will be some type of network service or configuration not working optimally, but there could be some sort of file corruption too.

If the system is slow to load the desktop following sign-in, the issue could be a corrupt user profile. The registry settings file NTUSER.DAT is particularly prone to this. **Rebuilding a local user profile** means creating a new account and then copying files from the old, corrupt profile to the new one, but excluding the following files: NTUSER.DAT, NTUSER.DAT.LOG, and NTUSER.INI.

14.4.11 Troubleshoot Performance Issues

Degraded performance can have many causes. Use the following general procedure to try to quantify the degree to which the system is “slow” and identify probable causes:

1. Use Task Manager to determine if any resources are at 90–100% utilization, and then note which process is most active.
   You may need to identify a particular Windows service running within a svchost.exe process. Windows Update/Installer, the SuperFetch/Prefetch caching engine, Windows Telemetry data collection, Windows Search/Indexing, and Windows Defender (or third-party security software) are often the culprits.

2. Wait for these processes to complete. If there is a mix of CPU, memory, and disk activity, then the process is probably operating normally, but slowly.
   If there is no disk activity or, conversely, if disk activity does not drop from 100%, the process could have stalled.

3. If the process or system continues to be unresponsive, you can either restart the service or kill the task process.

4. If ending the process doesn't restore system performance, try **rebooting** the computer.
   The problem could be transitory and might not reoccur.
   Rather than simply rebooting, you might want to fully power down the machine, disconnect it from the supply for 30 seconds, and then power back on. This ensures that all data is completely cleared from caches and system memory.

5. If the service or process becomes unresponsive again after restarting, disable it (if possible) and check with the software vendor for any known problems.

6. If Windows displays an error message such as **Low memory**, try running fewer programs, and see if the issue can be isolated to one process.
   The software might have a memory leak fault that will need to be fixed by the vendor. If the issue only occurs when the user tries to run more programs, either the system will need to be fitted with more system RAM or the user will need to lower his or her expectations for multitasking.

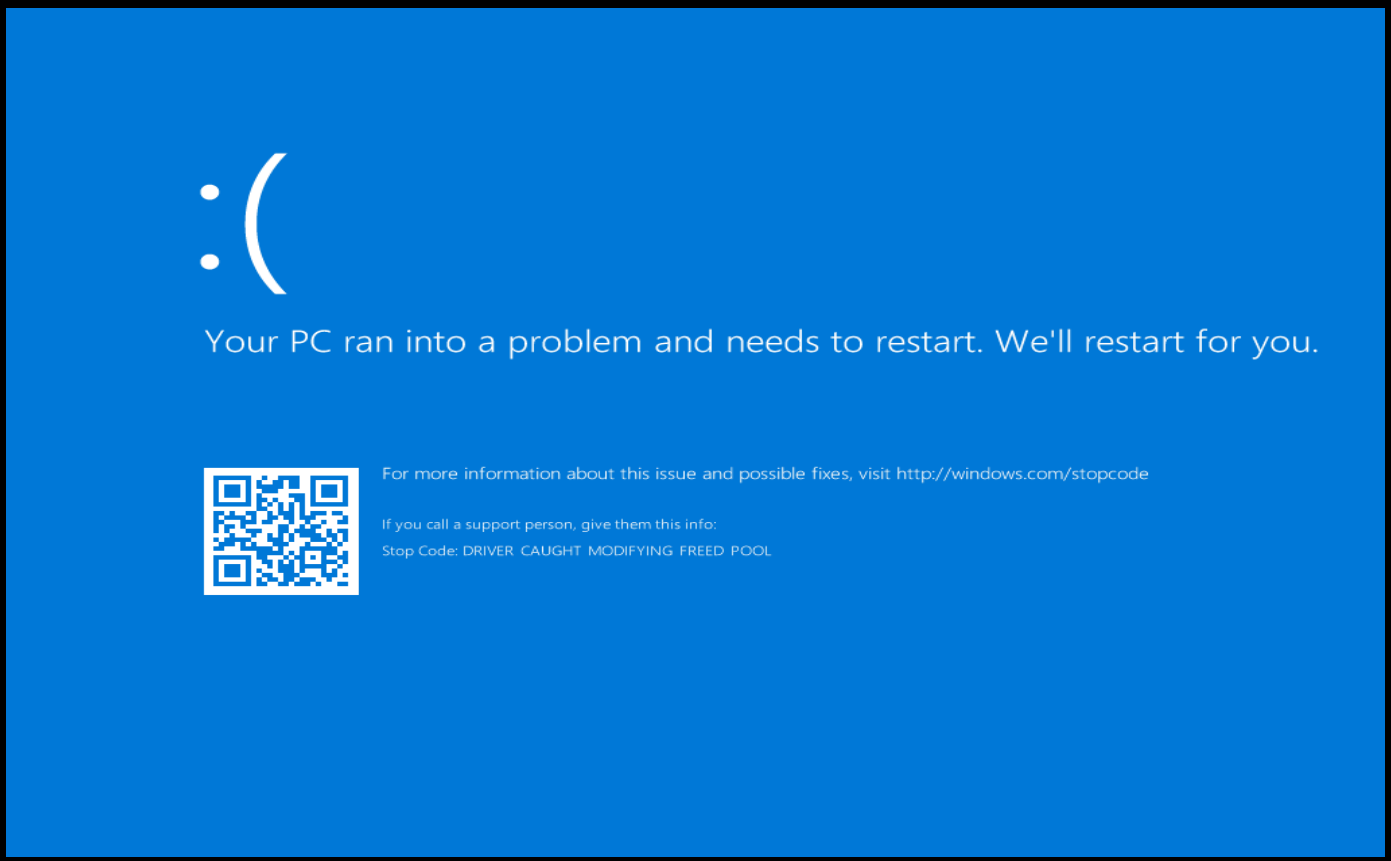
7. If Windows displays an error message such as **Low disk space**, use Disk Clean-up to delete unnecessary files. If the problem keeps recurring, check for any unusual behavior by an application, such as excessive logging or temp file creation. If you can rule out these as issues, the system will need additional storage.
   If you can't identify overutilization as a probable cause, consider the following troubleshooting techniques and solutions:

   - **Apply updates**- Check for any missing Windows and application updates and install the latest drivers for hardware devices.
   - **Defragment the hard drive**- Running defrag regularly on a hard disk drive (HDD) improves file I/O by putting files into contiguous clusters. Also, make sure there is sufficient free disk space.
   - **Verify OS and app hardware requirements, and add resources if necessary**—As well as consulting the official system requirements, check resource utilization using Task Manager, Resource Monitor, or (for more extended periods) Performance Monitor. If CPU, system memory, disk, or network resources are continually stretched, then the system will have to be upgraded. For example, Windows performance when installed to a hard disk is not nearly as good as when installed to an SSD.
   - **Disable startup items**- Use the System Configuration Utility (`msconfig`) or Task Manager to prevent unnecessary services and programs from running at startup. If you need to run the services, consider setting them to delayed startup or manual startup to avoid slowing down boot times too much. If a service is not required and is causing problems, you can set it to Disabled to prevent it from being started. Note that some security-critical services (such as Windows Update) can be re-enabled automatically by the OS.
   - **Scan the computer for viruses and other malware, but also check the configuration of antivirus software**- While necessary to protect against malware threats, security scanning software can reduce system performance. Try disabling scanning temporarily to test whether performance improves. Make sure the software is configured to exclude Windows system files it shouldn't scan, and configure any exceptions for software applications recommended by the vendor. These typically include database files and the image files used for virtual hard disks.
   - **Check for power management issues**- If the user has been closing sessions using sleep or hibernate, try restarting the computer. Verify that the system is not operating in a power-saving mode (CPU throttling). Be aware that this might have an underlying cause, such as overheating.

14.4.12 Troubleshoot System Fault Issues

A **Blue Screen of Death** (BSOD) displays a Windows STOP error. A STOP error causes Windows to halt. STOP errors can occur when Windows loads or while it is running. Most BSoDs, especially those that occur during startup, are caused by faulty hardware or hardware drivers. Use the following procedures to try to troubleshoot the issue:

- Use System Restore or (if you can boot to Safe Mode) driver rollback, or update rollback to restore the system to a working state.
- Remove a recently added hardware device, or uninstall a recently installed program.
- Check seating of hardware components and cables.
- Run hardware diagnostics, chkdsk, and scan for malware.
- Check fans and chassis vents for dust and clean if necessary.
- Make a note of the stop error code (which will be in the form: Stop: 0x0...), and search the Microsoft Knowledge Base (support.microsoft.com/search) for known fixes and troubleshooting tips. The various newsgroups accessible from this site offer another valuable source of assistance. Figure 1. Blue Screen of Death (BSoD)



Note:

If the system auto restarts after a blue screen and you cannot read the error, open the Advanced Options menu, and select the Disable automatic restarts option. This option can also be set from Advanced System PropertiesStartup and Recovery Settings.

System Instability and Frequent Shutdowns

A system that exhibits instability will freeze, shutdown, reboot, or power off without any sort of error message. This type of error suggests an overheating problem, a power problem, a CPU/chipset/RAM issue, or corrupt kernel files.

Windows includes a **Windows Memory Diagnostics** tool to test memory chips for errors. You can either run the tool from **Administrative Tools** or boot to the recovery environment. The computer will restart and run the test. Press **F1** if you want to configure test options.

If errors are found, first check that all the memory modules are correctly seated. Remove all the memory modules but one and retest. You should be able to identify the faulty board by a process of elimination. If a known-good memory module is reported faulty, the problem is likely to lie in the motherboard.

If you suspect file corruption, run chkdsk to verify the boot volume's file system and sfc /verifyonly to scan Windows system files. If a tool reports errors, run it in repair mode (chkdsk /f or chkdsk /r and sfc /scannow) to attempt to fix the issue.

USB Issues

If there are issues with USB devices not working after connection, not working after the computer resumes from sleep/hibernation, or generating warning messages, make sure the controllers are using the latest driver:

1. Use Windows Update or the vendor site to obtain the latest chipset or system driver. There may also be a specific USB 3 host controller driver.

2. Use Device Manager to uninstall each USB host controller device, and then reboot to reinstall them with the new driver.
3. If this does not resolve the issue, disable USB selective suspend power management either for a specific port or device or system-wide.

A **USB controller resource warning** indicates that too many devices are connected to a single controller. This typically occurs if you use an unpowered USB hub to expand the number of ports available and connect more than five devices to a single controller. If updating the chipset drivers doesn't resolve the issue, try the following:

1. Connect the hub to a USB 2 port rather than a USB 3 port. While USB 3 is higher bandwidth, in some chipset implementations each controller supports fewer device connections (endpoints). Use the hub to connect low-bandwidth input/output devices over USB 2, and reserver use of USB 3 ports for external disks and network adapters.

2. Reduce the number of devices to see if that solves the problem. If it doesn't, test to see if one device is the source of the errors.

14.4.13 Troubleshoot Application and Service Fault Issues

As well as system-wide issues, some errors may be isolated to a particular application or background service.

Applications Crashing

If an **application crashes**, the priority is to try to preserve any data that was being processed. Users should be trained to save regularly, but modern suites such as Microsoft Office are configured to save recovery files regularly, minimizing the chance of data loss. If enabled, the Windows File History feature or using OneDrive cloud storage can also function as a continuous backup for file versions.

Try to give the process time to become responsive again, and establish if you need to try to recover data from temporary files or folders. When you have done all you can to preserve data, use Task Manager to end the process. If the application crashes continually, check the event logs for any possible causes. Try to identify whether the cause lies in processing a particular data file or not.

If you cannot identify a specific cause of a problem, the generic solution is to check for an application **update** that addresses the issue. Remember that applications need to be updated independently of Windows Update. The option is usually located in the Help menu. If an update does not fix the problem, the next step is to **uninstall then reinstall** or perform a repair installer if that is supported. Sometimes the Windows installer fails to remove every file and registry setting; if this is the case, then following manual uninstall instructions might help.

Services Not Starting

If you see a message such as **One or more services failed to start** during the Windows load sequence, check Event Viewer and/or the Services snap-in to identify which service has failed. Troubleshooting services can be complex, but bear the following general advice in mind:

- Try to start or restart the service manually- As most computers run a lot of services at startup, some can sometimes become "stuck." If a service is not a critical dependency for other services, it may help to set it to delayed start.

- Verify that disabling one service has not inadvertently affected others- Some services cannot start until a dependent service is running.
- Make sure that the service has sufficient privileges- Services depend on account permissions to run. Check that the service is associated with a valid user or system account and that the password configured for the account is correct.

- If a core Windows service is affected, check system files, and scan the disk for errors and malware.
- If an application service is affected, try reinstalling the application.
- Use `regsvr32` to re-register the software component- a dynamic link library (DLL)—that the service relies upon.
- Check whether the service is supposed to run- Faulty software uninstall routines can leave "orphan" registry entries and startup shortcuts. Use the System Configuration Utility (`msconfig`) or Registry Editor (`regedit`) to look for orphaned items.

Time Drift

Processes such as authentication and backup depend on the time reported by the local PC being closely synchronized to the time kept by a server. Some authentication systems are intolerant of 30 or 60-second discrepancies.

Each PC motherboard has a battery-powered real-time clock (RTC) chip, but this is not a reliable authoritative time source. Relying on the internal time can lead to servers and clients **time drift**, especially if some of the clients access the network remotely. Servers and clients can also be configured to use Internet time sources, but if some clients are remote, they may be set to use different sources than the network servers.

Ideally, the network services should be configured in a domain and use either GPS-synchronized time sources or a pool of Internet time sources. Sampling from a pool helps to identify and resolve drifts. The clients can then be configured to use the servers as authoritative time sources.

15.1.1 Logical Security Controls

A security control is a safeguard or prevention method to avoid, counteract, or minimize risks relating to personal or company property. For example, a firewall is a type of security control because it controls network communications by allowing only traffic that has specifically been permitted by a system administrator. There are many ways of classifying security controls, but one way is to class them as physical, procedural, or logical:

- Physical controls work in the built environment to control access to sites. Examples include fences, doors, and locks.
- Procedural controls are applied and enforced by people. Examples include incident response processes, management oversight, and security awareness training programs.
- Logical controls are applied and enforced by digital or cyber systems and software. Examples include user authentication, antivirus software, and firewalls.

The goal of cybersecurity systems is often defined by the CIA triad which stands for Confidentiality, Integrity, and Availability:

- Confidentiality ensures that sensitive data is only accessible by authorized users.
- Integrity ensures that the data is accurate and trustworthy.
- Availability means that resources are readily available for users to access when they need to.

One framework which can be used to meet the goals of the CIA triad is Identity and Access Management (IAM). This framework ensures that only authorized users have the appropriate access to the right resources at the right time. The core components of IAM include:

- **Identification** - This involves identifying and defining users, devices, and applications within the system.
- **Authentication** - This identifies users attempting to access resources. This can be done with passwords, biometrics, and multi-factor authentication.
- **Authorization** - This determines what resources and actions a user is allowed to access based on their role, responsibilities, and permissions.
- **Access Control** - Enforces authorization policies and restricts access to resources based on predefined rules.

Access Control Lists

A permission is a security setting that determines the level of access an account has to a particular resource. A permission is usually implemented as an **access control list** attached to each resource. Within an ACL, each access control entry (ACE) identifies a subject and the permissions it has for the resource.

A subject could be a human user, a computer, or a software service. A subject could be identified in several ways. On a network firewall, subjects might be identified by MAC address, IP address, and/or port number. In the case of directory permissions in Windows, each user and security group account has a unique security ID (SID).

Note:

While accounts are identified by names in OS interface tools, it is important to realize that the SID is the only identifier used in the underlying permission entries. If an account is deleted and then recreated with the same username, the SID will still be different, and any permissions assigned to the account will have to be recreated.

Implicit Deny

ACL security is typically founded on the principle of implicit deny. **implicit deny** means that unless there is a rule specifying that access should be granted, any request for access is denied. This principle can be seen clearly in firewall policies. A firewall filters access requests using a set of rules. The rules are processed in order from top to bottom. If a request does not fit any of the rules, it is handled by the last (default) rule, which is to refuse the request.

Principle of Least Privilege

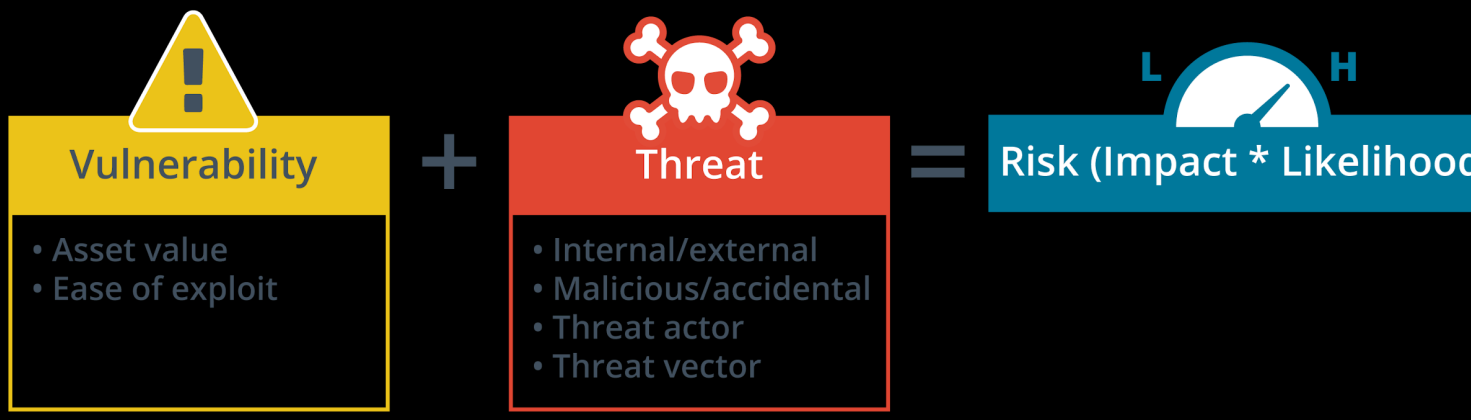
A complementary principle to implicit deny is that of **least privilege**. This means that a user should be granted the minimum possible access necessary to perform the job. This can be complex to apply in practice, however. Designing a permissions system that respects the principle of least privilege while not generating too many support requests from users is a challenging task.

15.1.2 Information Security

Information security is assured by developing security policies and controls. Making a system more secure is also referred to as hardening it. Different security policies should cover every aspect of an organization's use of computer and network technologies, from procurement and change control to acceptable use.

As part of this process, security teams must perform assessments to determine how secure a network is. These assessments involve vulnerabilities, threats, and risks:

- **Vulnerability** is a weakness that could be accidentally triggered or intentionally exploited to cause a security breach.
- **Threat** is the potential for someone or something to exploit a vulnerability and breach security. A threat may be intentional or unintentional. The person or thing that poses the threat is called a **threat actor** or threat agent. The path or tool used by a malicious threat actor can be referred to as the attack vector or threat vector.
- **Risk** is the likelihood and impact (or consequence) of a threat actor exercising a vulnerability. Figure 1. Relationship between vulnerability, threat, and risk



Description
Vulnerability includes Asset value and Ease of exploit. Threat includes Internal or External, Malicious or Accidental, Threat actor, and Threat vector. Risk is Impact times Likelihood.

To assist with workstation and network security assessments, you need to understand the types of threats that an organization is exposed to and how vulnerabilities can be exploited to launch attacks.

15.1.3 Hashing and Encryption Concepts

Many logical security controls depend to some extent on the use of **encryption** technologies. A message encrypted by a cipher is only readable if the recipient has the correct key for that cipher. The use of encryption allows sensitive data to travel across a public network, such as the Internet, and remain private.

There are three principal types of cryptographic technology: symmetric encryption, asymmetric encryption, and cryptographic hashing.

Symmetric Encryption

A **symmetric encryption** cipher uses a single secret key to both encrypt and decrypt data. The secret key is so-called because it must be kept secret. If the key is lost or stolen, the security is breached. Consequently, the main problem with symmetric encryption is secure distribution and storage of the key. This problem becomes exponentially greater the more widespread the key's distribution needs to be. The main advantage is speed. A symmetric cipher, such as the Advanced Encryption Standard (AES), can perform bulk encryption and decryption of multiple streams of data efficiently.

Asymmetric Encryption

An **asymmetric encryption cipher** uses a key pair. A key pair is a **private key** and a **public key** that are mathematically linked. For any given message, either key can perform either the encrypt or decrypt operation but not both. Only the paired key can reverse the operation. For example, if the public key part is used to encrypt a message, only the linked private key can be used to decrypt it. The public key cannot decrypt what it has just encrypted.

A key pair can be used the other way around. If the private key is used to encrypt something, only the public key can then decrypt it. The point is that one type of key cannot reverse the operation it has just performed.

The private key must be kept a secret known only to a single subject (user or computer). The public key can be widely and safely distributed to anyone with whom the subject wants to communicate. The private key cannot be derived from the public key.

Cryptographic Hashes

A **hash** is a short representation of data. A hash function takes any amount of data as input and produces a fixed-length value as output. A cryptographic hash performs this process as a one-way function that makes it impossible to recover the original value from the hash. Cryptographic hashes are used for secure storage of data where the original meaning does not have to be recovered (passwords, for instance).

Perhaps the most used cryptographic hash algorithms are the Secure Hash Algorithm (SHA) family of algorithms. SHA-256 and SHA-3 are the most used version of the SHA algorithms.

15.1.5 Digital Signatures and Key Exchange

Cryptographic hashes and encryption ciphers have different roles in achieving the information security goals of confidentiality, integrity, and availability. Often two or more of these three different types are used together in the same product or technology.

The main drawback of asymmetric encryption is that a message cannot be larger than the key size. To encrypt a large file, it would have to be split into thousands of smaller pieces. Consequently, asymmetric encryption is used with cryptographic hashes and symmetric encryption keys to implement various kinds of security products and protocols.

For example, when logging into your online banking account, the web browser initiates a secure connection with the bank server using a TLS handshake. During this handshake, the client and bank generate a unique session key that is then used to encrypt all further communication. The bank then sends its TLS certificate which contains its public key and digital signature to prove who it is. The browser verifies the digital signature using the public key to confirm the certificate is valid.

Digital Signatures

A **digital signature** proves that a message or digital certificate has not been altered or spoofed. The sender computes a cryptographic hash of a message, encrypts the hash with their own private key, and attaches the output to the message as a digital signature. When the recipient receives the message, they can decrypt the signature using the public key to obtain the sender's hash. The recipient then computes their own hash of the message and compares the two values to confirm they match.

Key Exchange

Key exchange allows two hosts to know the same symmetric encryption key without any other host finding out what it is. A symmetric cipher is much faster than an asymmetric one, so it is often used to protect the actual data exchange in a session. Asymmetric encryption only operates efficiently on data that is smaller than the key size. This makes it well-suited to encrypt and exchange symmetric cipher keys.

The sender uses the recipient's public key to encrypt a secret key. The recipient uses the private key to retrieve the secret key and then uses the secret key to decrypt whatever data message was transmitted by the sender. In this context, the symmetric cipher secret key is also referred to as a session key. If it is changed often, it is also referred to as an ephemeral key.

15.1.6 User and Group Accounts

A **user account** is the principal means of controlling access to computer and network resources and assigning rights or privileges. In Windows, a user can be set up with a local account or a Microsoft account:

- A **local account** is defined on that computer only. For example, `PC1\David` is the username for an account configured on a host named PC1. A local user account is stored in a database known as the Security Account Manager (SAM), which is part of the HKEY_LOCAL_MACHINE registry. Each machine maintains its own SAM and set of SIDs for accounts. Consequently, a local account cannot be used to log on to a different computer or access a file over the network.
- A **Microsoft account** is managed via an online portal (account.microsoft.com) and identified by an email address. Configuring access to a device by a Microsoft account creates a profile associated with a local account. Profile settings can be synchronized between devices via the online portal.

The guided setup process requires a Microsoft account to be configured initially. However, the account type can be switched from Microsoft to local or local to Microsoft as preferred via the **Your info** page in the Settings app.

Security Groups

A **security group** is a collection of user accounts. Security groups are used when assigning permissions and rights, as it is more efficient to assign permissions to a group than to assign them individually to each user. You can set up a number of custom groups with least privilege permissions for different roles and then make user accounts members of the appropriate group(s).

Built-in groups are given a standard set of rights that allow them to perform appropriate system tasks.

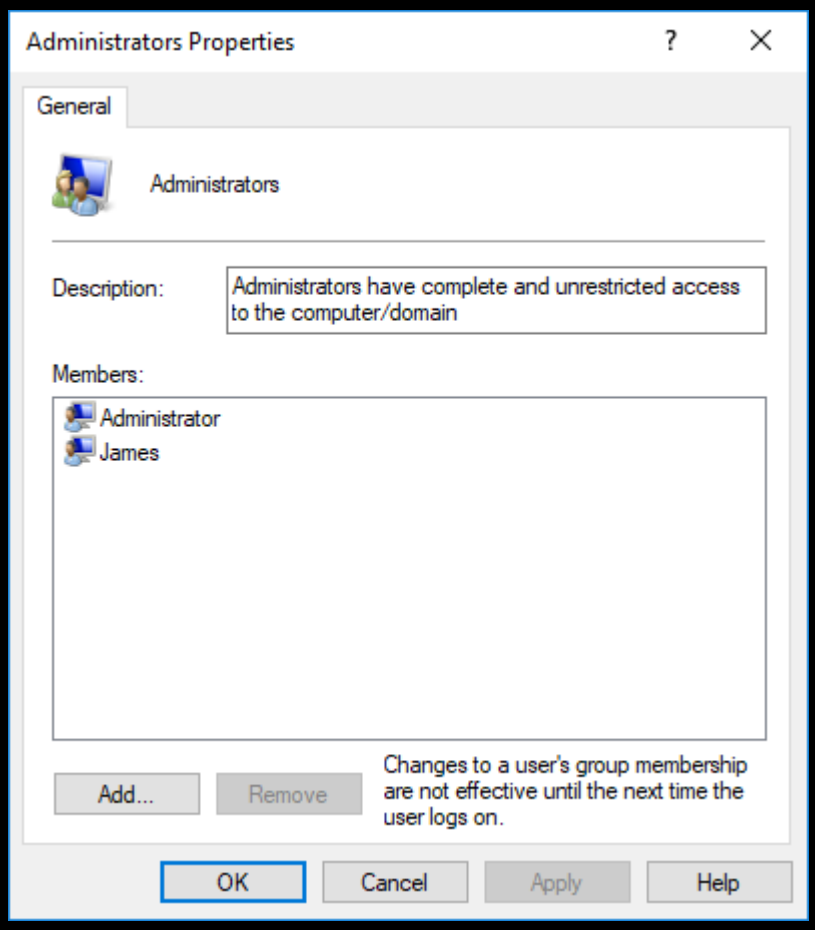
- A user account that is a member of the **administrator** group can perform all management tasks and generally has very high access to all files and other objects in the system. The local or Microsoft user created during setup is automatically added to this group. Other accounts should not routinely be added to the Administrators group. It is more secure to restrict membership of the Administrators group as tightly as possible.
  Note:
  There is also a *user* account named "Administrator," but it is disabled by default to improve security.
- A **standard account** is a member of the Users group. This group is generally only able to configure settings for its profile. However, it can also shut down the computer, run desktop applications, install and run store apps, and use printers. Additional accounts should be set up as standard users unless there is a compelling reason to add another administrative account.
- The **guest** group is only present for legacy reasons. It has the same default permissions and rights as the User group.

- The Guest *user* account is disabled by default. Microsoft ended support for using the Guest account to login to Windows in a feature update. The Guest account is only used to implement file sharing without passwords.
- The **power user** group is present to support legacy applications. Historically, this group was intended to have intermediate permissions between administrators and users. However, this approach created vulnerabilities that

allowed accounts to escalate to the administrators' group. In Windows 10/11, this group has the same permissions as the standard Users group.

Local Users and Groups

The **Local Users and Groups** management console provides an interface for managing both user and group accounts. Use the shortcut menus and object Properties dialogs to create, disable, and delete accounts, change account properties, reset user passwords, create custom groups, and modify group membership. Figure 1. Configuring members of the Administrators' built-in group



Screenshot courtesy of Microsoft.

Description

The general tab lists the administrators description and members. Add and remove button at the bottom are followed by ok, cancel, apply, and help buttons below them.

net user Commands

You can also manage accounts at the command line using **net user**. You need to execute these commands in an administrative command prompt.

- Add a new user account and force the user to choose a new password at first login:

```
net user dmartin Pa$$w0rd /add /fullname:"David Martin" /logonpasswordchg:yes
```

- Disable the dmartin account:

```
net user dmartin /active:no
```

- Show the properties of the dmartin account:

```
net user dmartin
```

- Add the dmartin account to the Administrators local group:

```
net localgroup Administrators dmartin /add
```

15.1.7 User Account Control

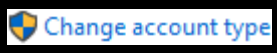
Just-in-Time (JIT) access is a security practice in which users are granted access to resources only when needed and for only as long as it takes to complete the needed task.

Privileged Access Management (PAM) focuses on securing, controlling, and monitoring access to privileged accounts. If these accounts are compromised, they can cause significant damage.

To help implement these security practices in Windows, User Account Control (UAC) can be used.

User account control is a Windows security feature designed to protect the system against malicious scripts and attacks that could exploit the powerful privileges assigned to accounts that are members of the Administrators group. UAC is an example of a least privilege security control. It requires the user to explicitly consent to performing a privileged task. UAC also allows an administrator to perform some action that requires elevated privileges within a standard user's session.

- Tasks that are protected by UAC are shown with a Security Shield icon:

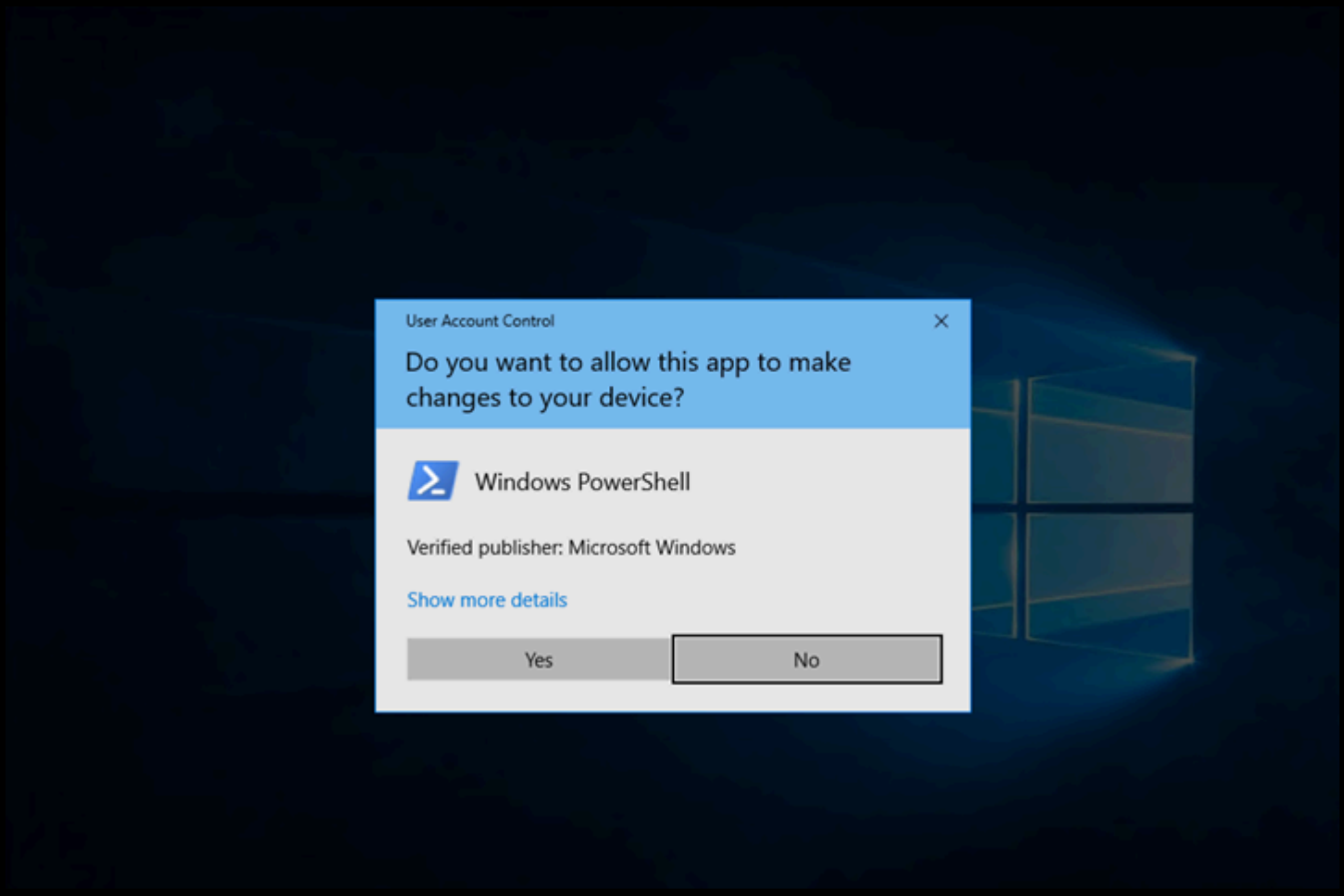


It is also possible to explicitly run a process as administrator. Some default shortcuts are set up this way. For example, the Windows PowerShell (Admin) shortcut will run as administrator. To run any shortcut as administrator, use its right-click context menu (MoreRun as administrator) or press CTRL+SHIFT+ENTER to open it.

When a user needs to exercise administrative rights, they must explicitly confirm use of those rights:

- If the logged-in account has standard privileges, an administrator's credentials must be entered via the consent dialog.
- If the logged-in account is already an administrator, the user must still click through the consent dialog.

Figure 1. UAC requires confirmation of the use of administrator privileges



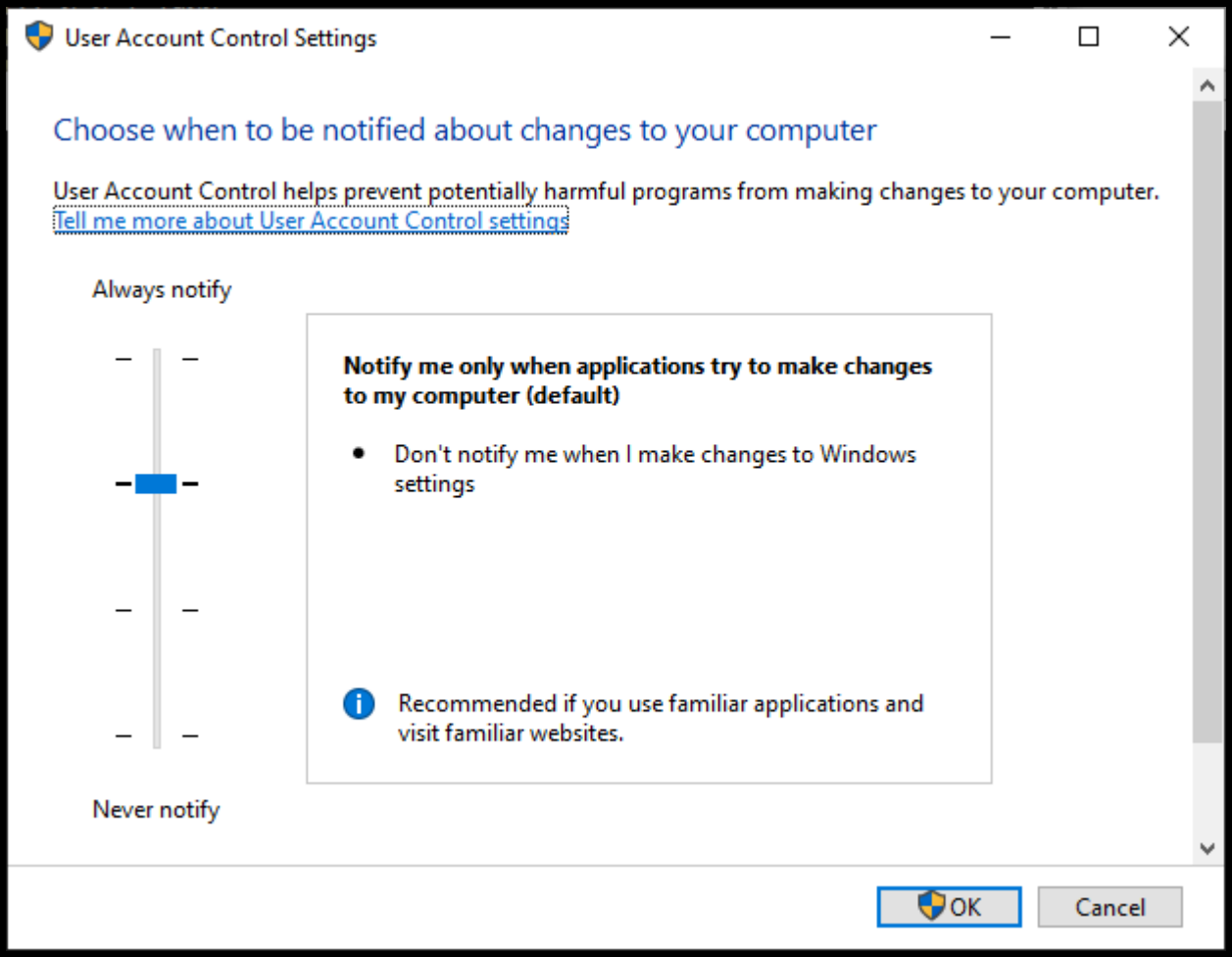
Screenshot courtesy of Microsoft.

Description

The screen reads, do you want to allow this app to make changes to your device. Windows PowerShell. Verified publisher: Microsoft Windows. A link to show more details is below. Yes and No buttons are at the bottom.

UAC protects the system from malware running with elevated administrator privileges. This is a good thing, but if you need to perform numerous system administration tasks at the same time, UAC can prove frustrating. You can configure UAC notifications to appear more or less frequently by using the configuration option in the User Accounts applet. Lowering the notification level will make the system more vulnerable to malware, however.

Figure 2. Configuring UAC notifications



Screenshot courtesy of Microsoft.

Description

The screen reads, choose when to be notified about changes to your computer. A link reads, tell me more about user account control settings. A vertical bar with never notify option at the bottom and always notify option at the top. The ok and cancel buttons are at the bottom.

Note:

Note that the default "Administrator" user account is not subject to UAC and so should be left disabled if the computer is to be used securely.

15.1.9 Authentication Methods

In an access control system, accounts are configured with permissions to access resources and (for privileged accounts) rights to change the system configuration. To access an account, the user must authenticate by supplying the correct credentials, proving that they are the valid account holder.

Zero trust is a security framework that is used in many organizations. This means that no user or device should ever be automatically trusted, regardless of their location or previous authentication. Instead of relying only on traditional security measures, zero trust requires that all users and devices are authenticated, authorized, and continuously validated before being granted access. Strict authentication should be used for all users and devices when trying to access resources on a network.

The validity of the whole access control system depends on the credentials for an account being known and used only by the account holder. The format of a credential is called an authentication factor. The principal factors are categorized as knowledge (something you *know*, such as a password), possession (something you *have,* such as a smart card or smartphone), and inherence (something you *are,* such as a fingerprint. This will typically involve biometrics).

Multifactor Authentication

Using a single factor makes authentication less reliable. A password could be shared, a device token could be stolen, or a facial recognition system could be spoofed using a photograph.

An authentication technology is considered strong if it is multifactor. **Multifactor-authentication (MFA)** means that the user must submit at least two different types of credentials, such as something you know and something you are. Submitting two of the same type of credentials is not considered multifactor authentication.

For example, the following would be a valid multifactor authentication:

- User inputs a username/password (knowledge) and also uses a fingerprint (Inherence) to sign in.

An invalid multifactor authentication example would be:

- User submits a username/password (knowledge) and a PIN (knowledge) to sign in.

Even though the user is submitting two types of authentication, they are both knowledge-based so therefore is not considered multifactor authentication.

MFA is a core component of the "never trust, always verify" principle of zero trust. By providing that second layer of authentication, it is much more difficult for an attacker to gain unauthorized access.

There are several standard multifactor technologies.

2-Step Verification

2-step verification is a means of using a soft token to check that a sign-in request is authentic. It works on the following lines:

1. The user registers a trusted contact method with the app. This could be an email account or phone number, for instance.
2. The user logs on to the app using a password or biometric recognition.
3. If the app detects a new device or that the user is signing on from a different location or is just configured by policy to require 2-step verification in all instances, it generates a token and sends this to a registered email account or phone number.
    1. The code could be delivered by email, Short Message Service (SMS text), or as an automated voice call.
4. The user must then input the soft token code within a given time frame to be granted access.

One-Time Passwords

The soft tokens may also be referred to as a one-time password (OTP). The OTP is only valid for a single login session and a new unique passcode is generated for each login attempt. OTPs add an additional level of security because even if the user's password is compromised, the attacker will not have access to the OTP.

There are a few types of one-time passwords including:

- **Time-based OTP (TOTP)** - This OTP is only valid for a set amount of time, such as 1 minute, before it expires. If the OTP is not entered within the specified timeframe, a new OTP will need to be requested.
- **Hash-based Message Authentication Code OTP (HOTP)** - This method uses an algorithm that generates the OTP using a counter-based approach. This means that each time the OTP is requested, the counter is increased which ensures that every password is unique and can only be used once.
- **Challenge-Response** - In this method, the server sends a challenge, such as a random number, to the user. This challenge is entered into the OTP generator which uses that to generate a unique OTP.

Because an OTP typically requires the user to have access to a specific device that is tied to their account, using OTPs works as a form of multifactor authentication.

Authenticator Application

An **authenticator app**, such as Microsoft Authenticator (microsoft.com/en-us/security/mobile-authenticator-app), can be used for passwordless access or used as a two-factor authentication (2FA) mechanism. This works as follows:

1. The authenticator app is installed on a trusted device that is under the sole control of the user, such as a smartphone.
    1. The smartphone must be protected by its own authentication system, such as a screen lock opened via a fingerprint.
2. The service or network that the user needs to authenticate with is registered with the authenticator app, typically by scanning a quick response (QR) code and then completing some validation checks.
    1. Registration uses encryption keys to establish a trust relationship between the service and the authenticator app.
3. When the user tries to sign in, the service or network generates a prompt on the authenticator.
    1. The user must unlock his or her device to authorize the sign-in request.
4. The authenticator then either displays a soft token for the user to input or directly communicates to the service or network that the user supplied their credential.
5. The service grants the user access.

Hard Token Authentication

A **hard token** works in the same sort of way as an authenticator app but is implemented as firmware in a smart card or USB thumb drive rather than running on a smartphone. The hard token is first registered with the service or network. When the user needs to authenticate, he or she connects the token and authorizes it via a password, PIN, fingerprint reader, or voice recognition. The token transmits its credentials to the service, and the service grants the user access. These devices are typically compliant with Fast Identity Online (FIDO) version 2 standards (fidoalliance.org/fido2).

15.2.1 Windows Login Options

Windows authentication involves a complex architecture of components (docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication), but the following three scenarios are typical:

- **Windows local sign-in** - The Local Security Authority (LSA) compares the submitted credential to the one stored in the Security Accounts Manager (SAM) database, which is part of the registry. This is also referred to as interactive logon.
    - It is still considered a local sign-in when logging in using a Microsoft Account. The Microsoft account credentials are cached in the Registry and compared when logging in using the Microsoft account.

- **Windows network sign-in** - The LSA can pass the credentials for authentication to a network service. The preferred system for network authentication is based on a system called **Kerberos**. This is typically performed when the device is connected to a domain.
- **Remote sign-in** - If the user's device is not connected to the local network, authentication can take place over some type of virtual private network (VPN) or web portal.

Username and Password

A **username and password** credential is configured by creating the user account and choosing a password. The user can change the password by pressing **CTRL+ALT+DELETE** or using account settings. An administrator can also reset the password using Local Users and Groups.

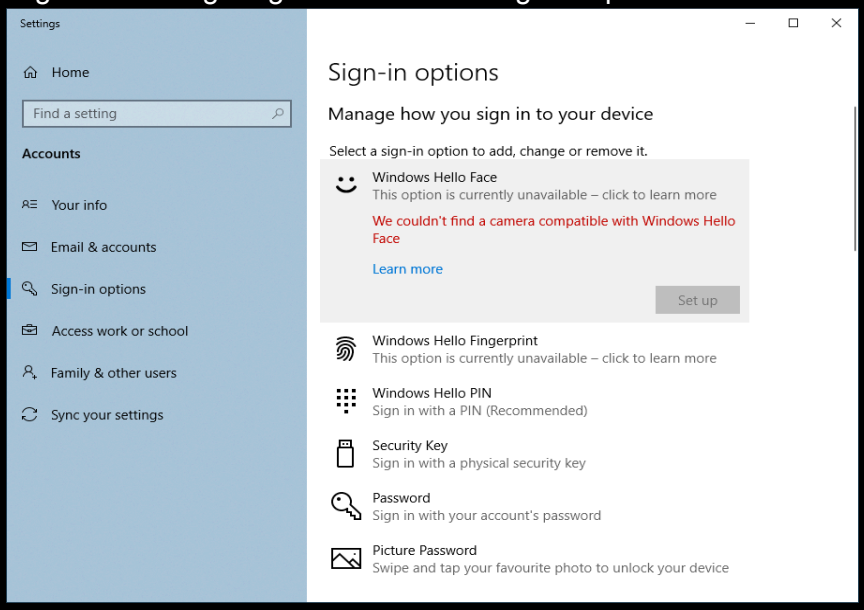
When creating passwords, you should always use a strong password or passphrase. It is important to keep up to date and follow the latest secure password creation recommendations. Organizations such as the National Institute of Standards and Technology (NIST) will release updates to secure password creation recommendations as needed.

Windows Hello

The **Windows Hello** subsystem allows the user to configure an alternative means of authenticating. Depending on hardware support, the following options are available:

- **Personal identification number (PIN)** - Unlike a normal Microsoft account password, a Windows Hello PIN is separately configured for each device. It uses the **trusted platform module** feature of the CPU or chipset and encryption to ensure that the PIN is not stored within Windows itself. This is designed to prevent the sort of sniffing and interception attacks that ordinary passwords are subject to. Despite the name, a PIN can contain letters and symbols.
  Note:
  Because the PIN is held in the TPM and the authentication happens on the device itself, the PIN will not need to be verified over a network link. This is a key feature of the Windows Hello PIN ensuring that a user can login to the device even when offline.

Figure 1. Configuring Windows Hello sign-in options



Description

The menu on the left has a find a setting field at the top followed by options your info, email and accounts, sign-in options, access work or school, family and other users, and sync your settings. The right panel displays the title Sign-in options to manage how you sign in to your device. Select a sign in option to add, change or remove it. The sign options listed below are: Windows Hello Face Windows Hello Fingerprint Windows Hello PIN Security Key Password Picture Password

Note:

A PIN must be configured to set up Windows Hello. The PIN acts as a backup mechanism in case other methods become unavailable. For example, a camera may fail to work and make facial recognition impossible, or a hardware token might be lost or temporarily unavailable.

- **Fingerprint** - This type of biometric gesture authentication uses a sensor to scan the unique features of the user's fingerprint.
- **Facial recognition** - This biometric login uses a webcam to scan the unique features of the user's face. The camera records a 3-D image using its infrared (IR) sensor to mitigate attempts to use a photo to spoof the authentication mechanism.
- Security key - This uses a removable USB token or smart card. It can also use a trusted smartphone with an NFC sensor.

Note:

From these descriptions, it might seem like only one factor is used, but there are two. The second factor is an encryption key stored in the TPM.

Single Sign-On

Single sign-on means that a user authenticates once to a device or network to gain access to multiple applications or services. The Kerberos authentication and authorization model for Active Directory domain networks implements SSO. A user who has authenticated with Windows has also authenticated with the Windows domain's SQL Server and Exchange Server services.

The advantage of SSO is that each user does not have to manage multiple digital identities and passwords. The disadvantage is that compromising the account also compromises multiple services. The use of passwords in SSO systems has proven extremely vulnerable to attacks.

The Windows Hello for Business mechanism seeks to mitigate these risks by transitioning to passwordless SSO. In general terms, this works as follows:

1. The user device is registered on the network. This uses a public/private encryption key pair. The private key is only stored within the TPM of the user device and never transmitted over the network or known by the user. The public key is registered on the server.

2. When the user authenticates to the device via Windows Hello, the device communicates a secret encrypted by its private key to the network authentication server.

3. The server uses the public key to decrypt the secret. This proves that the secret really did come from the device as it could only have been encrypted by the private key. Therefore, the network server can authenticate the user account and issue it with an authorization token to use network services and applications.

Security Assertions Markup Language (SAML)

Security Assertions Markup Language (SAML) is a special type of SSO. With SAML, an Identity Provider (IdP) is used to pass user credentials to a service provider (SP). This process works as below:

- The user attempts to login to the service provider, such as Google Workspace.

- The SP redirects the users to the identity provider which may be the company's login portal.

- The user authenticates with their company credentials.

- The IdP creates a SAML assertion which is a digitally signed document that contains the user's credentials.
- The SAML is sent to the service provider.
- The SP verifies the SAML assertion and grants the user access to the requested resources.

For example, a user signs in to Windows with a Microsoft account and is also signed in to cloud applications such as OneDrive and Microsoft 365.

15.2.2 Windows Domains and Active Directory

A local account is only recognized by the local machine and cannot be used to access other computers. For example, if the user David needs access to multiple computers in a workgroup environment, a separate local account must be configured on each computer (`PC1\David`, `PC2\David` , and so on). These accounts can use the same names and passwords for convenience, but the user must still authenticate to the accounts separately. Password changes are not synchronized between the machines and must be updated manually.

This model does not scale well to large numbers of users. Consequently, most business and educational organizations use Windows domain networks and accounts. A domain account can be authorized to access any computer joined to the domain. It can be assigned permissions on any resources hosted in the domain.

Domain Controllers

To create a **domain**, you need at least one Windows Server computer configured as a domain controller (DC). A DC stores a database of network information called **active directory**. This database stores user, group, and computer objects.

Active Directory is perhaps the most used directory service program, but there are other directory service products available.

Remember that accounts and security groups in a domain are configured in the Active Directory database stored on a Domain Controller, not on each PC. The Active Directory Users and Computers management console is used to create and modify AD accounts. When managing objects that only exist on a local machine, the local users and groups console would still be used.

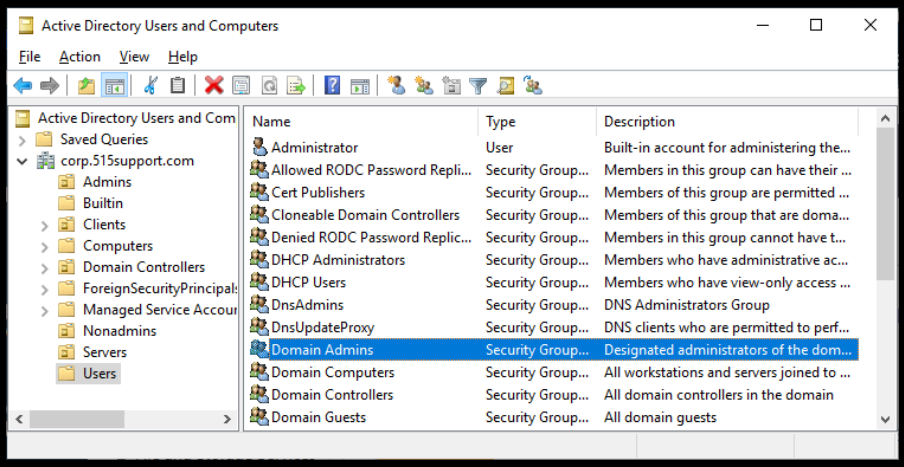
The DC is responsible for providing an authentication service to users as they attempt to sign in. Management of DCs and rights to create accounts in the domain is reserved to Domain Admins. This network model is centralized, robust, scalable, and secure.

Member Servers

A **member server** is any server-based system that has been joined to the domain but does not maintain a copy of the Active Directory database. A member server provides file and print and application server services, such as Exchange for email or SQL Server for database or line-of-business applications. AD uses the Kerberos protocol to provision single sign-on authentication and authorization for compatible applications and services.

Security Groups

A domain supports the use of a **security group** to assign permissions more easily and robustly. User accounts are given membership in a security group to assign them permissions on the network. These permissions apply to any computer joined to the domain. For example, members of the Domain Admins security group can sign in on any computer in the domain, including DCs. A member of the Domain Users security group can only sign in on certain workstations and has no rights to sign in on a DC. Figure 1. Security groups in Active Directory



The users option from the menu on the left is selected. A table with heads name, type, and description is on the right.

Users are not the only objects that are managed and listed in AD. Computers and devices that have joined the domain are also represented by account objects.

Organizational Units

An **organizational unit** is a way of dividing a domain up into different administrative realms. You might create OUs to delegate responsibility for administering company departments or locations. For example, a "Sales" department manager could be delegated control with rights to add and delete user accounts and assign them to a Sales security group, but no rights to change account policies, such as requiring complex passwords. Standard users in the Sales OU could be permitted to sign in on computers in the Sales OU, but not on computers in other OUs.

Using PowerShell

Organizational Units can be created in PowerShell using the `New-ADOrganizationalUnit` cmdlet along with the following commonly used switches:

- `-Name`: Specifies the name of the new Organizational Unit you are creating.
- `-Path`: Specifies the distinguished name (DN) of the container or OU where the new Organizational Unit will be created. This is typically written using components like `OU=` and `DC=` to represent OUs and domain components.
- `-ProtectedFromAccidentalDeletion`: Controls whether the OU is protected from accidental deletion:
    - `$true`: Enables protection, requiring extra steps to delete the OU.
    - `$false`: Disables protection, allowing the OU to be deleted more easily.

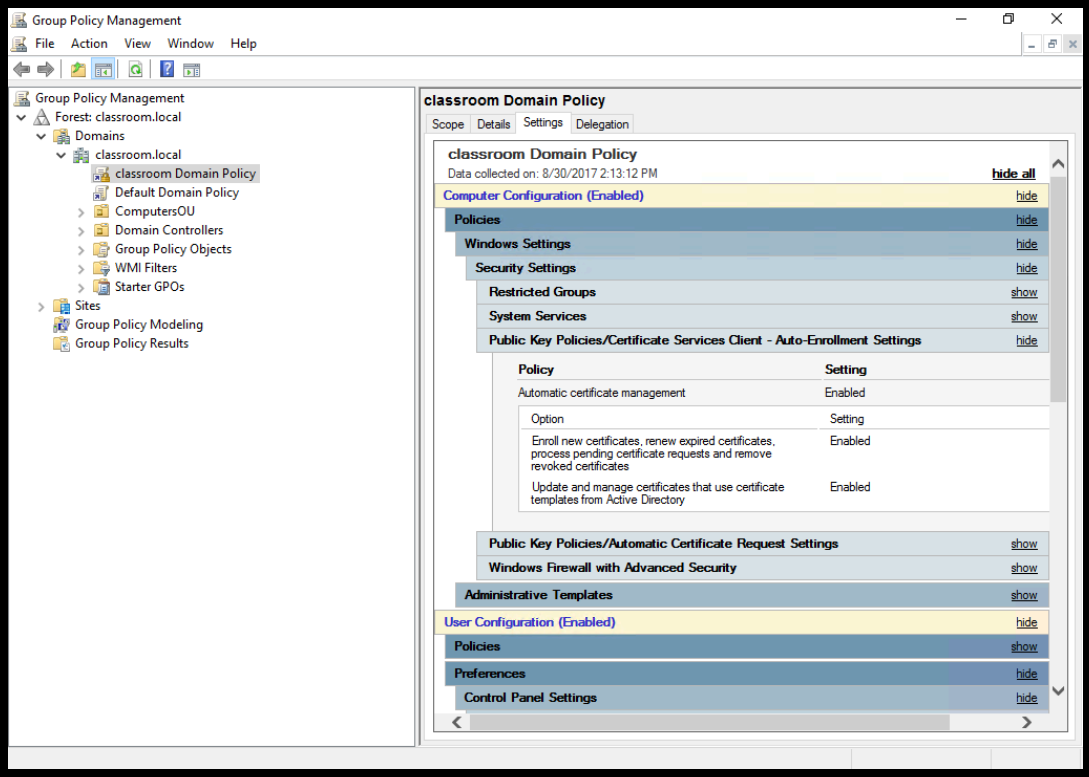
Example usage:

- `New-ADOrganizationalUnit -Name "OUName" -Path "ParentDN" -ProtectedFromAccidentalDeletion $true`

15.2.4 Group Policy and Login Scripts

A domain **group policy** configures computer settings and user profile settings. Some settings are exposed through standard objects and folders, such as Security Settings. Other settings are exposed by installing an Administrative Template. Administrative Templates can be used to define settings in third-party software too. Group policy can also be used to deploy software automatically.

Figure 1. Group Policy Management



Description

The classroom domain policy option from the menu on the left is selected. The settings tab on the right has tabs labeled policies, window settings, security settings, restricted groups, system services, public key policies or certificate services client, public key policies or automatic certificate request settings, windows firewall with advanced security, and administrative templates.

Unlike a local computer, domain **group policy object** can be applied to multiple user accounts and computers. This is done by linking a GPO to a domain or OU object in AD. For example, you could attach Sales GPOs to the Sales OU and the policies configured in those GPOs would apply to every user and computer account placed in the Sales OU. A

domain or OU can be linked to multiple GPOs. A system of inheritance determines the resultant set of policies (RSoPs) that apply to a particular computer or user account.

Group Policy Updates

When **updating** local or group security policies, it is important to be familiar with the use of two command-line tools:

- **gpupdate/gpresult commands** - Policies are applied at sign-in and refreshed periodically (normally every 90 minutes). The gpupdate command is used to apply a new or changed policy to a computer and account profile immediately. Using the `/force` switch causes all policies (new and old) to be reapplied. The `gpupdate` command can be used with `/logoff` or `/boot` to allow a sign-out or reboot if the policy setting requires it.

- `gpresult` - This command displays the RSoP for a computer and user account. When run without switches, the help page is displayed. The /s, /u, and /p switches can be used to specify a host (by name or IP address), user account, and password, and /r can be used to display policies for the desktop.

Login Scripts

A **login script** performs some type of configuration or process activity when the user signs in. A login script can be defined via the user profile or assigned to an account via group policy. A login script can be used to configure the environment for the user-setting environmental variables, mapping drives to specific server-based folders, and mapping to printers or other resources, for example.

A login script can also be used to ensure that the client meets the security requirements for signing on to the network. For example, if the client has out-of-date software, login can be denied until the software is updated.

Note:

Most of these tasks can be implemented via GPO. Some companies prefer to use login scripts, and some prefer GPO.

15.3.1 Workgroup Setup

As well as user management, the network model determines how shared resources are administered. A **workgroup** is a peer-to-peer network model in which computers can share resources, but management of each resource is performed on the individual computers. A **domain** is based on a client/server model that groups computers together for security and to centralize administration. Some computers are designated as servers that host resources, while others are designated as clients that access resources. Administration of the servers and clients is centralized.

Joining a Workgroup

Windows setup automatically configures membership of the default workgroup, named `WORKGROUP`. Each computer is identified in the network browser by a hostname. The hostname can be changed using the **System Properties** dialog (`sysdm.cpl`).

Note:

The workgroup name can be changed via System Properties. It is almost always left set to WORKGROUP.

Network Discovery and File Sharing

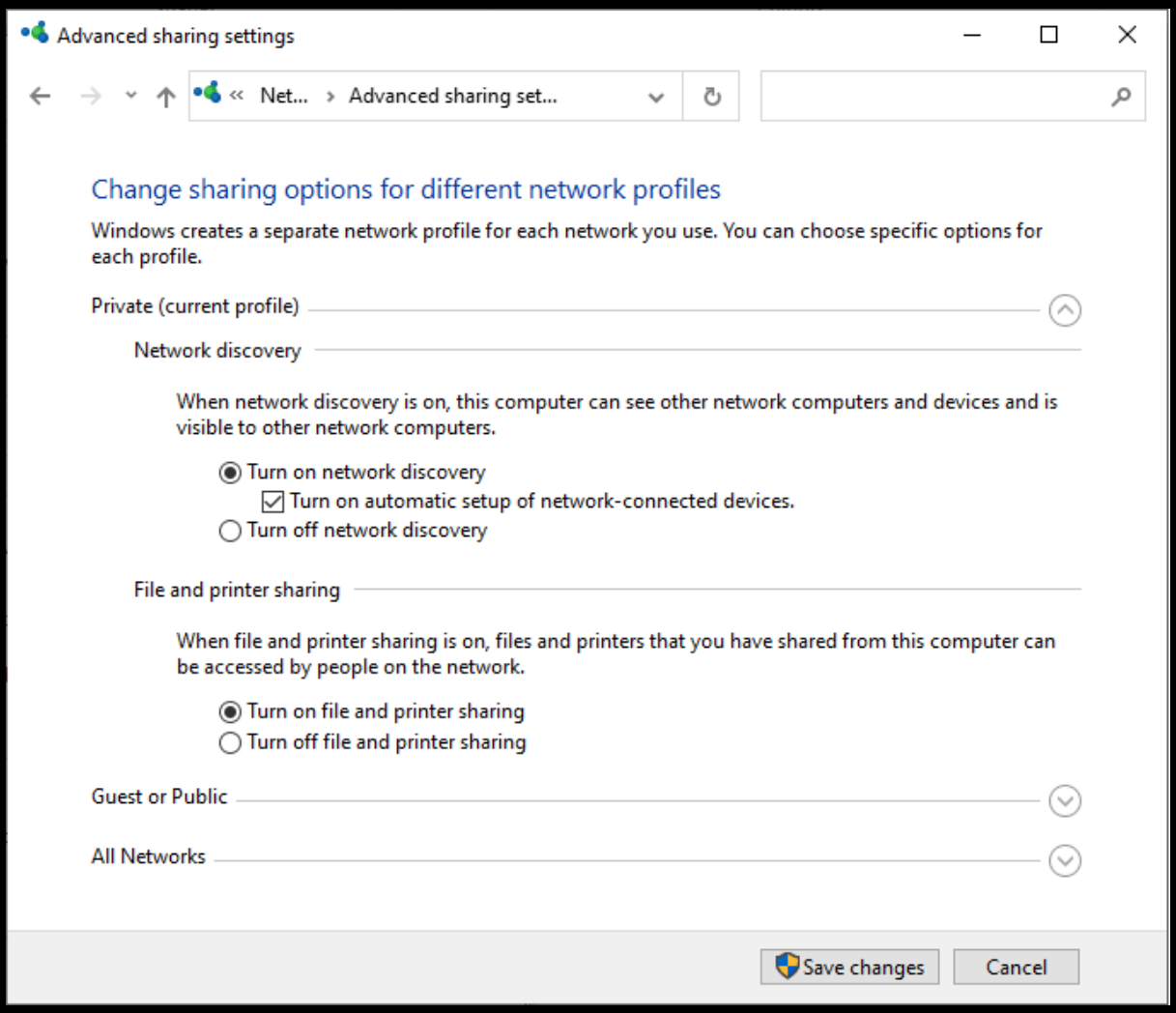
Within a workgroup, the network type must normally be set to Private to make the computer discoverable and allow sharing. If the network type is Public, a notification will display in File Explorer when the Network object is selected. You can use this notification to make the network private. You can also change the network type via Network & Internet settings.

Note:

It is possible to enable discovery and sharing on public networks, but this will apply to all public networks and so is not recommended

Sharing options are configured via the **Advanced sharing settings** applet in Control Panel. To share files on the network, **Turn on network discovery** and **Turn on file and printer sharing** must both be selected.

Figure 1. Advanced sharing settings



Description

The head reads, change sharing option for different network profiles. The three profiles are listed below: Private (Current profile) with network discovery and file and printer sharing options. Radio buttons to turn on and off are present under each option. Guest or Public. All networks. The save changes and cancel button are at the bottom.

Note:

For password-protected sharing, network users must have an account configured on the local machine. This is one of the drawbacks of workgroups compared to domains. Either you configure accounts for all users on all machines and manage passwords on each machine manually, use a single shared account for network access (again, configured on all machines), or disable security entirely.

Windows also supports nearby sharing. This refers to sharing data between a PC and smartphone or another device over Bluetooth in a personal area network (PAN). This is a simple way to exchange files between devices. Files are saved to the user's Downloads folder.

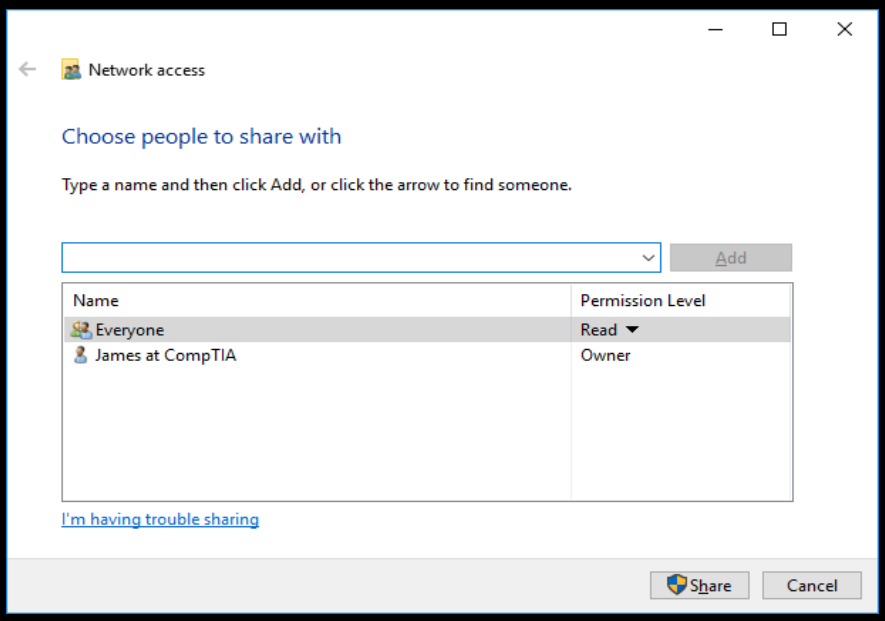
15.3.2 File Share Configuration

Simply enabling **file sharing** does not make any **resources** available. To do that, you need to configure a file share.

In a workgroup, you can enable Public folder sharing to make a shared resource available quickly. The public folder is a directory that all users of the computer can read and write to. This can be shared over the network by selecting the option under Advanced sharing settings All networks Turn on sharing so anyone with network access can read and write files in the Public folders.

To share a specific folder, right-click it and select **Give access to**. Select an account, and then set the **Permission level** to **Read** or **Read/write** as appropriate.

Figure 1. Configuring a file share



A link at the bottom reads, I'm having trouble sharing. Share and cancel buttons are at the bottom.

Note:

"Everyone" is a special system group that contains all user accounts. This system group is often used to configure shares.

The **Share** tab in the folder's Properties dialog can be used to customize permissions, change the share name, and limit the number of simultaneous connections. Windows desktop versions are limited to 20 inbound connections.

In addition to any local shares created by a user, Windows automatically creates hidden administrative shares. These include the root folder of any local drives (`C$`) and the system folder (`ADMIN$`). Administrative shares can only be accessed by members of the local Administrators group.

Note:

Note that if you disable password-protected sharing, the administrative shares remain password-protected.

In fact, if you add a `$` sign at the end of a local share name, it will be hidden from general browsing too. It can still be accessed via the command-line or by mapping a drive to the share name.

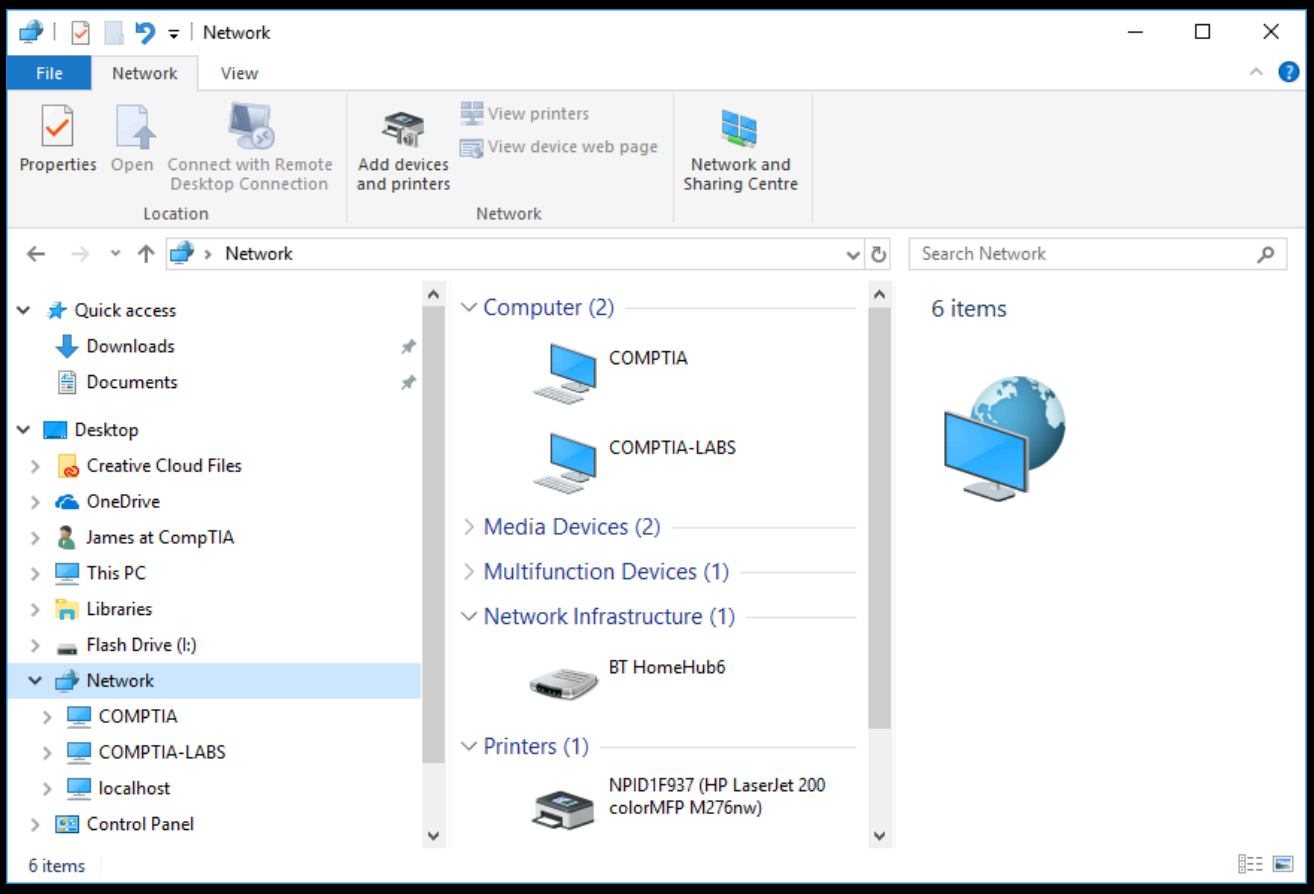
15.3.3 Network Browsing and Mapping Drives

On both workgroup and domain networks, shares are listed by the **file server** computer under the Network object in File Explorer. Each computer is identified by its hostname. You can browse shares by opening the computer icons. Any network-enabled devices such as wireless displays, printers, smartphones, and routers/modems are also listed here.

Note:

The Universal Naming Convention (UNC) syntax used to identify the path of a network resource is \\server\share.

Figure 1. Viewing devices in a workgroup network



Screenshot courtesy of Microsoft.

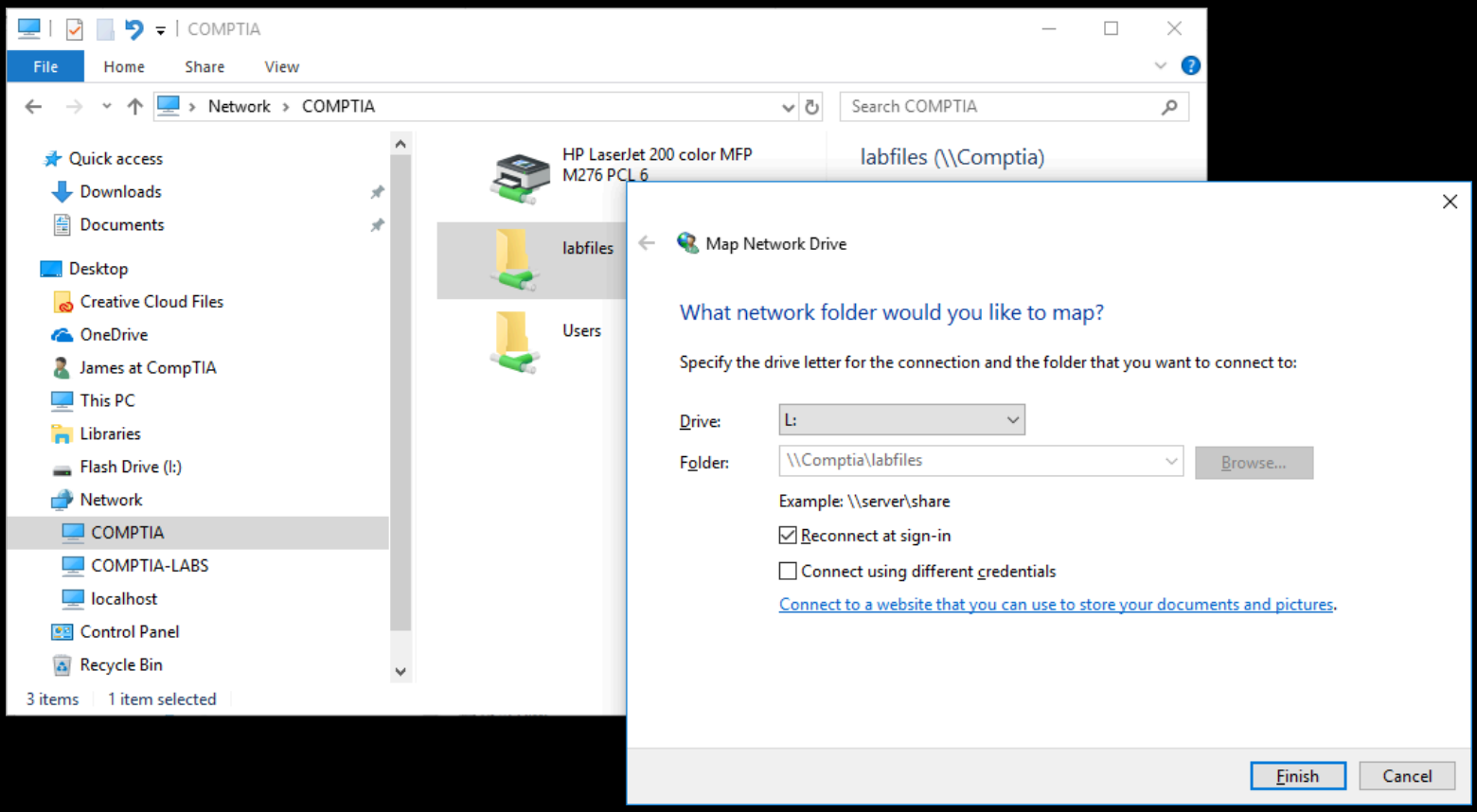
Description

The devices under the head computer (2) are COMPTIA and COMPTIA-LABS. Further media devices (2), multifunctional devices (1), and network infrastructure (1) containing B T HomeHub6 and Printers (1) containing N P I D 1 F 937 are listed below. 6 items is written on the right.

Mapped Drives

A **mapped drive** is a share that has been assigned to a drive letter on a client device. To map a share as a drive, right-click it and select **Map Network Drive**. Select a drive letter and keep **Reconnect at sign-in** checked unless you want to map the drive temporarily. The drive will now show up under This PC. To remove a mapped drive, right-click it and select **Disconnect.**

Figure 2. Mapping a network drive to a LABFILES share hosted on COMPTIA (\\COMPTIA\labfiles)



Screenshot courtesy of Microsoft.

Description

The question reads, what network folder would you like to map. The text below reads, specify the drive letter for the connection and the folder that you want to connect to. The fields for drive and folder are given below. The checkboxes read, reconnect at sign in and connect using different credentials. A link below reads, connect to a website that you can use to store your documents and pictures.

Network resources can be accessed by either using UNC or mapping as a drive. Mapping a drive provides a drive letter and the option to make the connection persistent whereas using UNC will provide on-demand access only.

net use Commands

There are several `net` and `net use` command utilities that you can use to view and configure shared resources on a Windows network. The net command will most often be used in an Enterprise Windows network for consistent access to shared network resources.

A few of the commands are provided here, but you can view the full list by entering `net /?`

net view

- Displays a list of servers on the local network.

net view \\MYSERVER

- View the shares available on a server named MYSERVER

net use M: \\MYSERVER\DATA /persistent:yes

- Maps the DATA folder on MYSERVER to the M: drive and sets the mapped drive to stay mapped even after a reboot.
- If the persistent switch is not used, then the shared resource will not stay mapped after a reboot and it will have to be manually mapped again.

net use M: /delete

- Removes the mapping of the M: drive

net use * /delete

- Removes all mapped drives.

If using the net command results in failure, it's a good idea to verify that the resource is reachable, permissions are properly configured, and the path is correct. These are the main reasons why the net command might fail.

15.3.4 Printer Sharing

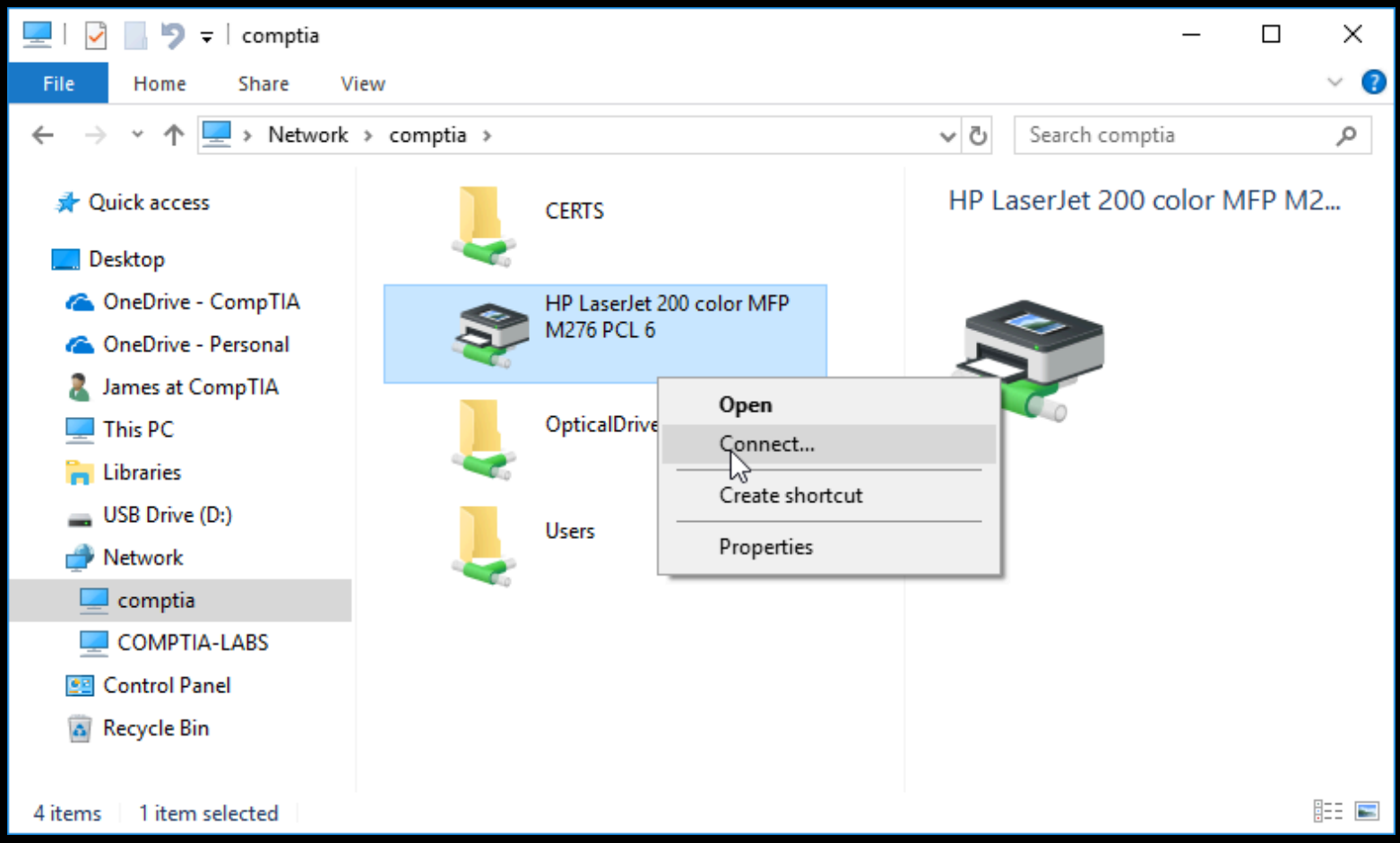
Many print devices come with an integrated Ethernet and/or Wi-Fi adapter. This means that they can communicate directly on the network. Such a printer can be installed using the Add Printer wizard (from Devices and Printers). Just enter the IP address or hostname of the printer to connect to it. Each computer on the network can connect to this type of printer independently.

Any printer object set up on a Windows host can also be shared so that other network users can access it. This means that the printer can only be accessed when the Windows machine is on. Print jobs and permissions are managed via the Windows host.

A printer is shared on the network via the **Sharing** tab in its **Printer Properties** dialog. Check **Share this printer** and enter a descriptive name. Optionally, use the **Additional drivers** button to make drivers available for different client operating systems. For example, if the print server is Windows 10 64-bit, you can make 32-bit Windows 7 drivers available for other client devices.

To connect to a shared printer, open the server object from Network and the printer will be listed. Right-click it and select **Connect**.

Figure 1. Connecting to a printer shared via the COMPTIA PC



Screenshot courtesy of Microsoft.

Description

The options read, CERTS, HP LaserJet 200 Color MFP M276 PCL 6, optical drive and users. HP LaserJet 200 Color MFP M276 PCL 6 has a context menu. The options in the menu reads, open, connect, create shortcut, and properties. Connect is selected.

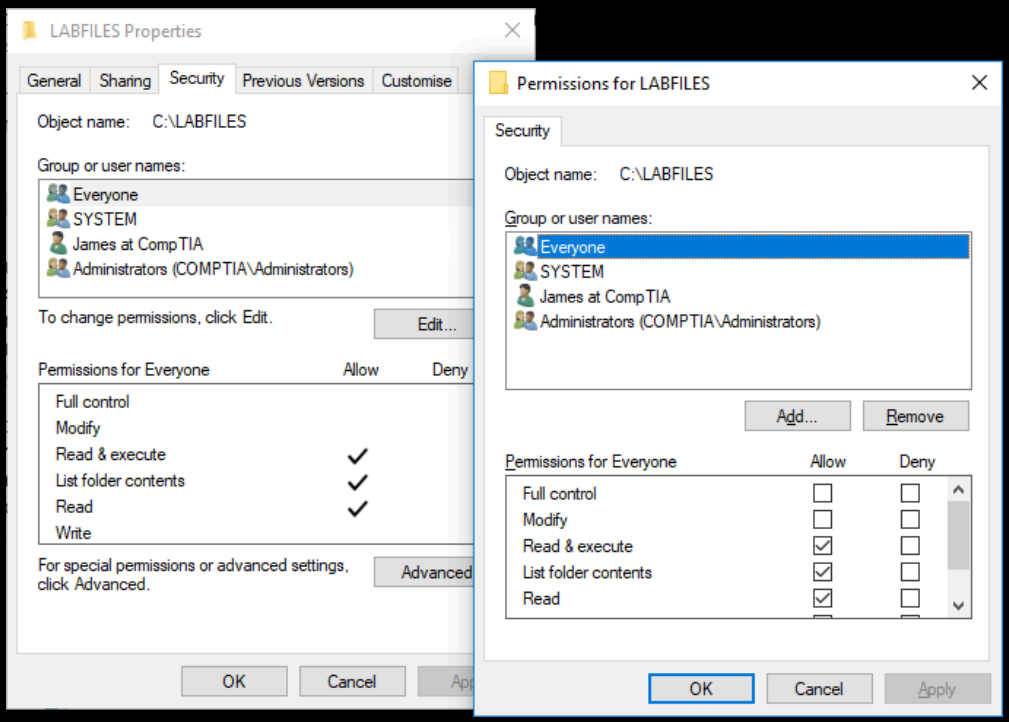
15.3.5 NTFS versus Share Permissions

When sharing a folder, the basic **Give access to** interface conceals some of the complexity of the Windows **NTFS versus share** permissions system:

- Share-level permissions only apply when a folder is accessed over a network connection. They offer no protection against a user who is logged on locally to the computer hosting the shared resource.
- **NTFS permissions** are applied for both network and local access and can be applied to folders and to individual files. NTFS permissions can be assigned directly to user accounts, but it is better practice to assign permissions to security groups and make users members of appropriate groups.

NTFS permissions can be configured for a file or folder using the **Security** tab in its properties dialog.

Figure 1. Configuring NTFS permissions via the Security tab for a folder



Screenshot courtesy of Microsoft.

Description

The security tab is selected under LABFILES properties. It lists the object name, group or user names. An edit button is on the left to change permissions. The screen further lists permissions for everyone with an advanced button for special permissions or advanced settings. Ok, cancel, and apply buttons are at the bottom. The security tab is selected

under permissions for LABFILES. It lists the object name and the group or user names. Add and remove buttons are at the bottom. Below are the permissions for everyone with a checkbox to allow and deny them. Ok, cancel, and apply buttons are at the bottom.

The Security tab shows the ACL applied to the file or folder. Each access control entry (ACE) assigns a set of permissions to a principal. A principal can either be a user account or a security group. The simple permissions are as follows:

- Read/list/execute permissions allow principals to open and browse files and folders and to run executable files.
- Write allows the principal to create files and subfolders and to append data to files.
- Modify allows the principal write permission plus the ability to change existing file data and delete files and folders.
- Full control allows all the other permissions plus the ability to change permissions and change the owner of the file or folder.

Each permission can be configured as either allow or deny. If permissions are not defined, then the default option of implicit deny takes effect. Permissions that are defined are known as explicit and permissions that take effect because they are not defined are known as implicit.

A user may obtain multiple permissions from membership to different groups or by having permissions allocated directly to his or her account. Windows analyzes the permissions obtained from different accounts to determine the most effective permissions. The order of permissions from most restrictive to least restrictive are:

- Explicit Deny
- Explicit Allow
- Implicit Deny
- Implicit Allow

If permissions conflict with each other, Windows will default to the most restrictive permission.

Putting explicit deny permissions to one side, the user obtains the most effective allow permissions obtained from any source. For example, if membership of a "Sales" group gives the user `Read` permission and membership to a "Managers" group gives the user `Modify` permission, the user's effective permission is `Modify`.

Note:

If a user attempts to view or save a file with insufficient permissions to do so, Windows displays an Access Denied error message. The Advanced interface includes a tool that can be used to evaluate effective permissions for a given principal.

Using PowerShell

File and folder permissions can be configured with PowerShell using the `icacls` command. This tool allows you to adjust inheritance, remove existing permissions, and grant new permissions for users and groups.

The following `icacls` options are commonly used when setting custom permissions on folders:

- `"Path"`: Specifies the file or folder whose permissions you are modifying.
- `/inheritance:d`: Disables permission inheritance from the parent folder so that the item's permissions can be managed independently.
- `/remove:g GroupOrUser`: Removes all granted (allow) permissions for the specified user or group from the access control list.
- `/grant GroupOrUser:(OI)(CI)F`: Grants permissions to a user or group with additional flags:
  - `GroupOrUser`: The user or group to which you are granting permissions.
  - `(OI)`: Object Inherit – the permissions apply to files within the folder.
  - `(CI)`: Container Inherit – the permissions apply to subfolders within the folder.
  - `F`: Full control permission.

Example usage:

- `icacls "C:\Users\UserName\Pictures" /inheritance:d`
- `icacls "C:\Users\UserName\Pictures" /remove:g Users`
- `icacls "C:\Users\UserName\Pictures" /grant GroupName:(OI)(CI)F`

15.3.7 Permissions Inheritance

When folders are secured using NTFS and/or share permissions, the matter of **inheritance** needs to be considered.

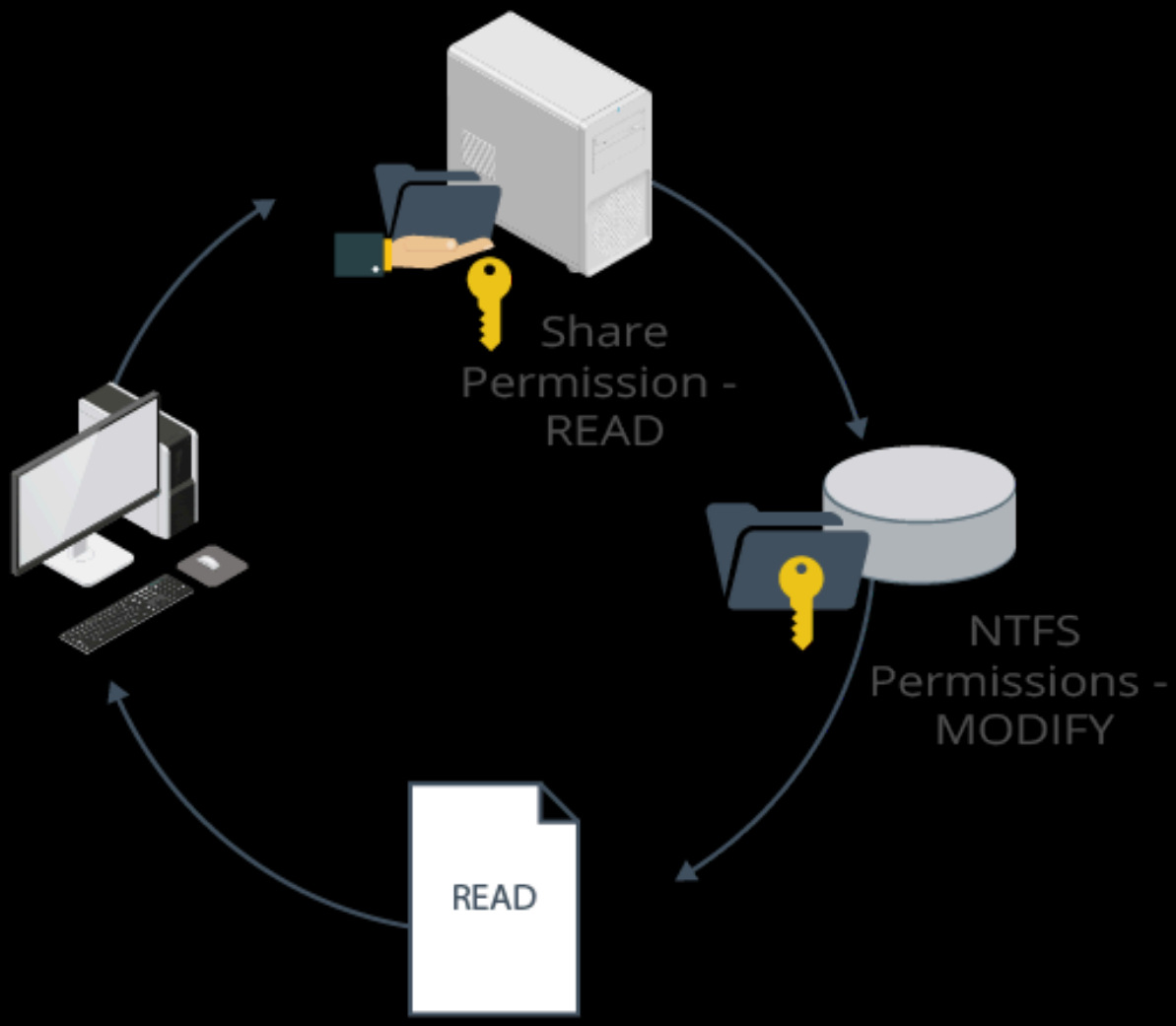
The first consideration is that NTFS permissions assigned to a folder are automatically inherited by the files and subfolders created under the folder. This default inheritance behavior can be disabled via Security Advanced Permission tab, however.

Note:

Directly assigned permissions (explicit permissions) always override inherited permissions, including "deny" inherited permissions. For example, if a parent folder specifies deny write permissions but an account is granted write permissions directly on a child file object, the effective permission will be to allow write access on the file object.

The second consideration is the combination of share and NTFS permissions. The permissions design needs to account for the following factors:

- Share permissions only protect the resource when it is accessed across the network; NTFS permissions apply locally and across the network.
- Share permissions are set at the root of the share and all files and subdirectories inherit the same permissions.
- NTFS permissions inheritance is configurable and therefore is used in combination with the share permissions to provide greater flexibility; for example, to place more restrictive permissions at lower levels in the directory structure.
- If both share and NTFS permissions are applied to the same resource, the most restrictive applies when the file or folder is accessed over the network. For example, if the group "**everyone**" has `Read` permission to share and the "Users" group is given `Modify` permission through NTFS permissions, the effective permissions for a member of the "Users" group will be `Read`. Figure 1. Effective permissions through a shared folder



Note:

Disk partitions using the FAT32 file system can only be protected using share permissions.

As the interaction between these permissions is quite complex, most of the time, the shared folder permission is set to **Full Control** for either the Everyone or Authenticated Users default groups. The effective permissions are managed using NTFS security.

Note:

The Authenticated Users system group excludes guests.

A+ Core 1 and Core 2 CertMaster Perform 15.0

15.3.8 Domain Setup

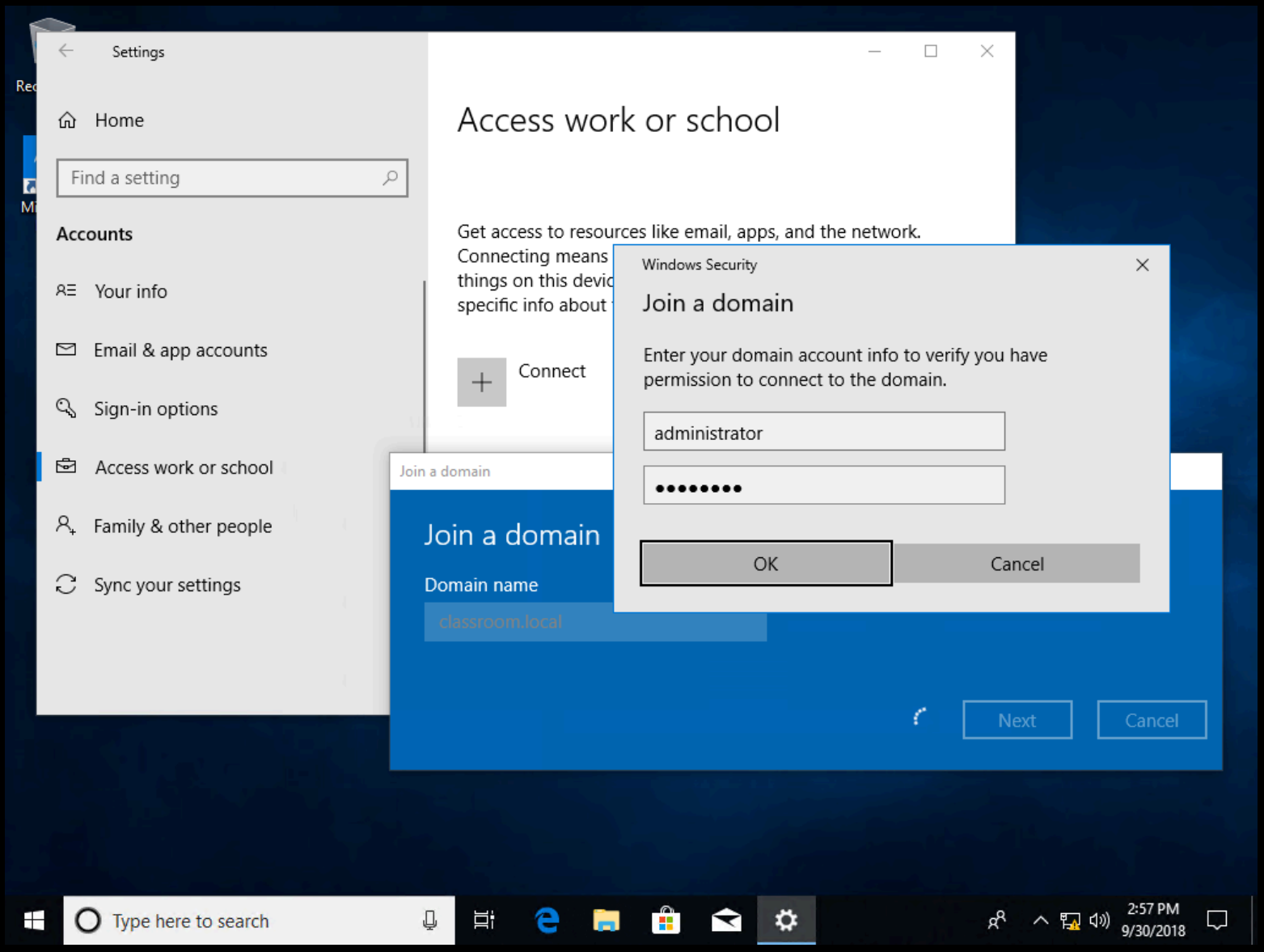
When a computer is joined to a domain rather than a workgroup, it is put under the control of the domain administrators. To communicate on a domain, the computer must have its own account in the domain. This is separate from any user accounts that are allowed to sign in.

Note:

The Windows Home edition cannot join a domain.

Windows does not support joining the computer to a domain during an attended installation. The computer can be joined during an unattended installation by using an answer file or script. Otherwise, you use either the **Access work or school** option in the **Account** settings app or the **System Properties** (`sysdm.cpl`) dialog to join a domain. The computer must be on the domain network and configured by DHCP with an appropriate IP address and DNS servers. Each domain is identified by a FQDN, such as `ad.company.example`, and the local computer must be able to resolve this name via DNS to join. The credentials of an account with appropriate administrative privileges on the domain must be input to authorize the new computer account.

Figure 1. Joining a domain using the Settings app



Screenshot courtesy of Microsoft.

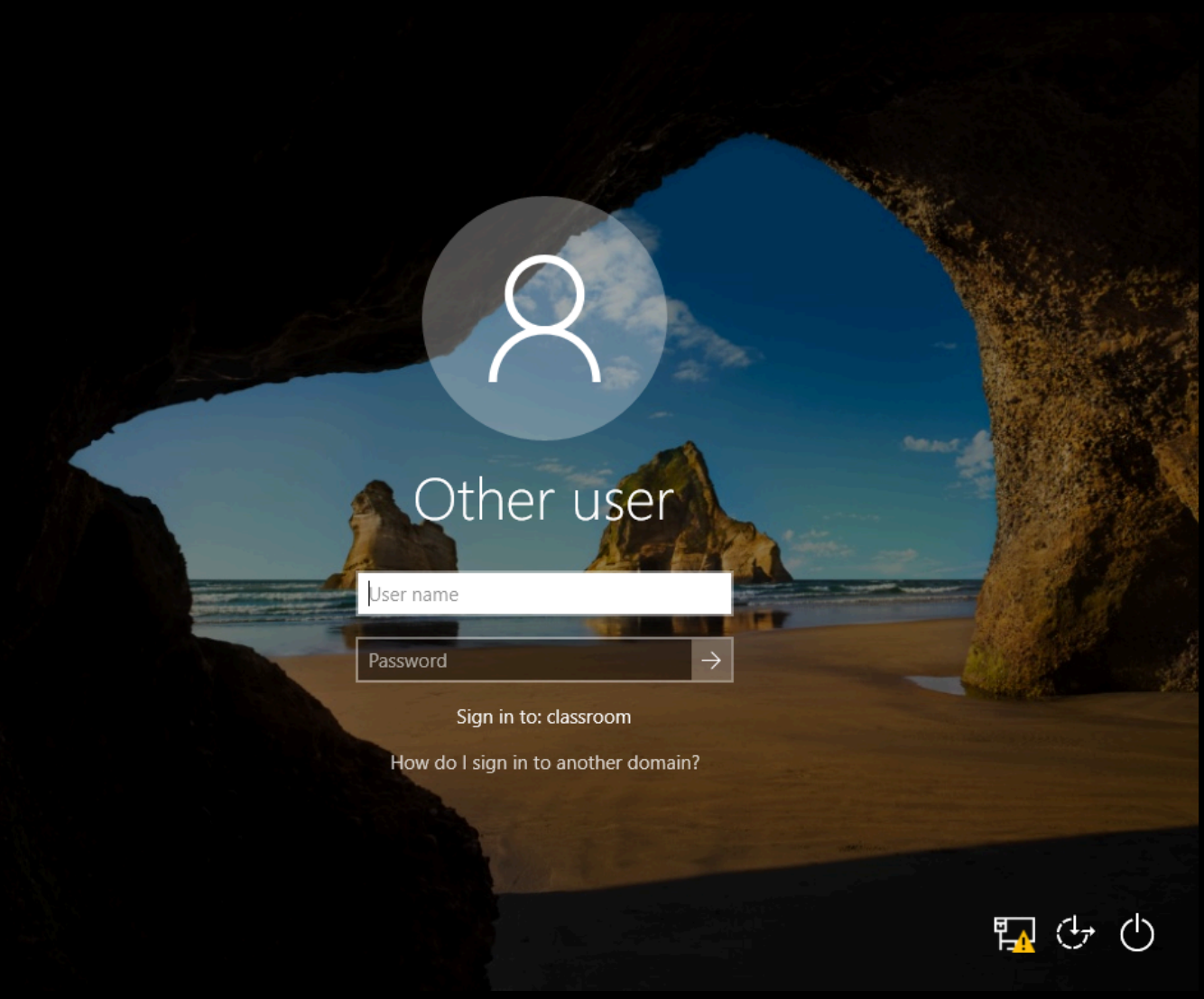
Description

The join a domain prompt asks to enter your domain account info to verify you have permission to connect to the domain. A field below reads, administrator and another has a password. Ok and cancel buttons are below.

The same interfaces can be used to detach the computer and revert to workgroup use. This requires a user account that is a member of the local Administrators group.

To use services in the domain, the user must sign in to the PC using a domain account. The **Other user** option in the sign-in screen will provide a domain option if it is not the default. You can also enter a username in the format `Domain\Username` to specify a domain login.

Figure 2. Signing in to a domain



Description

A question at the bottom reads, How do I sign in another domain.

Note:

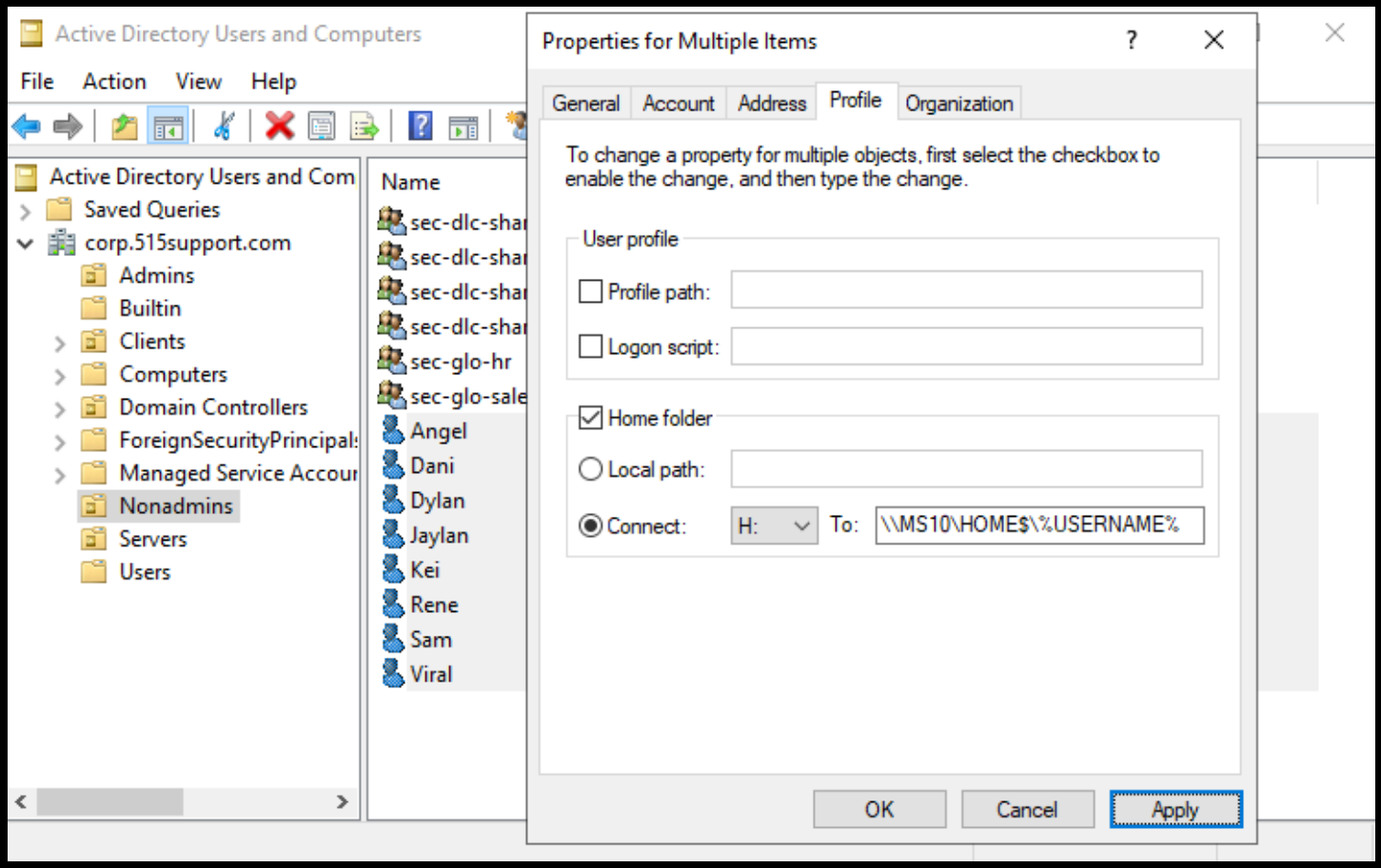
Conversely, when a machine is joined to a domain, `.\Username` or `hostname\username` will authenticate against a local user account.

15.3.9 Home Folders

On a domain, data storage and PC configuration should be as centralized as possible so that they can be more easily monitored and backed up. This means that user data should be stored on file servers rather than on local client computers. Various settings in Active Directory can be used to redirect user profile data to network storage.

A **home folder** is a private drive mapped to a network share in which users can store personal files. The home folder location is configured via the account properties on the **Profile** tab using the Connect to box. Enter the share in the form `\\SERVER\HOME$\%USERNAME%` , where `\\SERVER\HOME$` is a shared folder created with the appropriate permissions to allow users to read and write their own subfolder only.

Figure 1. When the user signs in, the home folder appears under This PC with the allocated drive letter

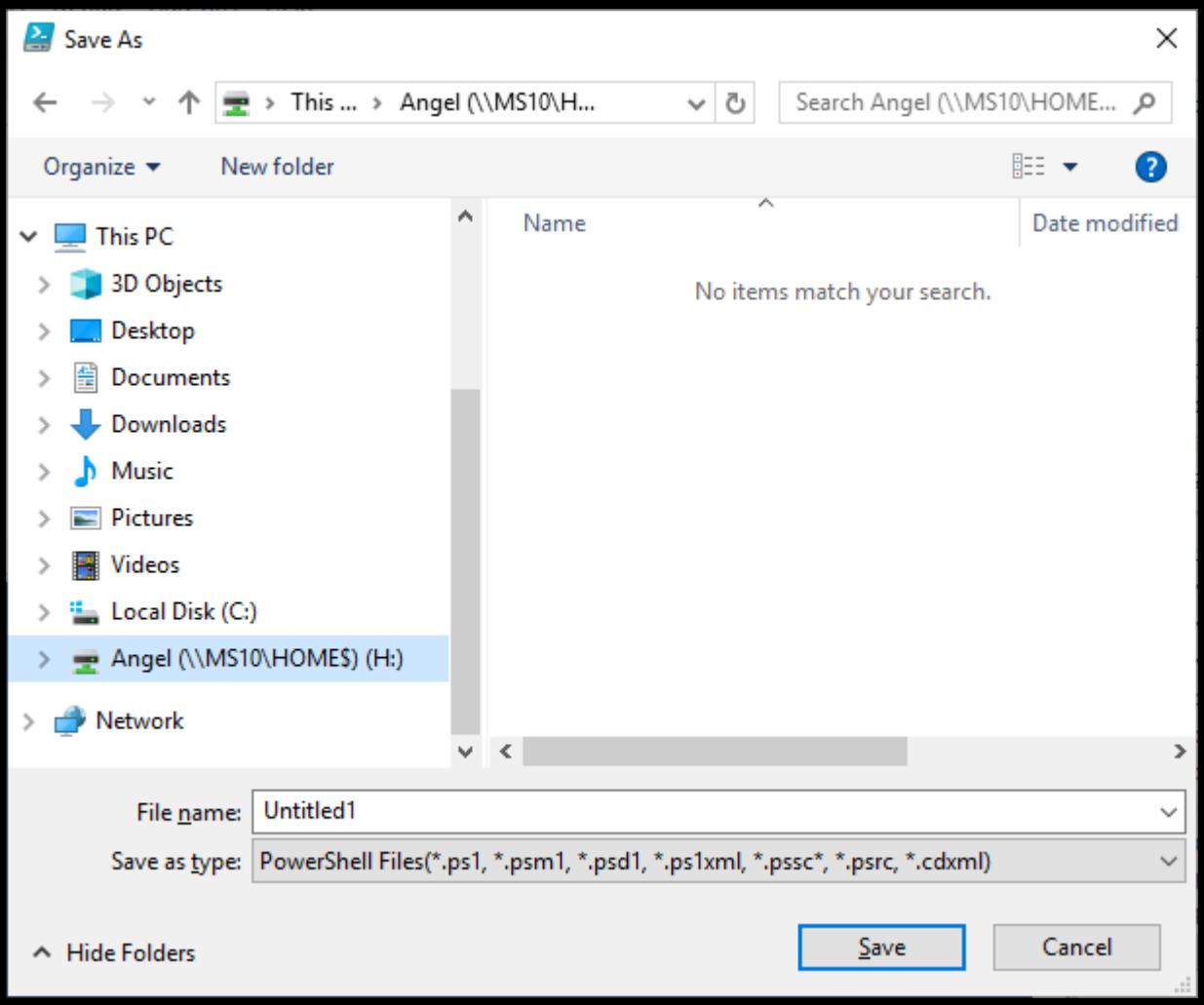


Description

Nonadmins is selected from the menu on the left. The text in the dialog box reads, to change a property for multiple objects, first select the checkbox to enable the change, and then type the change. The user profile has blank fields for profile path and logon script. The home folder is checked in and has blank filed for local path and a radio button to connect H colon to a user. Ok, cancel, and apply buttons are at the bottom.

When the user signs in, the home folder appears under This PC with the allocated drive letter:

Figure 2. Using the home folder location to save a file



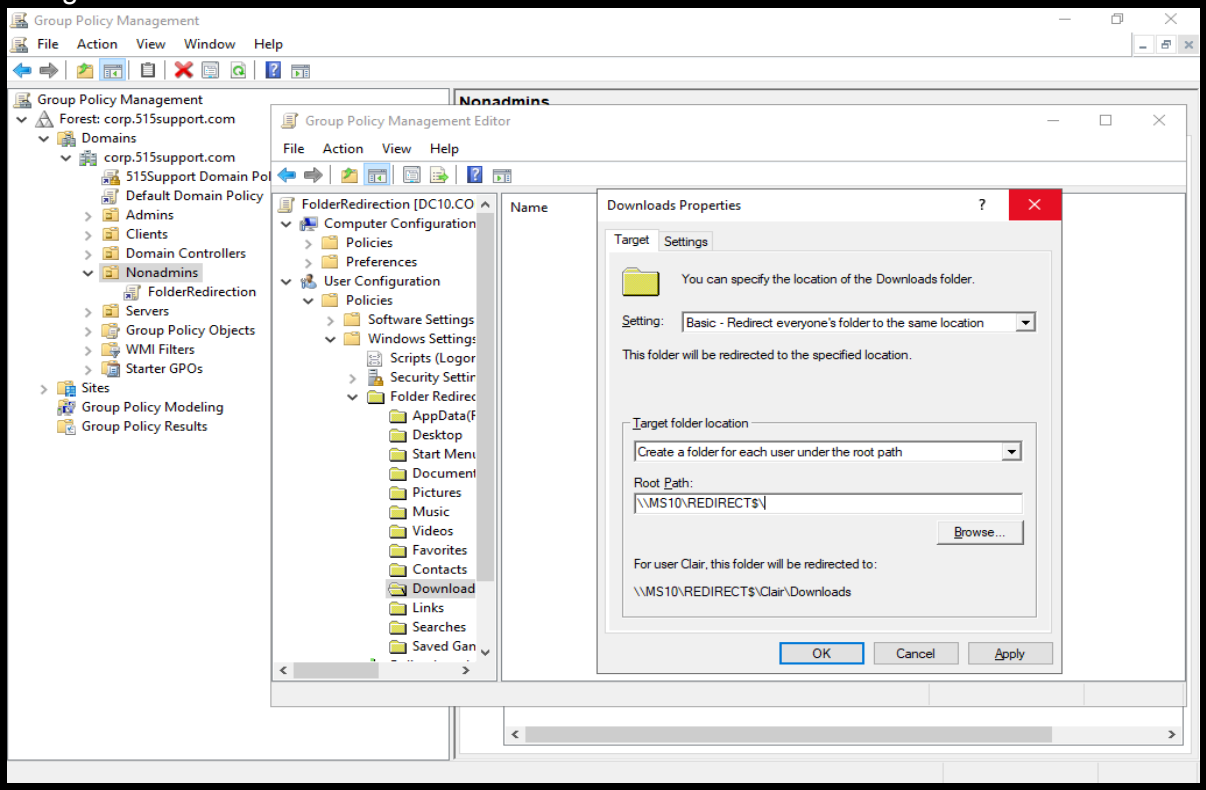
Description

Fields for file name and save as type are given below. Save and cancel button are at the bottom right.

15.3.10 Roaming Profiles and Folder Redirection

The home folders feature predates the design of modern Windows user profiles, and it can require extra user training to develop the habit of using it. Most users expect to save personal files in their profile folders: Documents, Pictures, Downloads, and so on. Users who work on more than one computer will have separate profiles on each computer, and the data files stored on the first computer will not be available on the second computer. This issue can be mitigated by implementing roaming profiles and/or folder redirection:

- **Roaming profile** copies the whole profile from a share at logon and copies the updated profile back at logoff. Roaming profiles are enabled by entering the path to a share in the **Profile** path box in the general form `\\SERVER\ROAMING$\%USERNAME%` . The main drawback is that if a profile contains a lot of large data files, there will be a big impact on network bandwidth and sign-in and sign-out performance will be slow.
- **Folder redirection** changes the target of a personal folder, such as the Documents folder, Pictures folder, or Start Menu folder, to a file share. The redirected folder is only available across the network. This can be used independently or in conjunction with roaming profiles. Folder redirection is configured via a GPO. Figure 1. Using GPO to redirect the Nonadmins OU Download folder to a network file server



Description

Nonadmins is selected from the group policy management menu on the left. The target tab is selected under the download properties dialog box. A filed for settings is at the top. A field for target folder location and root path is at the bottom. The browse button is on the bottom right. Ok, Cancel, and Apply buttons are at the bottom.

16.1.1 Windows Versions

Windows 10 and Windows 11, available in Home, Pro, and Enterprise editions, represent the currently supported versions of the Windows client OS. These editions target different market sectors, such as home users and corporate environments. Additionally, both versions have undergone several feature updates, introducing changes to the **desktop** style, user interface, new features, and support for new hardware types.

Windows also offers a Pro for Workstations edition, which is designed for advanced users, offering unique features like support for high-performance hardware, ReFS (Resilient File System), and advanced processing capabilities for demanding workloads.

32-bit Versus 64-bit

Each version and edition of Windows 10 was initially available in both 32-bit and 64-bit formats. A 32-bit CPU can only run 32-bit editions, while a 64-bit CPU can run either. All 32-bit Windows editions are limited to 4 GB of RAM, whereas 64-bit editions support more RAM, with limits varying by license.

64-bit Windows can run most 32-bit applications, though exceptions may exist, so it's best to check with the software vendor. However, 32-bit Windows cannot run 64-bit applications. Additionally, 64-bit Windows requires 64-bit hardware drivers to be digitally signed by Microsoft; without a 64-bit driver, the hardware won't function.

Note: Windows 10 version 2004 (released May 2020) and later, as well as Windows 11, are 64-bit only.

Desktop Styles

The Windows user interface (UI) revolves around the desktop, Start menu, taskbar, and notification area. While these elements remain consistent, Windows versions, editions (such as Home, Pro, Pro for Workstations, and Enterprise), and feature updates often bring changes. For example, the Start menu has seen various designs, including a full-screen version with live tiles. Update 1607 introduced dark theme support, with subsequent tweaks to theme configurations.

Windows 11 introduced a center-aligned taskbar and a redesigned Start menu, along with improved support for multiple desktops, allowing users to separate work and personal spaces.

N Versions

N versions of Microsoft Windows are specialized editions of the Home, Pro, Enterprise, and Education editions created to comply with European Union (EU) regulations, which require that consumers have the option to choose third-party media software rather than relying solely on Microsoft's built-in solutions. These versions are available in Europe and differ from standard Windows editions by excluding certain pre-installed multimedia applications, such as Windows Media Player, Music and Video apps, Voice Recorder, and Skype. This absence is intended to promote consumer choice and prevent Microsoft's dominance from limiting the software market.

While the core operating system remains unchanged, the lack of media applications can impact tasks involving audio or video playback or programs that rely on Windows Media Player. However, users can restore these features by downloading the Media Feature Pack from Microsoft, aligning N versions with the full feature set of non-N editions.

16.1.2 Windows Home Edition

Designed for domestic consumers and small office/home office (SOHO) use, Windows Home lacks unique features and has fewer capabilities than other editions, notably unable to join a Windows domain network.

Windows 11 Home: Mirrors the editions of Windows 10, requiring an internet connection and Microsoft account for setup. It includes gaming enhancements like Auto HDR and DirectStorage for faster load times, appealing to home users.

The main management tasks for Windows Home are configuring secure use by family members and simple file sharing of pictures, music, and video files in a workgroup network with other Windows computers and smart home devices, such as smart speakers and TVs. Many home computers are also configured to play games.

Windows Home Licensing

Windows Home offers two licensing models:

1. **Original Equipment Manufacturer (OEM) License**: This license comes pre-installed on a PC or laptop and is valid only for that device. The computer vendor provides support. Most new devices can upgrade to Windows 11.

2. **Retail License**: This license can be transferred between computers but can only be active on one device at a time. Microsoft provides support, and it includes upgrade rights to Windows 11.

Windows Home System Limitations

Windows Home supports multicore processing (up to 64 cores) and HyperThreading but does not support multiple CPUs. The 64-bit edition is limited to 128 GB of RAM.

16.1.3 Work and Education Features

Windows Editions for Work and Education

- **Windows Pro**: Designed for small and medium-sized businesses, available through OEM or retail licensing. It offers features like Group Policy, BitLocker, and Remote Desktop host for enhanced network administration. The Pro for Workstations edition supports more advanced hardware.

- **Windows Enterprise**: Tailored for large organizations, it includes advanced security, deployment, and management features such as AppLocker and Windows Defender Credential Guard. Available only through volume licensing agreements.
- **Windows Education/Pro Education**: These are versions of the Pro and Enterprise editions, customized for educational institutions. They include education-specific settings and features, with Pro Education based on Windows Pro and Education based on Windows Enterprise. Licensing is typically through academic volume agreements.

Domain Network Support

The primary distinction between Pro, Enterprise, and Education editions versus Windows Home is domain network support. These editions can join a domain, allowing centralized management of computers, user accounts, and policies via a Domain Controller (DC) server. This is essential for large organizations needing enhanced security and control.

Workgroup vs. Domain Networks

- Workgroup: Devices share files and resources but are managed independently.
- Domain: Devices connect to a centralized Domain Controller for consistent management and security policies.

Notable Features of Windows Pro, Enterprise, and Education Editions

- **Group Policy Editor (gpedit.msc)**: Configures and enforces OS and application settings across devices, ensuring consistent configurations. Not available in Windows Home.

- **BitLocker**: Provides disk encryption to protect data, even if a device is stolen. Not supported in Windows Home.
- **Remote Desktop Protocol** (RDP): Supports RDP as both client and server, enabling remote connections to and from computers. Windows Home only includes the RDP client software.

16.1.4 Windows Pro and Enterprise Editions

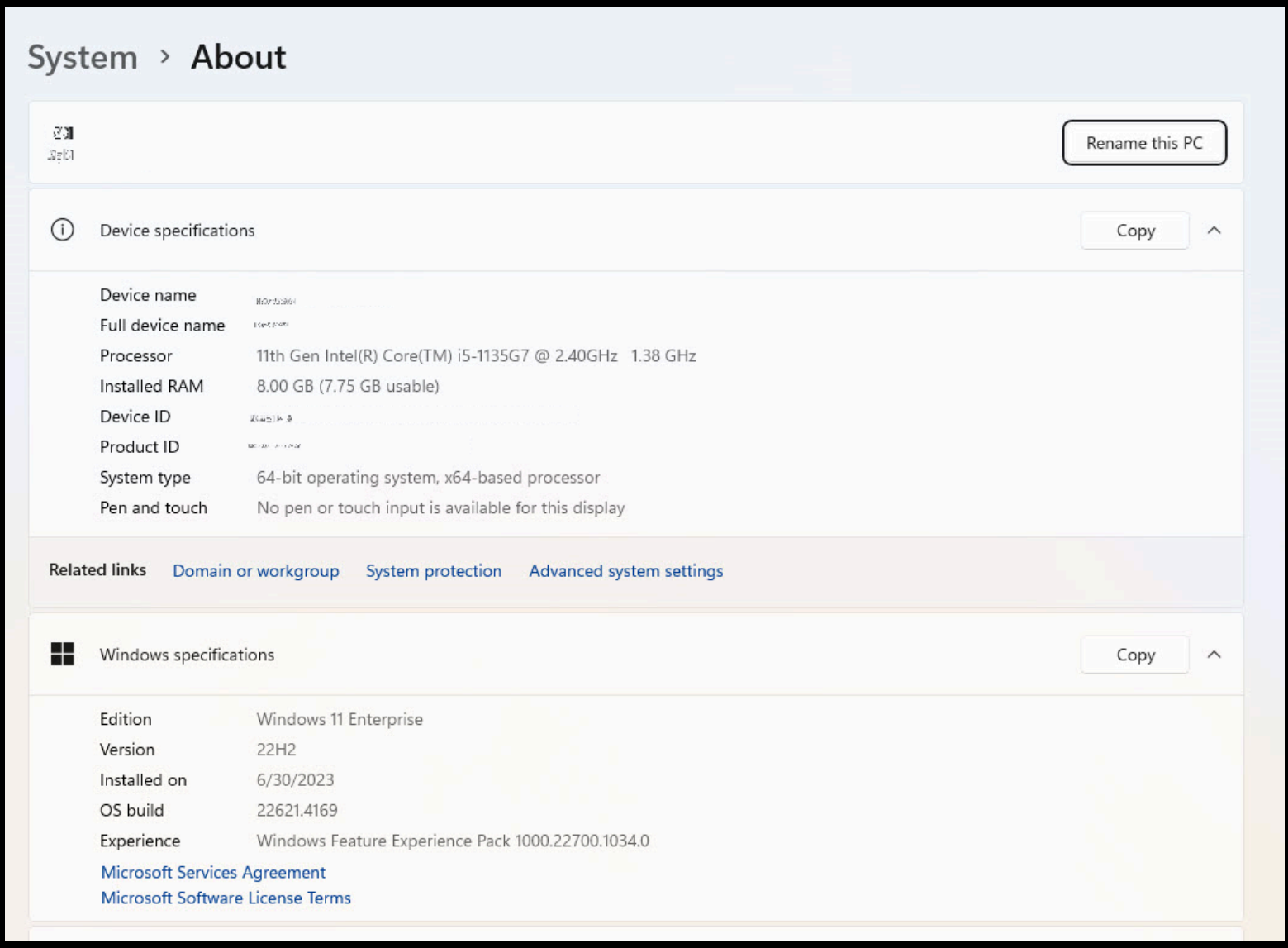
Windows Pro and Enterprise Editions:

- **Windows Pro**: Available as an OEM, retail/full packaged product (FPP), or through volume licensing, which offers discounts for bulk purchases and allows custom installation images for quick deployment. Windows Pro for Workstations includes all Pro features but supports more RAM and advanced hardware like persistent system RAM (NVDIMM).
- **Windows Enterprise and Education**: Only available via volume licensing. Enterprise includes exclusive features like DirectAccess virtual private networking technology, AppLocker software execution control, and the management and monitoring feature Microsoft Desktop Optimization Pack, which are not in the Pro edition.
- **Processors and RAM Requirements**:
    - Pro/Enterprise/Education editions support multiple processors:
        - Pro and Education: 2-way multiprocessing, up to 128 cores.
        - Pro for Workstations and Enterprise: 4-way multiprocessing, up to 256 cores.
    - RAM support:
        - Pro and Education: Up to 2 TB.
        - Pro for Workstations and Enterprise: Up to 6 TB.
    - As of version 22H2, Windows 11 Pro requires an Internet connection and a Microsoft account for personal use setup.

Note:

Visit microsoft.com/en-us/windows/business/compare-windows-11 for a complete list of feature differences.

Figure 1. Use the About settings page to report the edition that is installed



Description

The device specifications are device name, full device name, processor, installed RAM, Device ID, Product ID, System Type, and Pen and touch. The related links for Domain or workgroup, System protection, and Advanced system settings are given below. The windows specifications are edition, version, installed on, OS build, and experience. The links for Microsoft services agreements and Microsoft software license terms is given below.

16.1.5 Windows Upgrade Paths and Feature Updates

An in-place upgrade allows you to upgrade to a new Windows version while preserving applications, settings, and data, provided they are compatible.

Note:

Before upgrading, use a compatibility advisor (e.g., PC Health Check for Windows 11) to identify any incompatible software or hardware that may need to be updated or uninstalled.

Upgrade Paths

Supported **upgrade paths** for Windows 10 and Windows 11 are published by Microsoft:

- **Windows 10 to Windows 11** requires specific hardware features, including:
  - **TPM 2.0** (Trusted Platform Module): This is a security chip that ensures platform integrity by securing cryptographic keys and authenticating the system at startup. TPM 2.0 is mandatory for Windows 11, and the system will not install or upgrade without it.
  - **UEFI with Secure Boot**: UEFI (Unified Extensible Firmware Interface) is a modern firmware that replaces legacy BIOS and improves security. **Secure Boot** ensures that the device boots only with trusted software, preventing malicious code from loading. This is required for Windows 11 to enhance system security.
  - **Supported CPU**: Only specific processors listed by Microsoft are compatible with Windows 11. Devices without supported CPUs will not be eligible for upgrade.

Edition Considerations:

- You can upgrade within the same or higher edition (e.g., Windows 10 Home to Windows 11 Home or Pro), but you cannot upgrade from Home to Enterprise directly.
- Downgrades (e.g., Pro to Home) only preserve personal files, not apps or settings. Downgrading from Enterprise is not supported.

Feature Updates

- As of October 14, 2025, **Windows 10** is no longer supported by Microsoft, which means there are no free security updates, technical assistance, or feature updates. To ensure protection, users should upgrade to Windows 11 if the hardware is compatible. Users can also purchase Extended Security Updates (ESU) program to receive security updates for the year.
- **Windows 11** will follow an annual feature update cycle (e.g., 23H2), with each release bringing new features and improvements.

Windows 11 receive **quality updates** regularly, addressing security vulnerabilities and bug fixes. While these updates generally pose fewer compatibility risks, they can occasionally cause issues with certain hardware or software.

16.2 OS Installations and Upgrades

You need to implement a strategy for upgrading the clinic's computers to the latest Windows editions, ensuring minimal disruption to daily operations and maintaining patient data confidentiality. This involves choosing between clean installations and in-place upgrades, managing hardware compatibility, and utilizing unattended installations for efficiency.

Core 2 Exam Objectives Covered

- 1.2 Given a scenario, perform OS installations and upgrades in a diverse OS environment.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the main differences between a clean install and an in-place upgrade, and when would you choose one over the other?
- How do you verify hardware compatibility before performing an OS upgrade, and what tools can assist in this process?
- What is the role of an answer file in unattended installations, and how does it streamline the deployment process?
- How does the GUID Partition Table (GPT) differ from the Master Boot Record (MBR) in terms of partition support and boot method requirements?
- What are the advantages of using network-based deployment for OS installations in large organizations, and how does it differ from using physical media?
- How does a multiboot installation work, and what are the key considerations for setting up multiple operating systems on a single computer?

16.2.1 Installation and Upgrade Considerations

An operating system (OS) installation involves copying files from the installation media to a partition on the computer's fixed disk. There are a few installation types, each with unique planning considerations.

Clean Install or In-Place Upgrade

An attended installation requires the installer to input configuration information in response to prompts from a setup program. There are two main types:

- **Clean Install**: This involves installing the OS on a new computer or completely replacing the existing OS on an old one by repartitioning and reformatting the disk. All existing user data and settings are deleted.
- **In-Place Upgrade**: This involves running the setup from an existing OS version, preserving third-party applications, user settings, and data files for use in the new version.

A clean install is generally considered more reliable than an upgrade. In-place upgrades are typically designed for home users.

You can only upgrade within the same type of operating system; for example, you cannot upgrade from Windows to Linux.

Upgrade Considerations

1. **Check Hardware Compatibility**: Ensure the computer's CPU, chipset, and RAM meet the OS requirements. Modern PC operating systems often require a 64-bit CPU and may have higher RAM requirements than older versions.
2. **Check Application and Driver Support**: Most upgrades aim to support applications and drivers from older versions. Before an in-place upgrade, uninstall any incompatible software or hardware. If an app or driver isn't compatible, check if the vendor offers a new version that can be reinstalled post-upgrade. Incompatible apps and devices must be replaced.

   Note: Microsoft provides a Windows Logo'd Product List (LPL) catalog, previously called the Hardware Compatibility List (HCL), listing tested devices and drivers. If a device hasn't passed Windows logo testing, check the vendor's website for available drivers.

   Note: Automated Upgrade Advisor software can help determine if existing hardware and software are compatible with a new Windows version. This tool might be included with the setup program or available on the vendor's website.

3. **Backup Files and User Preferences**: For a clean install, use a backup to restore data and settings after setup. For an in-place upgrade, a backup is crucial in case of upgrade issues requiring data recovery.

4. **Obtain Third-Party Drivers**: The OS setup media might lack drivers for certain hardware, such as RAID controllers. Without the controller driver, the setup can't use the RAID volume. Ensure drivers for Ethernet or Wi-Fi adapters are available.

Note:

Unsupported hardware or software can cause issues during an in-place upgrade and should be uninstalled. Obtain the latest drivers from the vendor's website, as Windows setup media may not have up-to-date or comprehensive drivers. Store these drivers on a USB drive or network location for efficient hardware updates.

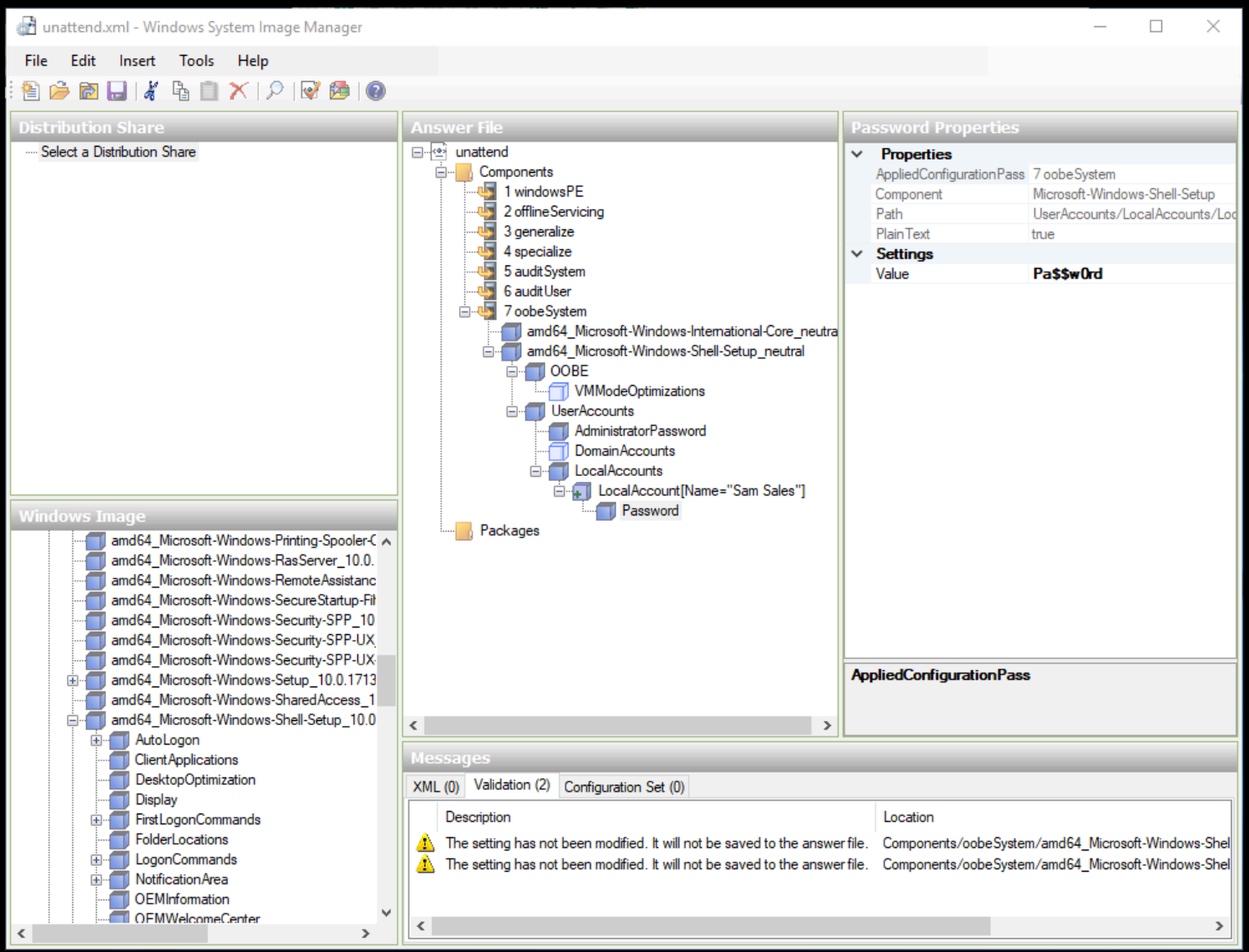
Feature Updates

Windows 10 and 11 receive feature updates to introduce changes to the desktop environment and bundled apps via Windows Update. While these updates rarely require new hardware, it's best to verify compatibility and back up data before applying them. Additionally, each version follows a product life cycle, with feature updates supported for a limited time, after which users must upgrade to a newer version to continue receiving security updates and support.

16.2.2 Unattended Installations

Attended installations are time-consuming, requiring the installer to monitor the setup and input information. Despite improvements in the setup process, this method remains labor-intensive. For large deployments, whether simultaneous or over a period of months, fully or partially **unattended installations** are more efficient.

Figure 1. The Windows System Image Manager is used to configure answer files



Description

The screen lists the distribution share, answer file, password properties, windows image, and messages.

An unattended installation uses a script or configuration file, known as an answer file in Windows, to automate choices and settings during setup. Often, unattended installations utilize **image deployment**, where an image—a clone of an existing installation—is stored in a single file. This image can include the base OS, configuration settings, service packs, updates, and application software. It can be stored on DVD, USB media, or accessed over a network. Image deployment ensures machines have a consistent set of software and configuration options.

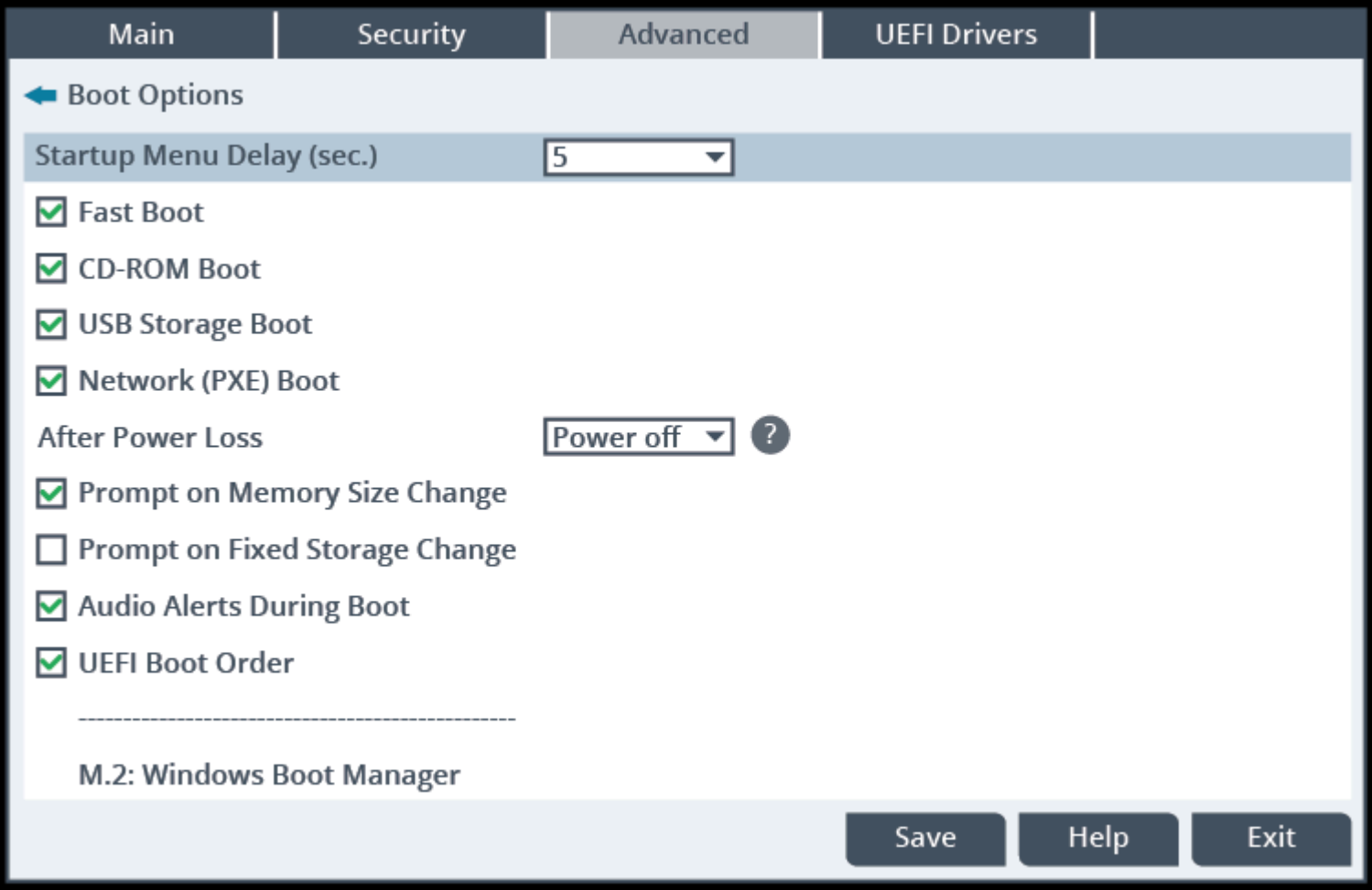
Remote network installation is a key aspect of unattended installations, allowing images to be deployed over a network. This method enables IT administrators to install or update multiple machines simultaneously without physical access, ensuring consistency in software and configuration across all devices. Network-based deployment is particularly advantageous for large organizations, as it reduces the need for physical media and streamlines the installation process.

Remote **zero-touch deployment** takes this a step further by enabling devices to be set up and configured automatically without any user intervention. This approach leverages cloud-based services to deploy configurations and applications as soon as the device connects to the internet. Zero-touch deployment is ideal for organizations looking to minimize IT involvement and provide a seamless setup experience for end-users, ensuring devices are ready to use right out of the box.

16.2.3 Boot Devices

The installation **boot-method-os-setup** method refers to how the setup program, answer file (if used), and OS files or system image are loaded onto the target PC. Accessing the computer's firmware setup program may be necessary to ensure the correct boot device is enabled and prioritized.

Figure 1. Configuring boot devices and priority in a computer's firmware setup program



Description

The startup menu delay (sec) lists the checkboxes for Fast Boot, CD-ROM Boot, USB Storage Boot, Network (PXE) Boot. After power loss: Power loss. Below are check boxes for Prompt on Memory Size Change, Prompt on Fixed Storage Change, Audio Alerts During Boot, and U E F I Boot Order. Save, help, and exit buttons are at the bottom.

Optical Media

Historically, attended installations and upgrades were performed by booting from optical media (CD-ROM or DVD). The optical drive must be set as the priority boot device.

USB, External Drives, Flash Drives, and Hot-Swappable Drives

With fewer computers featuring optical drives, USB flash drives, external drives, and hot-swappable drives have become more common for installations. Disc-based installs can quickly become outdated, requiring additional time for updates and drivers. Slipstreamed media, containing all necessary patches and drivers, can be created on CD-ROM, DVD, USB drives, or even external hot-swappable drives. When using these drives, set the USB-connected or external device as the priority boot option. Hot-swappable drives add the convenience of connecting or disconnecting storage devices without shutting down the system, further enhancing flexibility during installation or data transfer processes.

Note:

Microsoft's Media Creation Tool can create installation media on a bootable USB drive, external drive, or generate an ISO file for a DVD, making it easier to perform installations or updates.

Network Boot

Network booting involves connecting to a shared folder with installation files, which may be slipstreamed or use image deployment. The target PC needs a partition for temporary files and a way to boot without a formatted local drive. Most computers support this via **preboot execution environment** (PXE)-compliant firmware and network adapters. The client uses DHCP (Dynamic Host Configuration Protocol) server information to locate a server with installation files and initiate setup.

Internet-Based Boot

Computers supporting network boot can also be configured for Internet-based setup. The local network's DHCP server must provide the DNS name of the installation server. Typically, setup installers connect to the Internet to download updates and optional packages.

Note:

OS installations and deployments are often performed on virtual machines in cloud environments, using orchestration and automation tools.

Internal Hard Drive (Partition)

After OS installation, set the internal hard drive as the default (highest priority) boot device and disable others to prevent booting from setup media again. This also secures the system against unauthorized OS installations if firmware access is restricted. Internal partitions may also serve as recovery partitions, as discussed later.

Multiboot

A multiboot installation allows multiple operating systems to coexist on a single computer, enabling users to select which OS to boot into during startup. This setup is useful for testing software across different environments or running specific applications that are exclusive to certain operating systems. Each OS is installed on its own partition, with a boot loader like GRUB or Windows Boot Manager managing the boot process and presenting a menu for OS selection at startup.

Important considerations include proper partitioning to ensure each OS has sufficient space, configuring the boot loader correctly to recognize all installed systems, and ensuring driver compatibility across operating systems. Setting up a shared partition formatted with a universal file system (e.g., FAT32) allows for easy data access between OSes. Regular backups of data and system configurations are recommended to prevent data loss during partitioning or installation.

Note:

When installing both Windows and Linux, install Windows first as it overwrites the boot loader, whereas Linux's GRUB can detect other OS, and for multiple Windows versions, install the older version first to prevent boot configuration issues.

16.2.4 Disk Configuration

Mass storage devices like HDDs or SSDs require partitioning and formatting before use. Partition and file system options can be selected during setup, configured in an answer file, or included in a cloned image. A partition is a logically separate storage area, and at least one must be created before formatting to establish a file system. Partition information is stored on the disk as either Master Boot Record (MBR) or GUID Partition Table (GPT).

MBR-Style Partitioning

The **master boot record (MBR)** partition style stores a partition table in the first 512-byte sector of the disk, allowing up to four primary partitions, any one of which can be marked as active and bootable. This supports multiboot systems and separate areas for data storage or databases, with each partition formatted differently if needed. Partitions can be used to create separate areas for user data, log files, or databases, each formatted using a different file system.

Note:

If more than four partitions are needed and GPT isn't an option, one partition can be extended into multiple logical drives, though these cannot be made active.

Each primary partition starts with a boot sector, or Partition Boot Record (PBR), which points to the OS boot loader when marked active. In Windows, this is known as the system partition or system reserve. The boot partition, containing Windows OS files, can be on a logical drive in an extended partition and doesn't need to be the same as the system drive. MBR requires the legacy BIOS boot method; a UEFI method will not recognize the disk as a boot drive.

GPT-Style Partitioning

The **GUID Partition Table (GPT)** is a more up-to-date partitioning scheme that overcomes MBR's limitations, supporting more than four primary partitions (up to 128 in Windows) and larger partitions (over 2 TB). It includes a backup of partition entries and a protective MBR for compatibility with non-GPT systems. GPT requires the UEFI boot method; BIOS will not recognize it as a boot device.

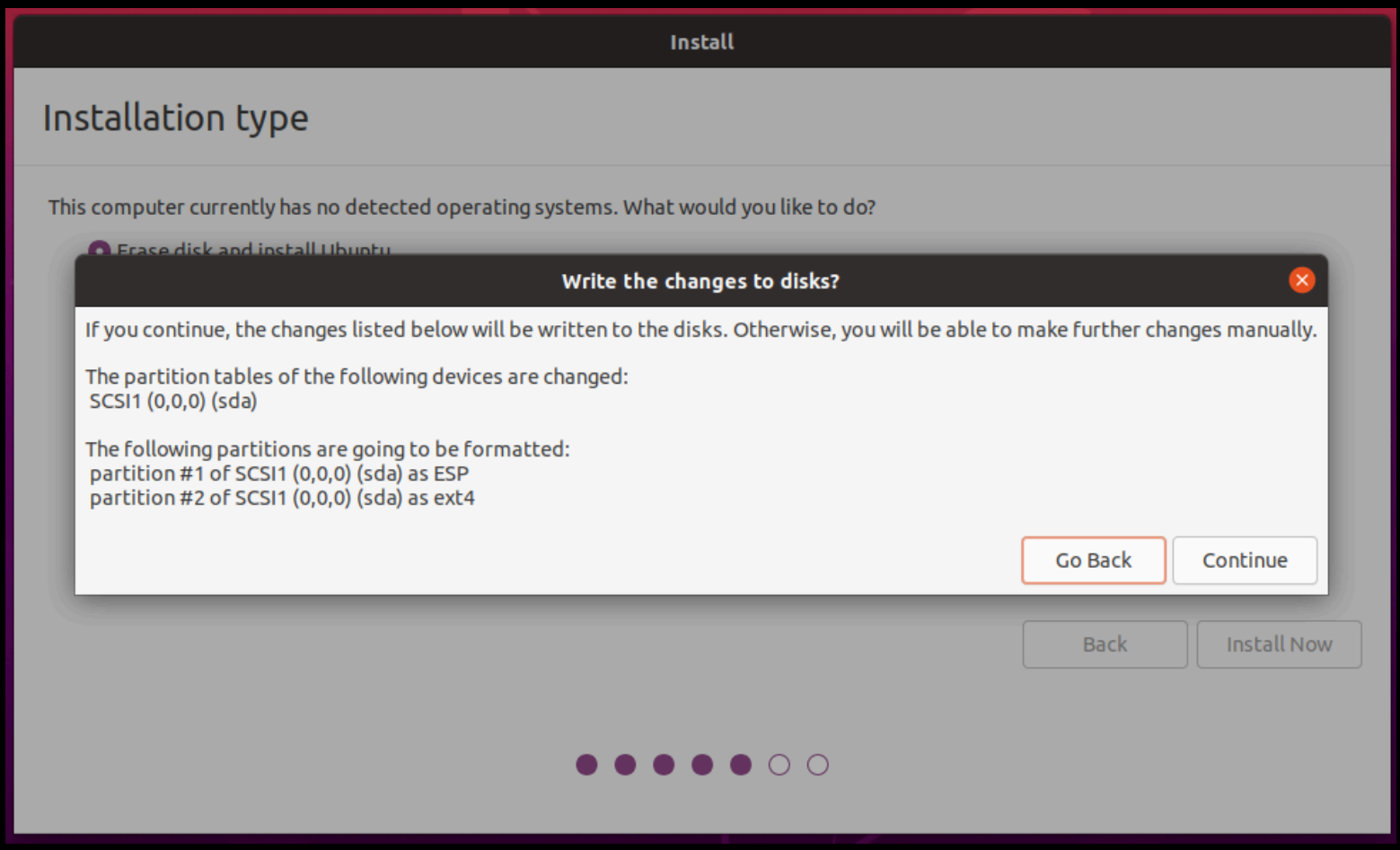
Note:

The mbr2gpt utility (learn.microsoft.com/en-us/windows/deployment/mbr-to-gpt) in Windows 10 version 1703 and later can convert MBR to GPT without data loss, but a backup is recommended. After conversion, switch the firmware to UEFI boot mode. Third-party utilities can also perform this conversion.

Drive Format

An OS must be installed on a partition with a compatible file system: NTFS for Windows, APFS for macOS, and ext3/ext4 (or a variety of others) for Linux. During installation, partitioning and formatting are guided by the setup program.

Figure 1. Default choices made by the guided setup program for Ubuntu Linux



Description

The screen reads, Write the changes to disks? If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually. The partition tables of the following devices are changed: S C S I 1 (0, 0, 0) (sda). The following partitions are going to be formatted. Partition 1 of S C S I 1 (0, 0, 0) (sda) as E S P Partition 2 of S C S I 1 (0, 0, 0) (sda) as ext4 Go back and continue buttons are at the bottom.

16.2.5 Repair Installation

If a computer won't boot or has persistent issues like slow performance without a known cause, a repair installation may be necessary.

Recovery Partition

A factory **recovery partition**, created by OEMs on the **internal fixed drive**, restores the OS to its original state. If the main installation fails to boot, the system can boot from this partition by pressing a key during startup (often F11 or CTRL+F11). This process resets the system to factory settings, erasing user data, settings, and third-party applications, so backups should be made beforehand.

Be aware that the recovery tool only works with the original hard disk and doesn't include updates applied after shipping. It also occupies significant disk space, reducing available capacity.

Reset Windows

Windows offers refresh and reset options for repair. The refresh option reinstalls system files and resets most settings to default, while preserving user personalization, data files, and Windows Store apps, but it removes desktop applications. A full reset deletes the OS, apps, settings, and data, preparing the system for a fresh OS installation.

17.1 Linux Features

Core 2 Exam Objectives Covered

- 1.9 Identify common features and tools of the Linux client/desktop operating system.

TechEd Academy's computer science lab runs on various Linux distributions to support programming and development courses. Recently, students have reported issues with accessing certain applications and navigating the file system. Your task is to troubleshoot these issues, ensuring that the Linux environment is user-friendly and fully functional for educational purposes.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the differences between interactive and non-interactive shell usage, and how can you switch between different shell environments?
- How can you configure multiple desktops in a Linux environment to optimize workspace for different tasks?
- How do you use the cd command to navigate between directories, and what is the significance of the root directory in Linux?
- How do you mount a filesystem in Linux, and what role does the /etc/fstab file play in this process?
- How do you use the cp and mv commands to manage files, and what precautions should be taken when using the rm command?

17.1.1 Shells, Terminals, and Consoles

So far in this course, you worked mostly with the Microsoft Windows operating system. A CompTIA A+ technician should be capable of supporting diverse OS environments. The various operating systems you might encounter use different interfaces and command syntax, but the functionality of those tools is common across all types of systems.

The kernel is the core software component of an operating system, managing hardware and enabling communication between software and hardware. A Linux distribution (distro) combines the Linux kernel with a package manager, software repository, and customizable shells, utilities, and applications. Distros may offer community-supported or commercial licensing and support options.

Bootloaders

Before the operating system loads, a **bootloader** initializes the system. It is responsible for loading the kernel into memory and starting the operating system. Bootloaders support multi-boot configurations, allowing multiple operating systems on the same device. Common bootloaders for Linux include GRUB (GRand Unified Bootloader) and LILO (Linux Loader).

Shells and Terminals

A **shell** provides a command-line environment for users to interact with the OS and applications. Popular Linux shells include **bash**, zsh, and ksh (Korn shell), each offering features like command history, tab completion, spelling correction, and syntax highlighting.

Many Linux distros operate without a desktop environment, launching a **terminal** interface connected to the default shell command interpreter during boot. The terminal and shell communicate via a teletype (tty) device, handling text input and output through separate streams:

- **stdin (0)**: Captures keyboard input for processing by the shell's command interpreter.
- **stdout (1)**: Displays data generated by the shell from the tty device on the terminal.
- **stderr (2)**: Outputs error information.

Using a terminal interactively involves direct command input, while non-interactive use involves executing commands from a script file.

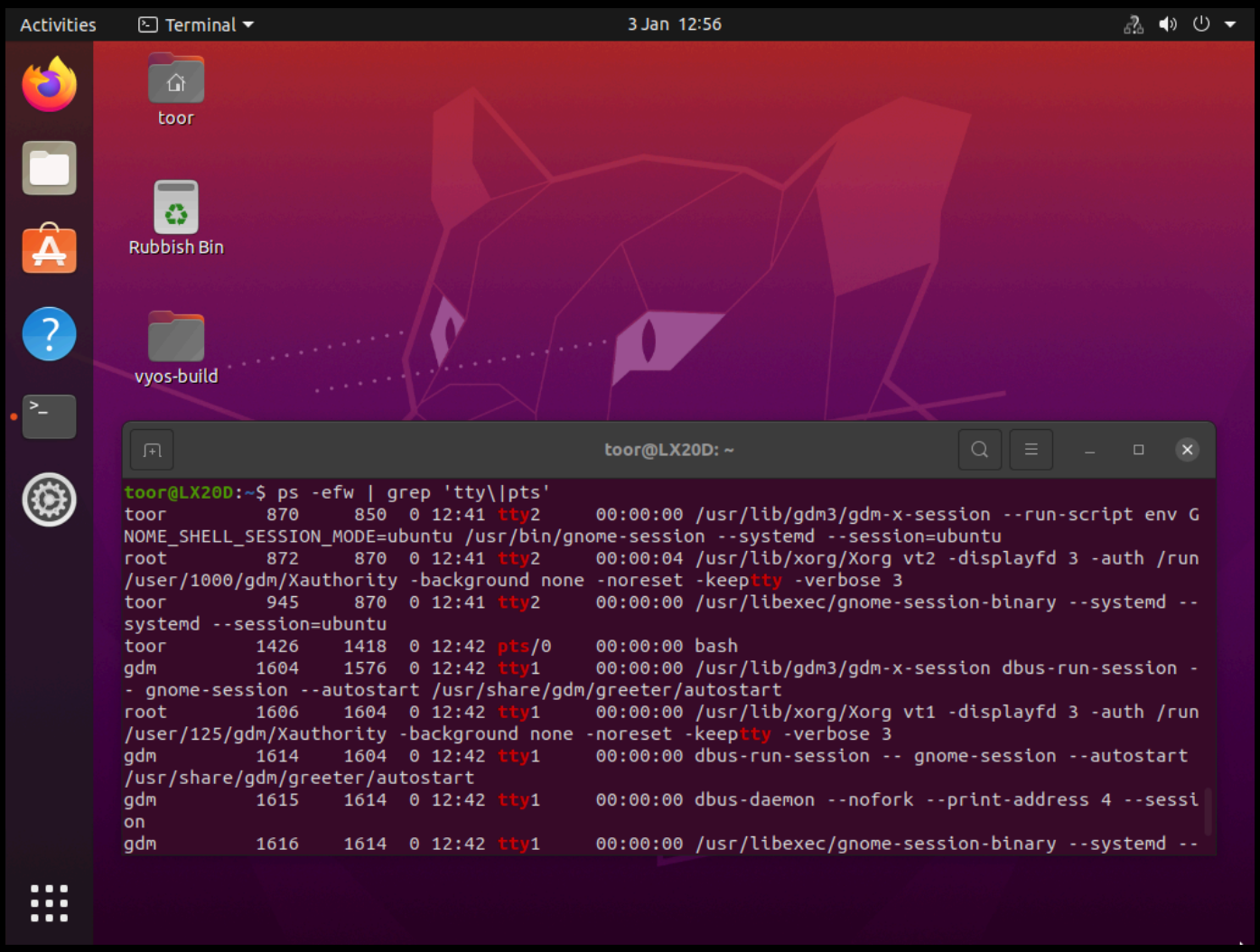
Desktop Environments

Linux distros intended for client PCs usually start with a graphical desktop environment. This environment is powered by Xorg, an open-source implementation of the X Window System. Within Xorg, users can launch various desktop programs, such as Gnome (GNU Object Model Environment), KDE (K Desktop Environment), Cinnamon, and Xfce.

Note:

GNU stands for "GNU is Not UNIX," a recursive acronym. Many non-kernel software components developed under the GNU license replace proprietary UNIX equivalents and are compatible with Linux.

Figure 1. Ubuntu 20 running the GNOME desktop with a virtual terminal window open to run commands in the Bash command environment



Description

The toor, rubbish bin, and vyos-build are displayed on the screen. Few lines of code is under the head toor at the rate LX20D.

Within a desktop environment, you can open a terminal emulator to use the default command shell (or an alternative shell if needed). The terminal emulator runs within a window on the desktop. The terminal emulator connects to the shell via a pseudoterminal (pty/pts) interface.

Console Switching

In systems with a graphical environment, the X server runs on a virtual tty console, typically tty1. Users can switch between consoles using **CTRL+ALT+Fx** keys, with each console supporting different login prompts and shells.

17.1.2 Command Interface

Linux **commands** follow a standard format:

- **Command**: The first "word" is the command, which can be a full or relative path to an executable, or simply the name of an executable located in a directory specified by the PATH environment variable. The command is recognized up to the first space character.
- **Options**: Options (or switches) modify the command's behavior. They can be single letters (preceded by a single hyphen) or words (preceded by a double hyphen). The order of options is generally flexible.
- **Arguments**: Arguments are values, such as file names, that the command operates on. They must be provided in the correct order according to the command's syntax.
- **Pipes**: Use a pipe (|) to redirect the output of one command to another command.
- **Multiple Commands:** Use a semicolon (;) to execute multiple commands sequentially on a single line. Press ENTER to run the commands in order.

Case Sensitivity

In Linux, commands, parameters, and file and directory names are all case-sensitive. For instance, ls -l file.data and ls -L File.data will yield different results. Typing a command name with incorrect capitalization will result in an error message.

Help System

To view a Linux command's function and syntax, use the --help option. Since the help output can be lengthy, it's common to pipe it to the more command for viewing one page at a time, e.g.,ls --help | more . Alternatively, use the man command to access detailed manual pages for any command, such as man man for the manual on the man command itself.

Note: Terminal emulators often support TAB completion to assist with entering commands. Use the UP and DOWN arrow keys to navigate through command history. In some terminals, you can scroll through output using SHIFT+PAGEUP/PAGEDOWN or CTRL+SHIFT+UPARROW/DOWNARROW.

Text Editors

Most Linux files are in plain text format and can be easily edited. There are many text editors available. For those familiar with Windows, the **nano** editor is a simple option. To open or create a file, use nano filepath , or nano -l filepath to display line numbers. Navigate with the cursor keys and use **CTRL** + key shortcuts for operations, like **CTRL+O** to save changes and **CTRL+X** to exit.

Many administrators prefer editors like vi or vim, which have two modes: command and insert. In command mode, you perform file operations like saving and closing. To enter text, switch to insert mode with keys like i (insert at cursor), a

(append after cursor), A (append at line end), or o (insert new line below). Press **ESC** to return to command mode. To display line numbers, type:set number in command mode. Save with :w , save and quit with :wq , or quit without saving with :q! .

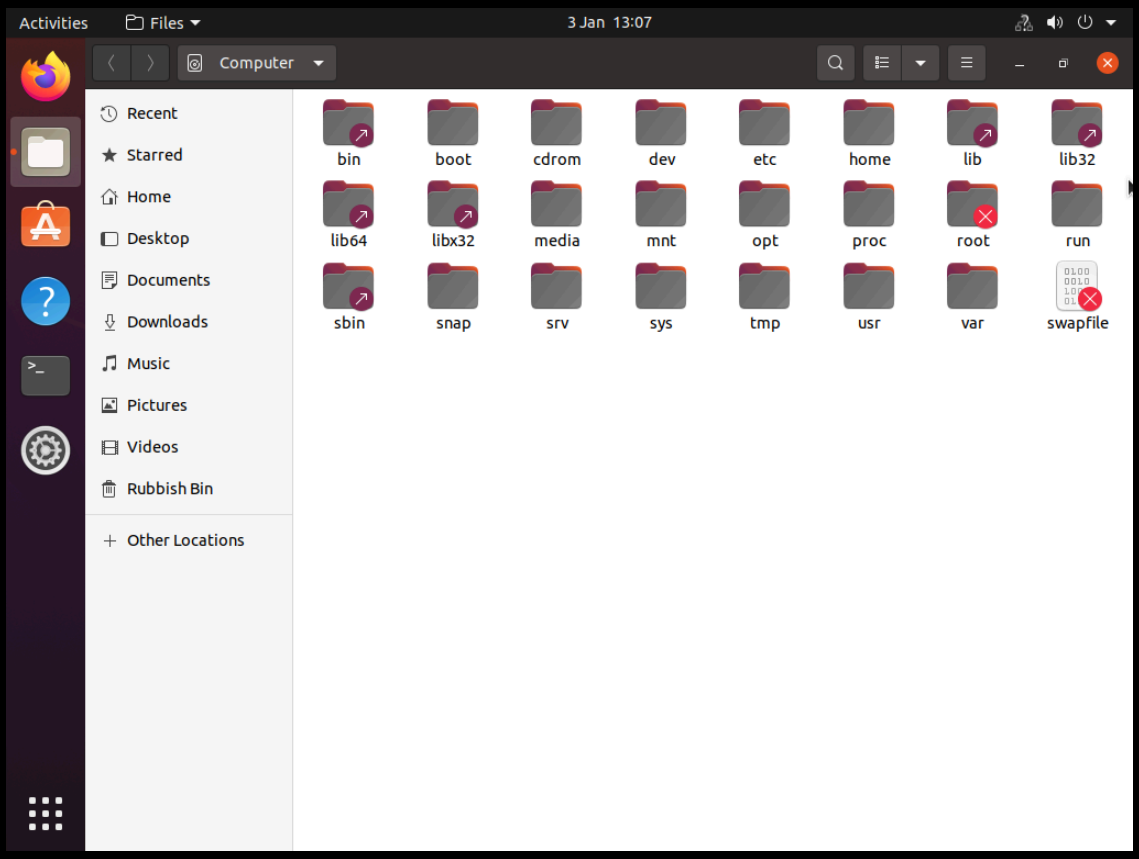
17.1.3 Navigation Commands

In Linux, everything is represented as a file within a unified file system. The first fixed disk is typically /dev/sda , while additional devices, like a USB drive, appear as /dev/sdb .

During boot, Linux loads the system kernel and a virtual file system into a RAM drive. The unified file system then locates the persistent root partition on the storage device and loads the disk's file system.

Unlike Windows, Linux doesn't use drive letters like C: or D:. The file system begins at the root, represented d by */*. From the root, directories and subdirectories can be created to organize files. The File System Hierarchy Standard (FHS) dictates directory naming and file placement. For example, /home contains user subdirectories for personal data, and /etc directory contains configuration files.

Figure 1. Viewing the root directory and file system hierarchy standard (FHS) subdirectories in Ubuntu Linux



Description

A menu is on the left. The system directories are listed as bin, boot, cdrom, dev, etc, home, lib, lib32, lib64, libx32, media, mnt, opt, proc, root, run, sbin, snap, srv, sys, tmp, usr, var, and swapfile.

Key commands for navigating the Linux file system include pwd,cd,ls, and cat.

pwd Command

The **pwd command** displays ("prints") the current working directory on the terminal, unless the standard output (stdout) is redirected. The working directory is important because commands without specified paths default to it. In some distributions, the prompt shows your current directory or a tilde (~) if you're in your home directory.

cd Command

The **cd command** changes the working directory. Here are some common uses:

- To change to an absolute path, such as /etc , use: cd /etc . This works from any current directory.
- To change to a subdirectory named **documents**, use a relative path: cd documents . The documents directory must be within the current directory.
- To move to the parent directory of your current location, use: cd .. .



ls Command

The **ls command** lists directory contents, similar to the dir command in Windows. Common options include -l for a detailed list and -a to show all files, including hidden or system files. For example, ls -la /etc displays all contents of the /etc directory in detail.

cat Command

The **cat command** displays the contents of files specified through arguments. Use the -n option to add line numbers to the output.

To control scrolling, you can pipe the output to a pager like more or less (e.g.,cat file | more).

The cat command can also be used to combine (concatenate) multiple files into one or display them sequentially. For example:

- To concatenate and display two files: cat file1 file2
- To concatenate and redirect the output to a new file:
    - Overwrite the destination file: cat file1 file2 > destination
    - Append to the destination file: cat file1 file2 >> destination

These redirection operators can be used with other commands as well.

17.1.4 Search Commands

Linux supports very fast and accurate file system informational search commands.

find Command

The **find command** searches for files using the syntax find path expression , where path is the starting directory and expression specifies the search criteria. Options include -name , -size , -user (owner), and -perm (permissions). The -type option identifies file types, distinguishing between files, directories, block devices, network sockets, symbolic links, and named pipes, unlike Windows, which uses file extensions.

grep Command

The **grep command** (Globally search a Regular Expression and Print) searches and filters file contents, displaying lines that match a search string. The search string can be a simple text (literal) or a pattern using regular expressions (regex).

grep is particularly useful for searching long files like system logs. For example, grep -i "uid=1003" /var/log/messages displays lines in the system log containing "uid=1003", ignoring case with the -i option.



grep can also search file names by piping a directory list as input. For instance, ls -l | grep audit lists files in the current directory with "audit" in their names.



Note:

You can pipe output from other commands to grep to apply various filters.

Metacharacters and Escaping

In Linux, *escaping* means using a special character (usually a backslash \) to indicate that the following character should be treated as a literal rather than interpreted in its usual, special way. This is necessary when dealing with *metacharacters*, which have specific meanings in the shell. For example, the asterisk (*) is a metacharacter that matches any number of characters. To search for a literal asterisk, you must escape it. Similarly, expressions with spaces need escaping.

There are three ways to escape strings:

- **Backslash (\):** Escapes the next character only. For example,* treats * as a literal, and \\ treats \ as a literal.
- **Single Quotes (' '):** Provide strong escaping, treating everything inside as literal. For example,'$(pwd) * example one' is interpreted as: $(pwd) * example one.

- **Double Quotes (" "):** Provide weak escaping, allowing variable expansion and command substitution. For example,"$(pwd) * example one" expands to include the output of the pwd command, resulting in: /home/david * example one.

17.1.5 Filesystem Management

Filesystem management involves organizing, maintaining, and accessing data stored on disk drives. It includes tasks such as mounting filesystems, checking and repairing them, and configuring their behavior.

Linux uses a hierarchical directory structure starting at the root (/). Directories and subdirectories organize files, and each storage device or partition can have its own filesystem.

Key filesystem management tools include:

- **Mounting**: To access a filesystem, it must be mounted, which means attaching it to a directory in the existing filesystem hierarchy. The **mount command** is used for this purpose. For example, mount /dev/sda1 /mnt mounts the filesystem on /dev/sda1 to the /mnt directory.
- **/etc/fstab**: This file contains static information about filesystems. It defines how and where filesystems should be mounted automatically at boot time. Each line in /etc/fstab specifies a filesystem, its mount point, filesystem type, and mount options. For example, a typical entry might look like this: /dev/sda1 / ext4 defaults 0 1 This entry mounts the /dev/sda1 partition as the root filesystem (/) using the ext4 filesystem type with default options.
- **fsck (Filesystem Check)**: This utility checks and repairs filesystems. It's used to ensure filesystem integrity, especially after an improper shutdown or disk corruption. The command fsck is typically run with the filesystem's device name, like fsck /dev/sda1. It scans the filesystem for errors and attempts to fix them. It's often run automatically at boot if the system detects filesystem issues.

17.1.6 File Management Commands

File management commands are used to move, copy, and delete data.

cp Command

The cp command is used to create a copy of files either in the same or different directory with the same or different name. For example:

- Copy file1.txt in the current working directory to a new file called file1.old in the same directory: cp file1.txt file1.old
- Copy the file hosts from the directory /etc into the directory /tmp , keeping the file name the same: cp /etc/hosts /tmp
- Copy all files beginning with the name message from the /var/log directory into /home/david . The -v option displays the files copied: cp -v /var/log/message* /home/David

mv Command

The mv command is used to either move files from one directory to another or rename a file. For example:

- Move the file data.txt from the /home/david directory to the /tmp directory, keeping the file name the same: mv /home/david/data.txt /tmp
- Move and rename the file alarm.dat in the current directory to alarm.bak in /tmp : mv alarm.dat /tmp/alarm.bak
- Rename the file app1.dat in the /var/log folder to app1.old : mv /var/log/app1.dat /var/log/app1.old

The **cp command** with the -r (or --recursive) option is also used to copy directories. For example:

- Copy the directory project from the /home/david directory to the /tmp directory: cp -r /home/david/project /tmp
- Copy and rename the directory backup in the current directory to backup_old in /tmp: cp -r backup /tmp/backup_old

rm Command

The **rm command** can be used to delete files. It can also be used with the -r option to delete directories. For example:

- Remove the single file data.old from the current working directory: rm data.old
- Remove all files ending in .bak from the /var/log directory: rm /var/log/*.bak
- Remove the contents of the entire directory tree underneath the folder /home/david/data : rm -r /home/david/data

Note:

Use -r with caution, as Linux commands do not prompt for confirmation. There is no opportunity to cancel.

df and du Commands

The df/du commands check free space and report usage by the device, directory, or file specified as the argument:

- df ("disk free") enables you to view the device's free space, file system, total size, space used, percentage value of space used, and mount point.
- du ("disk usage") displays how a device is used, including the size of directory trees and files within it.

17.1.8 User Account Management

In Linux, the **root account**, or superuser, has full administrative privileges and can perform any action on the system. It should be used only when absolutely necessary. During setup, most Linux distributions prompt you to create a regular user account for daily tasks. Instead of staying logged in as root, you can use special commands to temporarily elevate your privileges when needed.

su Command

The **su (switch user) command** switches to the specified user's account using su username. To switch to the root account, omit the username. You'll be prompted for the target account's password before switching. Using su without options retains the original user's profile and home directory. Using su - switches to the root account and starts a new shell with root's environment, which is a better practice.

sudo Command

The **sudo (superuser do) command** allows users listed in the /etc/sudoers file to run specified commands with superuser privileges. In distributions using sudo, this setup is typically handled during installation. Users enter sudo followed by the desired command and may need to confirm their password if it hasn't been cached recently.

Note: The main advantage of sudo over su is that the root password doesn't need to be shared among multiple administrators.

User Management Commands

User settings are stored in the /etc/passwd file, while group settings are in the /etc/group file. User passwords are typically stored as encrypted hashes in the /etc/shadow file, along with other password settings like age and expiration date. Use the useradd,usermod, and userdel commands to add, modify, and delete user information. The passwd command is used to change passwords.

Group Management Commands

Each user account can be assigned to groups to manage file permissions. Use the groupadd, groupmod, and groupdel commands to manage group memberships. A user can belong to multiple groups but has only one effective group ID at a time, listed in /etc/passwd. The effective group ID can be changed using the newgrp command.

17.1.9 File Permissions Commands

Each file in Linux has a set of permissions that determine user access levels. The permissions system includes three rights:

- **Read (r)**: Allows viewing the contents of a file or directory.
- **Write (w)**: Allows modifying or deleting the object. For directories, it permits adding, deleting, or renaming files within.
- **Execute (x)**: Allows running an executable file or script. For directories, it enables actions like changing focus to the directory and accessing or searching items within it.

Permissions are set for the owner, the group, and other users ("the world"). In **symbolic mode** notation, permissions are shown as allowed (r, w, x) or denied (-).

For example, using ls -l for a long directory listing:

- drwxr-xr-x 2 bobby admins Desktop : The owner (bobby) has full (rwx) permissions, while the group (admins) and others have read and execute (r-x) permissions.
- -rwxr-xr-- 1 bobby admins scan.sh : The owner has read/write/execute (rwx) permissions, the group has read and execute (r-x), and others have read (r--) permissions.

Permissions can also be expressed numerically using octal values (0–7), where:

- **0**: No permissions
- **4**: Read
- **2**: Write
- **1**: Execute

For example, numeric permission 0754 translates to:

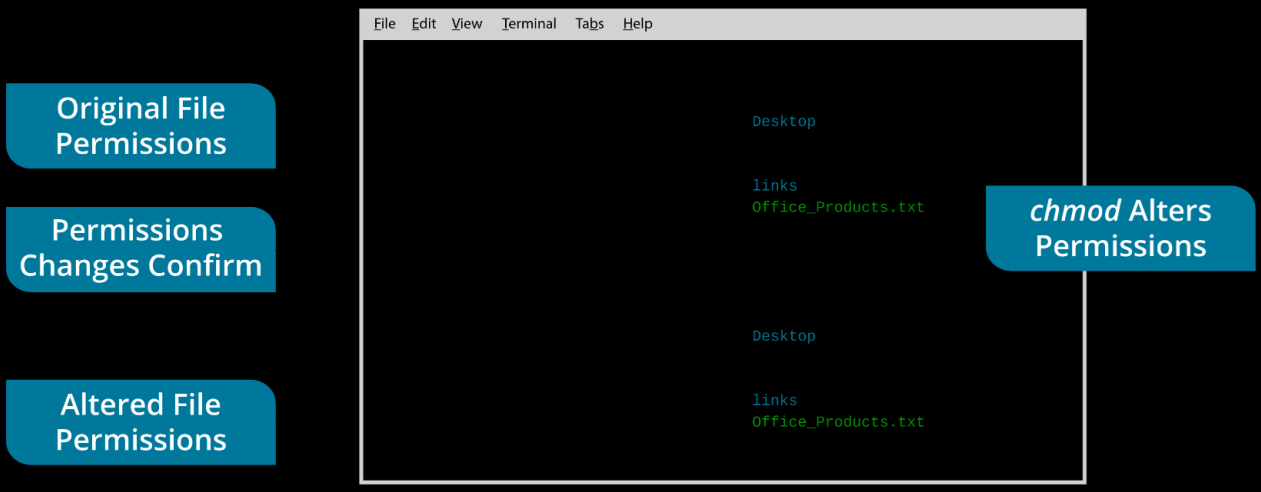
- **7**: Owner has all rights (4+2+1)
- **5**: Group has read and execute (4+0+1)
- **4**: Others have read (4+0+0)

The leading zero indicates octal format but can often be omitted. Another common combination is 6 (read and write).

chmod Command

The **chmod command** changes file and directory permissions using symbolic or **octal notation**. Only the owner can change permissions.

Figure 1. Modifying permissions using the chmod command



chown Command

The **chown command** allows the superuser or sudoers to change the owner of a file or directory. Regular users cannot use chown , even if they own the file, but they can change the group using the chgrp command.

The basic syntax for the chown command is: chown [OPTIONS] OWNER[:GROUP] FILE

- OWNER: The new owner of the file or directory.
- GROUP (optional): The new group for the file or directory. If omitted, only the owner is changed.
- FILE: The file or directory to modify.

Examples:

1. Change the owner of a file: chown username file.txt

2. Change both the owner and group: chown username:groupname file.txt

3. Change ownership recursively for a directory and its contents: chown -R username:groupname /path/to/directory

4. Change only the group (using :): chown :groupname file.txt

17.2 Package and Network Management

Core 2 Exam Objectives Covered

- 1.9 Identify common features and tools of the Linux client/desktop operating system.

TechEd Academy's network infrastructure requires regular updates and security checks to ensure reliable connectivity and data protection. You are responsible for managing software packages and network configurations across Linux systems, ensuring that all systems are up-to-date and secure against potential threats.

Learning Outcomes

As you study this lesson, answer the following questions:

- How do the apt and dnf commands differ in managing software packages, and what are their basic functions?
- How do you configure a package manager to access specific software repositories, and why is this important for system updates?
- How do the ps and top commands help in monitoring system processes, and what information do they provide?
- How do you configure persistent network settings using NetworkManager or systemd-networkd?

17.2.1 Package Management Commands

Linux software is available as source code and pre-compiled applications. Source code packages require compilation with the appropriate compiler and options. Pre-compiled packages can be installed using a package manager, which varies by distribution:

- **Advanced Packaging Tool (APT)**: Used by Debian-based distributions, working with .deb format packages.
- **DNF (Dandified YUM)**: Used by Red Hat-based distributions, working with .rpm format packages. DNF is the successor to YUM, offering improved performance and better dependency management.

Distributions and Repositories

A distribution includes precompiled software packages deemed appropriate by the vendor or sponsor. These packages, along with updates, are posted to software repositories. Vendors often maintain multiple repositories, such as stable, beta, and unsupported packages.

Figure 1. Listing package manager sources in Ubuntu Linux

```
toor@LX20D:/home$ cat /etc/apt/sources.list
#deb cdrom:[Ubuntu 20.04.2.0 LTS _Focal Fossa_ - Release amd64 (20210209.1)]/ focal main restricted

# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://gb.archive.ubuntu.com/ubuntu/ focal main restricted
# deb-src http://gb.archive.ubuntu.com/ubuntu/ focal main restricted

## Major bug fix updates produced after the final release of the
## distribution.
deb http://gb.archive.ubuntu.com/ubuntu/ focal-updates main restricted
# deb-src http://gb.archive.ubuntu.com/ubuntu/ focal-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://gb.archive.ubuntu.com/ubuntu/ focal universe
# deb-src http://gb.archive.ubuntu.com/ubuntu/ focal universe
deb http://gb.archive.ubuntu.com/ubuntu/ focal-updates universe
# deb-src http://gb.archive.ubuntu.com/ubuntu/ focal-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://gb.archive.ubuntu.com/ubuntu/ focal multiverse
# deb-src http://gb.archive.ubuntu.com/ubuntu/ focal multiverse
deb http://gb.archive.ubuntu.com/ubuntu/ focal-updates multiverse
# deb-src http://gb.archive.ubuntu.com/ubuntu/ focal-updates multiverse
```

Package managers must be configured with the web addresses of desired repositories, typically done automatically during setup. They handle installing, uninstalling, and updating software. Package integrity is verified using cryptographic hashes or signatures, such as MD5, SHA-256, or GPG, before installation or updates. The hash value and function are published on the package vendor's site.

apt Command

apt is the preferred command-line interface for APT. Basic commands include:

- Refresh package information: apt update
- Upgrade all packages: apt upgrade
- Install new application: apt install PackageName

For older systems or scripts, you may encounter the apt-get command, which provides similar functionality:

- Refresh package information: apt-get update

- Upgrade all packages: apt-get upgrade

dnf Command

dnf is the command-line interface for managing packages in Red Hat-based distributions. Basic commands include:

- Refresh package information: dnf check-update
- Upgrade all packages: dnf update or dnf upgrade

Note:

Both update and upgrade are interchangeable in DNF, but upgrade is the preferred term in modern usage.

- Install a new application: dnf install PackageName
- Remove an application: dnf remove PackageName

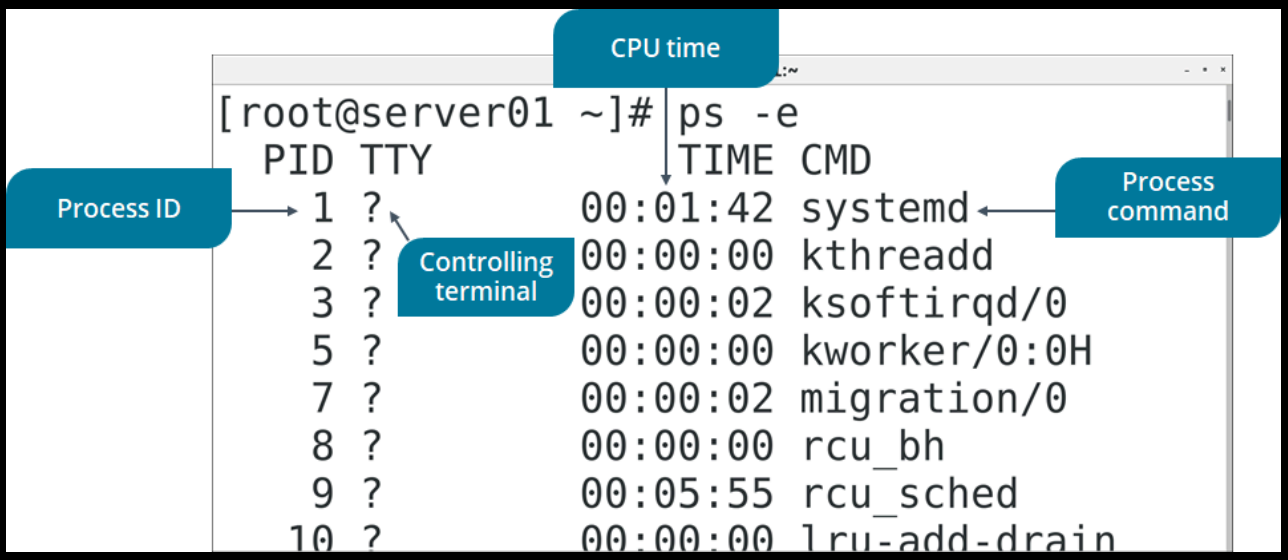
17.2.2 Process Monitoring Commands

Every process in Linux is assigned a unique process ID (PID) upon starting, allowing the system and users to identify it. This PID is a non-negative integer that increments with each new process. PID 1 is reserved for the initial daemon, the first process to start, serving as the parent of all other processes. Subsequent processes, whether initiated by the system or a user, receive the next available higher PID.

ps Command

The **ps command** displays the process table, summarizing the currently running processes on a system. Without options, it shows processes run by the current shell, including details like PID, associated terminal or pseudoterminal, accumulated CPU time, and the command that started the process. Various options can be used to filter and customize the displayed fields or processes.

Figure 1. Listing all processes on the system. Note that a question mark indicates that a process has no controlling terminal.



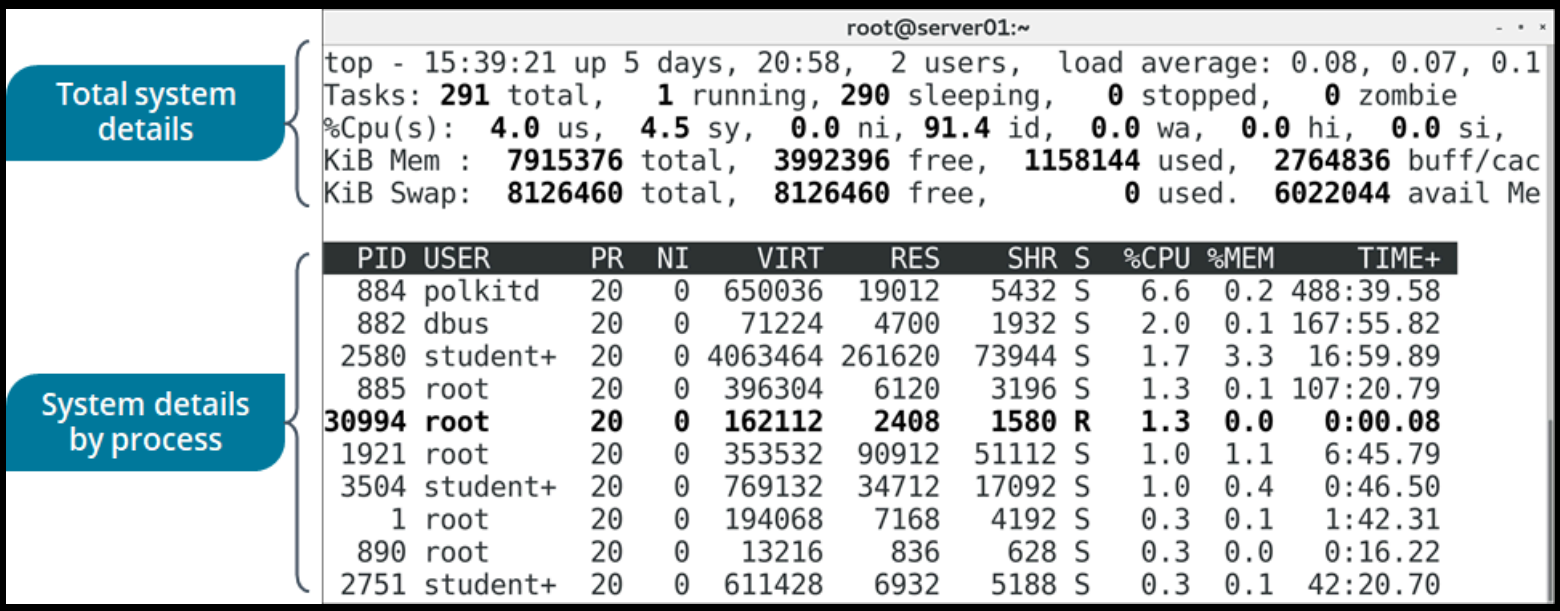
Description

The table includes process details such as Process I D, controlling terminal (T T Y), C P U time, and the command name.

top Command

The **top command**, like ps, lists all running processes on a Linux system. It serves as a process management tool, allowing you to interactively prioritize, sort, or terminate processes. It displays a dynamic, real-time view of process statuses.

Figure 2. Listing the state of running processes



Description

The top section shows total system details, including uptime, C P U usage, memory usage, and load averages. The lower section lists system details by process, such as P I D, user, priority, resident memory, C P U usage, and execution time (TIME plus).

Various keystrokes execute process management actions, including:

- **ENTER**: Refresh the status of all processes.
- **SHIFT+N**: Sort processes in decreasing PID order.
- **M**: Sort processes by memory usage.
- **P**: Sort processes by CPU usage.
- **u**: Display processes for a specified user at the prompt.
- **q**: Exit the process list.

systemd and systemctl Command

systemd is an init system and service manager for Linux operating systems. It is responsible for initializing the system and managing system services and processes.

The **systemctl** command is used to interact with **systemd** to control and manage system services. Key commands include:

- systemctl start [service] : Start a service immediately.
- systemctl stop [service] : Stop a running service.
- systemctl enable [service] : Enable a service to start automatically at boot.
- systemctl disable [service] : Disable a service from starting automatically at boot.
- systemctl status [service] : Check the status of a service, including whether it is active, inactive, or failed.

17.2.3 Network Management Commands

In Linux, Ethernet interfaces were traditionally named eth0, eth1, etc., but modern distributions often use names like enp0s3 or ens33, based on the system's hardware topology.

It's important to differentiate between the running and persistent configurations. The persistent configuration is applied after a reboot or when a network adapter is reinitialized, and the method for applying an IP configuration varies by distribution.

Historically, persistent configurations were managed by editing the /etc/network/interfaces file and using ifup and ifdown scripts to bring interfaces up or down. Now, many distributions use the NetworkManager package, manageable via a GUI or the nmcli command-line tool. Alternatively, network configurations can be managed using the systemd-networkd configuration manager.

ip Command

The **ip command** is a powerful tool for network configuration and management. It replaces older tools like ifconfig and route. It can be used to assign IP addresses, configure routing, and manage network interfaces.

Example usage:

ip addr show # Display all network interfaces and their IP addresses

ip link set enp0s3 up # Bring up the network interface enp0s3

ip route show # Display the routing table

/etc/hosts

The/etc/hosts file is a simple text file that maps hostnames to IP addresses. It is used for local hostname resolution before querying DNS servers. Entries in this file can be used to override DNS settings or to define local network names.

Example entry in /etc/hosts:

127.0.0.1 localhost

192.168.1.10 myserver.local

/etc/resolv.conf

The **/etc/resolv.conf** file contains information that defines how DNS (Domain Name System) resolution is handled. It specifies the DNS servers that the system should query to resolve domain names into IP addresses.

Example entry in /etc/resolv.conf:

nameserver 8.8.8.8

nameserver 8.8.4.4

ping Command

The **ping command** is used to test the reachability of a host on an IP network. It sends ICMP echo request packets to the target host and waits for an echo reply, helping to diagnose network connectivity issues.

Example usage:

ping example.com

dig Command

The **dig (Domain Information Groper) command** is a flexible tool for querying DNS name servers. It performs DNS lookups and displays the answers returned by the DNS server.

Example usage:

dig example.com

curl Command

The **curl command** is a tool for transferring data from or to a server using various protocols, including HTTP, HTTPS, FTP, and more. It is commonly used for testing and interacting with web services and is especially good for API interaction.

Example usage:

curl http://example.com

traceroute Command

The **traceroute command** is a network diagnostic tool used to track the pathway that a packet takes from the source to the destination. It helps in identifying the route and measuring transit delays of packets across an IP network.

Example usage:

traceroute example.com

This command will display each hop along the route to the destination, showing the IP address and the time taken for each hop. It is useful for diagnosing network issues and understanding the path data takes through the network.

17.2.5 Backup and Scheduling Commands

Linux doesn't have an "official" **backup** tool, but you can create a custom backup solution using the **cron job** task scheduler and file copy scripts, possibly incorporating compression utilities like tar or gzip. There are also many commercial and open-source backup products available, such as Amanda, Bacula, Fwbackups, and Rsync.

To run a batch of commands or scripts for backups or maintenance tasks, use the cron scheduling service. Each user can schedule tasks in their personal crontab (cron table), which cron merges into a system-wide schedule. The cron service checks this schedule every minute to execute tasks.

- Use the **crontab editor** to add or delete scheduled jobs.
- View a user's crontab jobs with crontab -l.
- Remove scheduled jobs with crontab -r.
- Enter the editor with crontab -e (default editor is vi).

Crontab Syntax

The basic syntax for scheduling a job in crontab includes:

- **mm**: Minutes past the hour (0–59).
- **hh**: Hour of the day (0–23).
- **dd**: Day of the month (1–31).
- **MM**: Month (1–12 or jan, feb, mar).
- **weekday**: Day of the week (0–7 or sun, mon, tue).
- **command**: Command or script to run, including the full path.

Time/date parameters can be replaced by wildcards:

- *: Any value.
- ,: Multiple values.
- -: Range of values.
- /n: Every nth value.

For example, consider the following crontab entry:

15 02 * * 5 /usr/bin/rsync -av --delete /home/sam

/mount/rsync

This entry runs the rsync backup program at 2:15 a.m. every Friday (day 5), synchronizing files from /home/sam to /mount/rsync with increased verbosity (-v). The --delete option removes files on the source side (/home/sam) that don't exist on the destination.

17.3 macOS Features

Core 2 Exam Objectives Covered

- 1.8 Explain common features and tools of the macOS/desktop operating system.

The faculty at TechEd Academy primarily use macOS devices for administrative tasks and content creation. Recently, there have been requests for improved security measures and efficient data management. Your role is to enhance the security and functionality of macOS systems, ensuring that faculty can work efficiently and securely.

Learning Outcomes

As you study this lesson, answer the following questions:

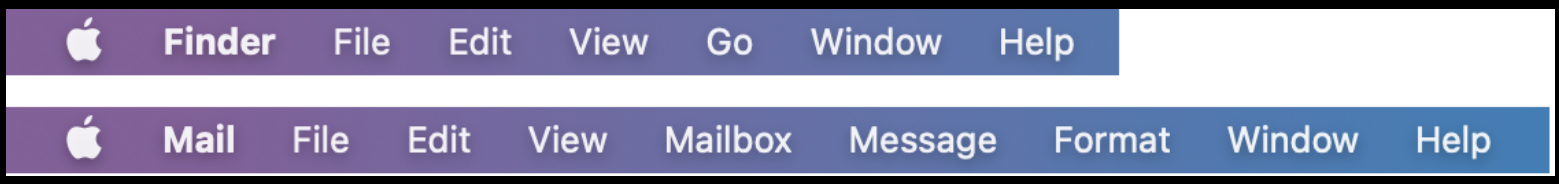
- How can Spotlight Search be used to quickly locate files and applications on macOS?
- What are the differences between the Z shell and Bash in macOS, and how do you access the Terminal?
- What is the role of the /Library folder in macOS, and how does it differ from the /System folder?
- How do you configure input device options in macOS System Preferences, and what are the key differences between Mac and PC keyboards?
- How do you link a local macOS account to an Apple ID, and what are the benefits of doing so?

17.3.1 Interface Features

When using an Apple Mac for the first time, you'll notice similarities and differences compared to a Windows-based PC. Like Windows, macOS boots to a graphical desktop environment, and any apps configured to launch at startup will do so.

Located at the top of the screen, the menu bar is always present and displays commands for the active window. To the left of the menu bar is the Apple menu, which provides options for support information (About), logging out, or shutting down.

Figure 1. Menu bars with different apps running



Screenshot reprinted with permission from Apple Inc.

Description

The first menu bar belongs to the Finder application, displaying options: Finder, File, Edit, View, Go, Window, and Help. The second menu bar belongs to the Mail application, displaying options: Mail, File, Edit, View, Mailbox, Message, Format, Window, and Help.

Dock

Positioned at the bottom of the screen, the **Dock** offers one-click access to favorite apps and files, similar to the Windows taskbar. Open apps display a dot below their icon.

Spotlight Search

Use **Spotlight Search** to find almost anything on macOS. Start a search by clicking the magnifying glass in the menu bar or pressing **COMMAND+SPACE**.

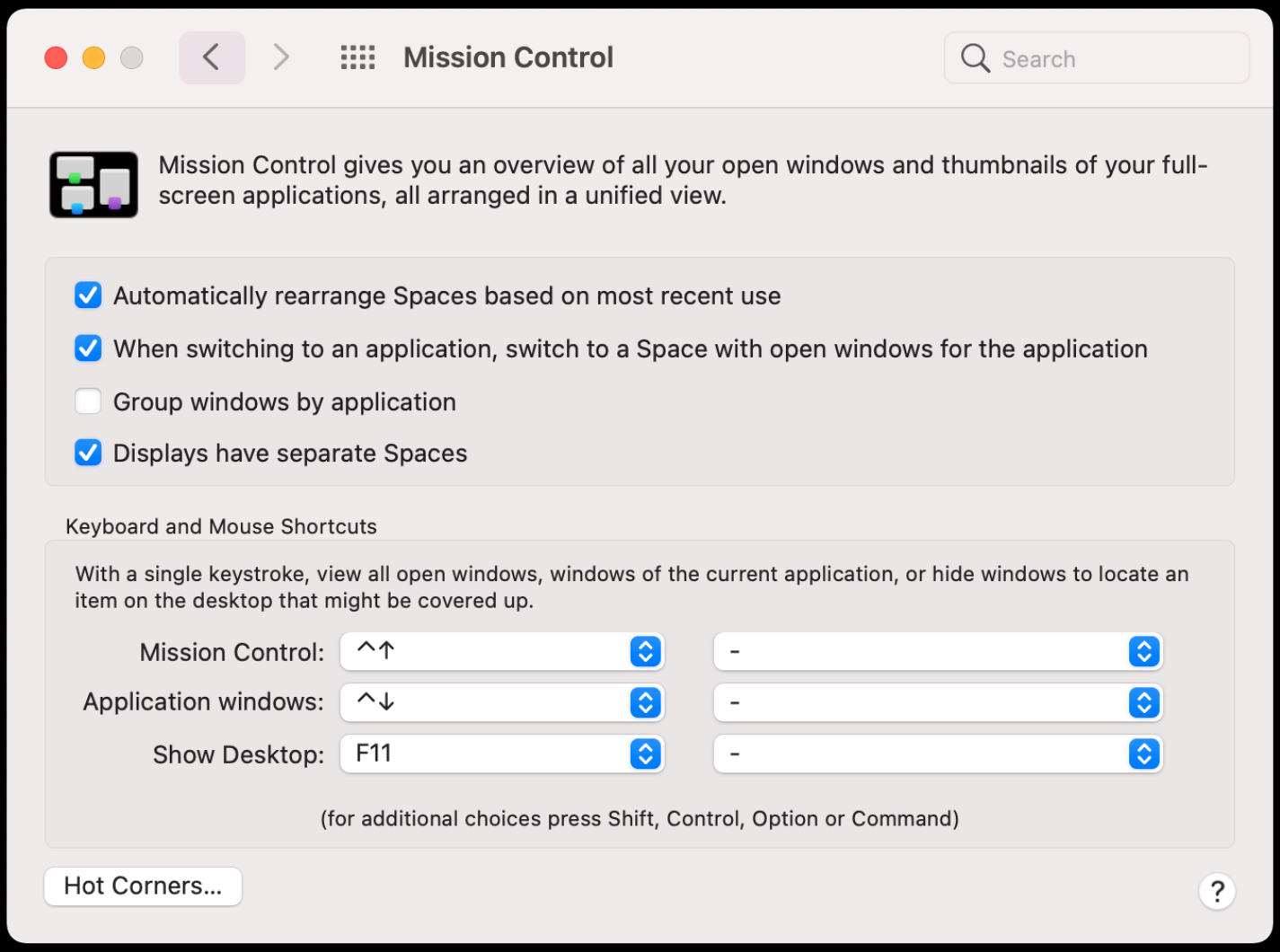
Terminal

Access the command-line environment via the **Terminal**, which uses the Z shell (zsh) by default from macOS Catalina onward. Older versions use Bash.

Mission Control and Multiple Displays

Mission Control manages windows and allows setting up **multiple desktops** with different apps and backgrounds. Activate Mission Control with the **F3** key. To move an app to a specific desktop, drag its window to the desired desktop at the top. Switch between desktops using the F3 key, **CONTROL+LEFT/RIGHT**, or a 3-/4-finger swipe gesture.

Figure 2. Mission Control is used to switch between windows and manage multiple desktops



Description

The screen includes checkboxes for options such as Automatically rearrange Spaces based on most recent use, When switching to an application, switch to a space with open windows for the application, group windows by application, and Displays have separate Spaces. Below, there is a section for keyboard and mouse shortcuts, listing key bindings for Mission Control, Application windows, and Show Desktop.

17.3.2 System Folders and Finder

System folders in macOS are directories that contain essential files and resources required for the operating system and applications to function properly. These folders are typically located at the root level of the system drive and include:

- **/Applications**: Contains applications installed for all users on the Mac.
- **/Library**: Stores system-wide resources and settings used by applications and macOS, such as fonts, application support files, and system preferences.
- **/System**: Contains core system files and resources essential for macOS operation. This folder is managed by the operating system and is generally not modified by users.
- **/Users**: Houses individual user accounts, with each user having a personal folder containing their documents, settings, and personal data.
- **/Users/Library**: A hidden folder within each user's home directory that stores user-specific application support files, preferences, caches, and other data.

These system folders are crucial for the stability and functionality of macOS, and users typically interact with them indirectly through applications and system settings.

Finder

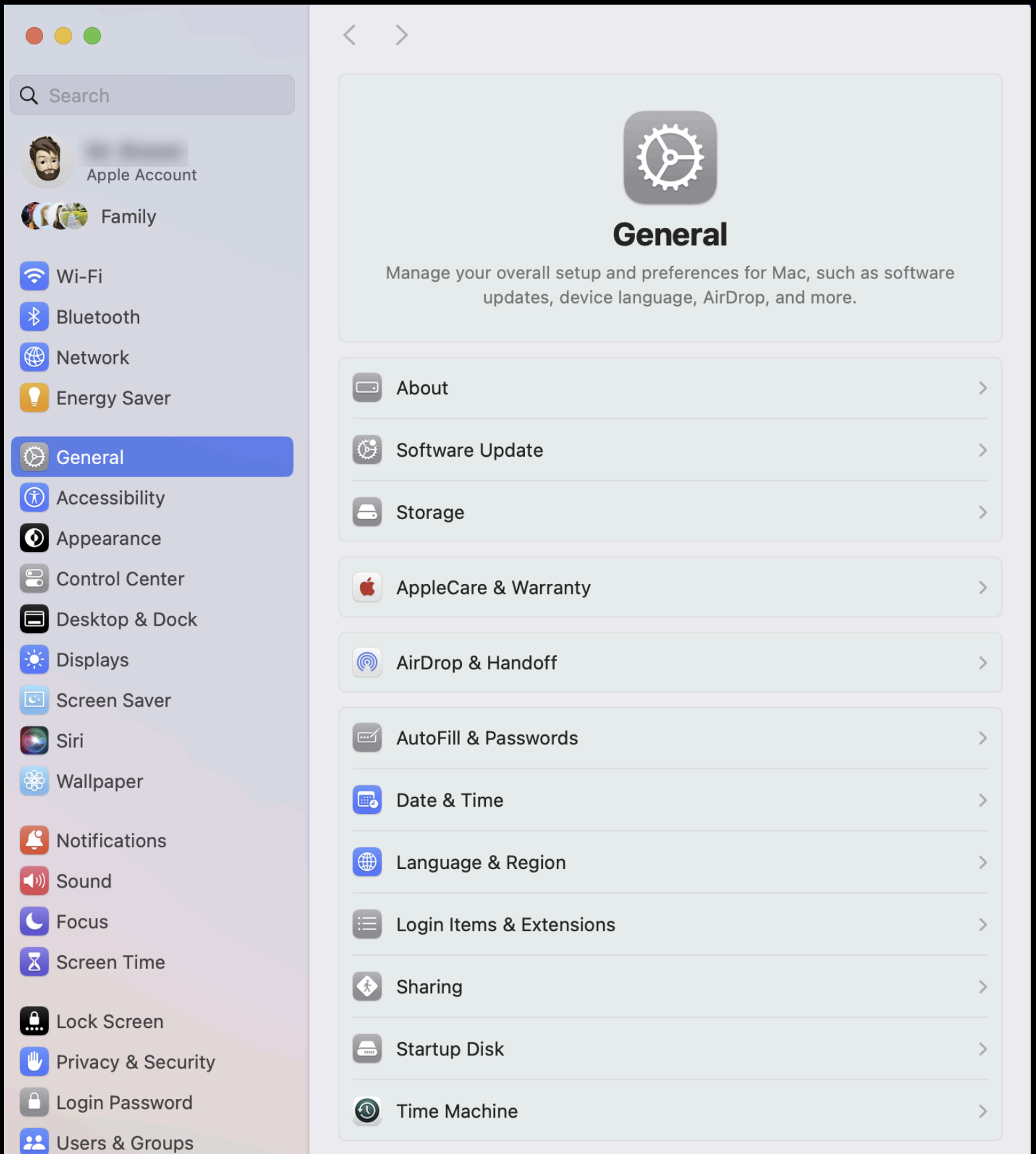
The **Finder** is the macOS equivalent of File Explorer in Windows. It lets the user navigate all the files and folders on a Mac. It is always present and open in the dock.

A+ Core 1 and Core 2 CertMaster Perform 15.0

17.3.3 System Settings

The **System Settings** panel in macOS is similar to the Windows Settings app. It serves as the central hub for changing settings, configuring network options, and optimizing macOS configurations.

Figure 1. System Settings


Search
Apple Account
Family
Wi-Fi
Bluetooth
Network
Energy Saver
General
Accessibility
Appearance
Control Center
Desktop & Dock
Displays
Screen Saver
Siri
Wallpaper
Notifications
Sound
Focus
Screen Time
Lock Screen
Privacy & Security
Login Password
Users & Groups
General
Manage your overall setup and preferences for Mac, such as software updates, device language, AirDrop, and more.
About
Software Update
Storage
AppleCare & Warranty
AirDrop & Handoff
AutoFill & Passwords
Date & Time
Language & Region
Login Items & Extensions
Sharing
Startup Disk
Time Machine

Screenshot reprinted with permission from Apple Inc.

Description

The general tab from the menu on the right is selected. The main screen lists the options below: About, Software Update, Storage, AppleCare and Warranty, Airdrop and Handoff, Autofill and Passwords, Date and Time, Language and Region, Login items and Extensions, Sharing, Startup Disk, Time Machine, Device Management, and Transfer or Reset.

System Settings also allows you to configure input device options. It's important to note some differences between input devices for Macs and PCs.

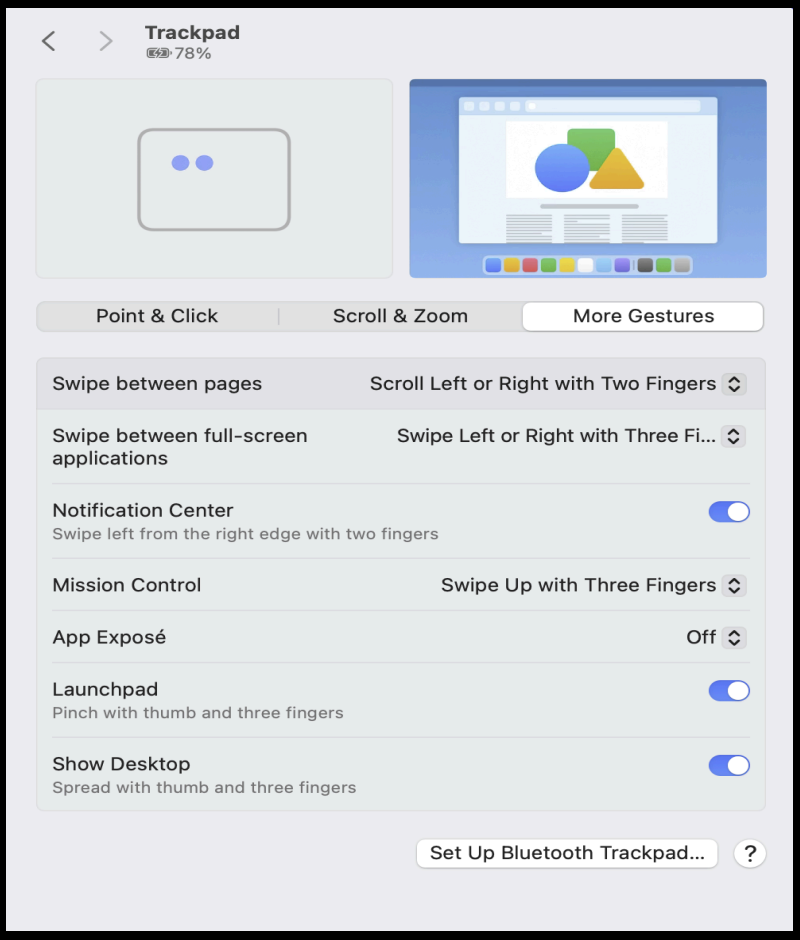
Apple Keyboards

Mac keyboards have **COMMAND**, **OPTION**, and **CONTROL** keys, along with an **APPLE/POWER** key. The **COMMAND** key functions similarly to the **CTRL** key on Windows and OPTION is often mapped to **ALT**. Use the Keyboard pane in System Preferences to map keys when using a non-Apple keyboard with a Mac.

Apple Magic Mouse and Trackpad with Gesture Support

While Macs do not support touchscreen interfaces, they do support gesture-enabled **Magic Mouse** and **Magic Trackpad** peripherals. To view or change available gestures, open the Trackpad preferences pane.

Figure 2. Configuring the trackpad



Description

The More Gestures tab is active, listing various touch gestures such as Swipe between pages, Swipe between full-screen apps, Notification Centre, Mission Control, and others. A set up bluetooth trackpad button is at the bottom.

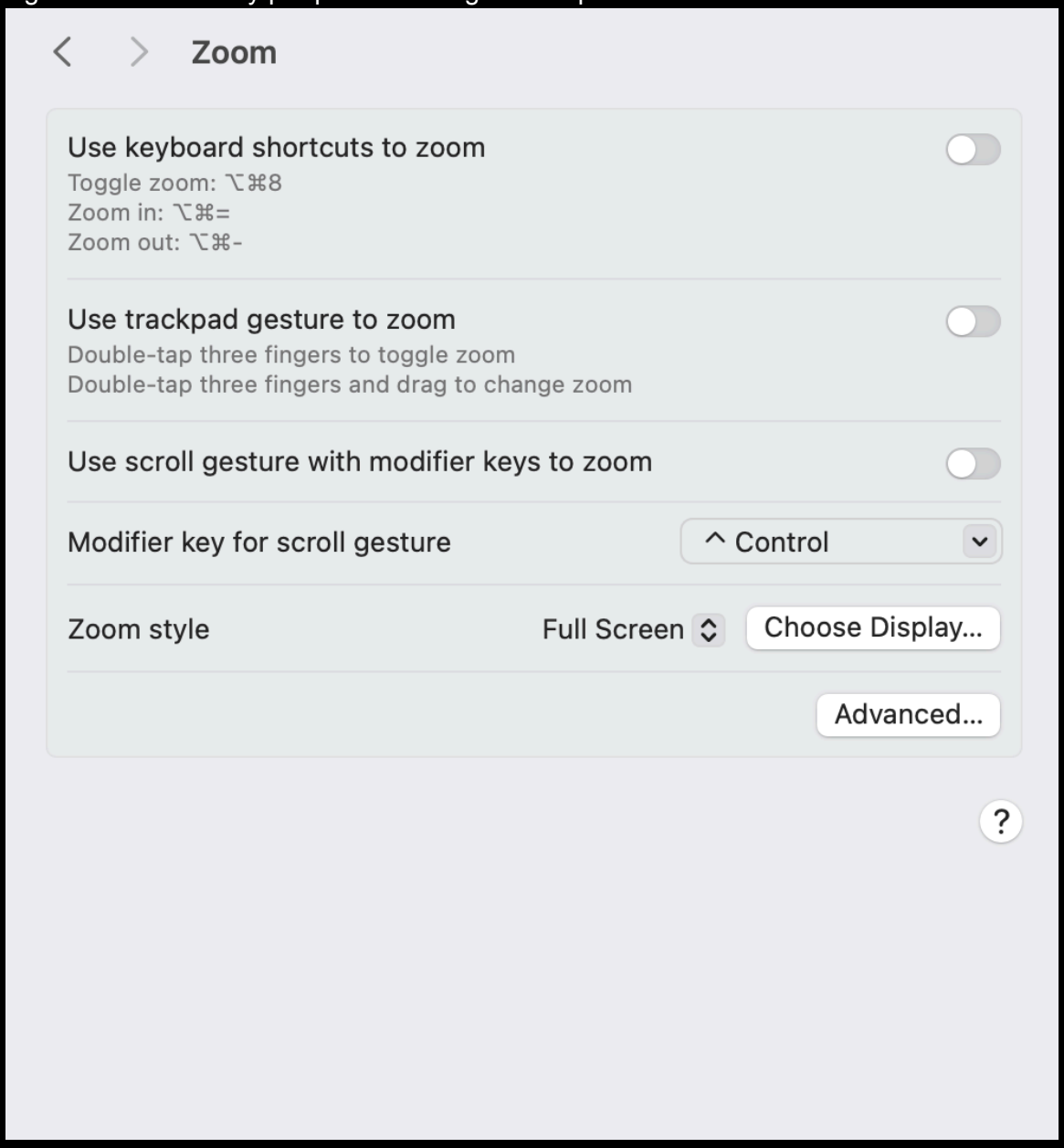
Displays

The **Displays** preferences pane allows you to adjust desktop scaling, set brightness levels, calibrate color profiles, and configure Night Shift settings to adapt the display to ambient light conditions.

Accessibility

The **Accessibility preferences** pane is used to configure assistive options for vision and sound, such as VoiceOver for screen narration, cursor size and motion settings, zoom tools, display contrast, font sizes, and captioning.

Figure 3. Accessibility prefpane showing Zoom options



Description

The pane lists the toggles for use keyboard shortcuts to zoom, use trackpad gesture to zoom, use scroll gesture with modifier keys to zoom, modifier key for scroll gesture, and zoom style. A choose display and advanced buttons are at the bottom.

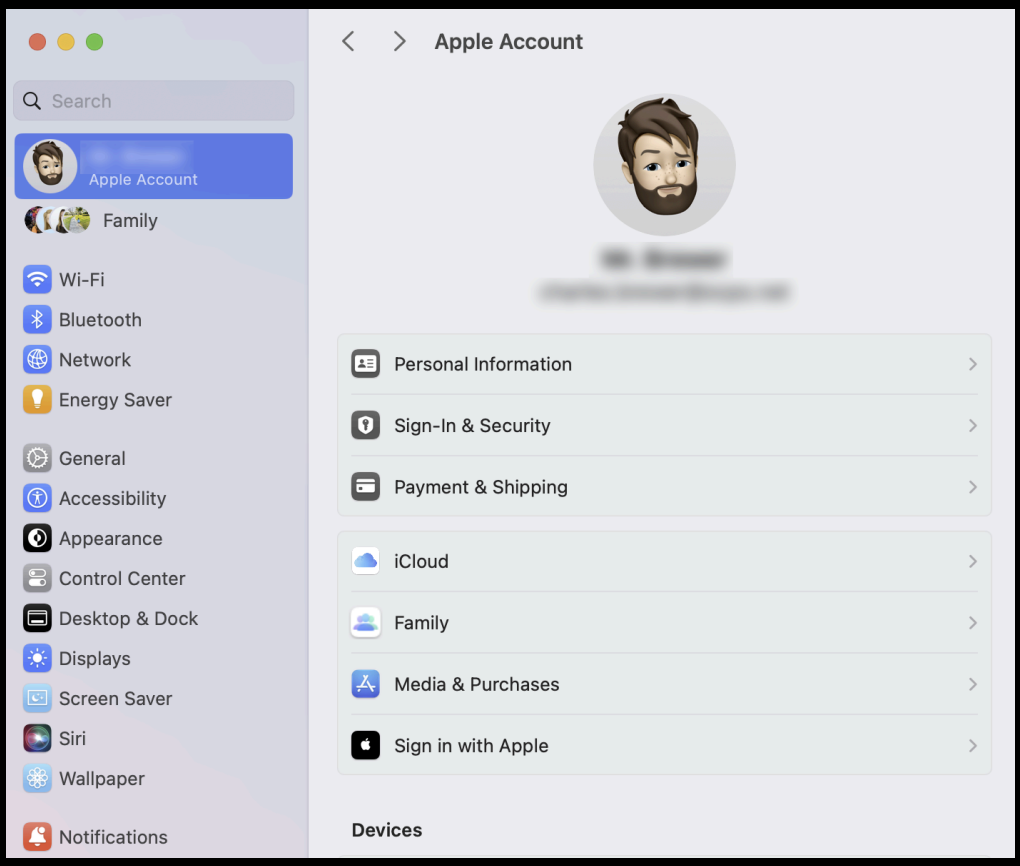
17.3.4 Security and User Management

When macOS is installed, an Administrator account and an optional Guest User account are created. To add a new account, go to **System Settings** > **Users & Groups**.

Apple ID

Each local account can be linked to an **Apple ID**, used for App Store purchases, iCloud access, and other functions. Users may already have an Apple ID from iTunes or iOS devices. You can sign in or out of your Apple ID via the System Preferences home page.

Figure 1. The Sign In & Security button in System Settings allows you to link an Apple ID to the local account



Screenshot reprinted with permission from Apple Inc.

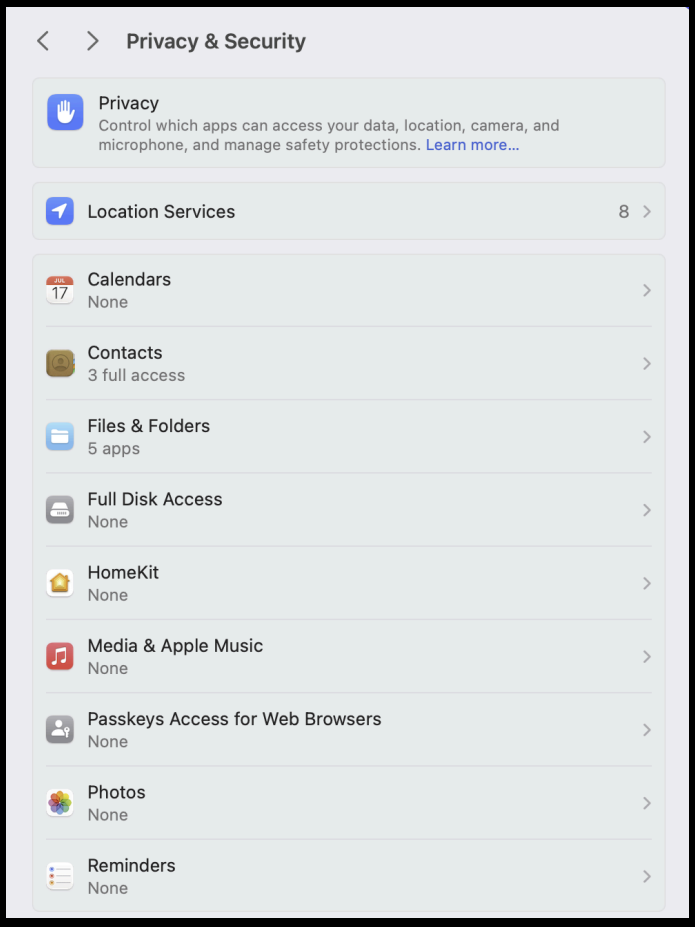
Description

The Apple account is selcted from the menu on the left. The options on the right are Personal Information, Sign-in and Security, Payment and Shipping, iCloud, Family, Media and Purchases, and Sign in with Apple.

Privacy & Security

macOS allows you to configure analytics, telemetry data, and app permissions for features like location services, camera, contacts, and calendar. Adjust these settings in the **Privacy & Security** preferences pane.

Figure 2. Privacy & Security showing privacy options



Screenshot reprinted with permission from Apple Inc.

Description

The options are location services, calendars, contacts, files and folders, full disk access, homekit, media and apple music, passkeys access for web browsers, photos and reminders.

Note:

Some changes require administrator approval; click the lock icon and authenticate to modify settings.

Internet Accounts and Keychain

The **Internet Accounts** pane lets you associate email and cloud accounts with your login. **Keychain** manages passwords for these accounts, websites, and Wi-Fi networks. iCloud Keychain syncs passwords across macOS and iOS devices. Use the **Keychain Access** app (in **Utilities**) to manage passwords. If you forget a password, search for it, select the entry, check "Show password," and enter an administrator password to view it. If issues arise, use **Keychain First Aid** for repairs.

FileVault

FileVault encrypts disk data to protect against unauthorized access if the disk is removed. When enabled, each user account requires a password. Configure a recovery method when encrypting for the first time. The recovery key can be stored in iCloud or recorded locally (avoid saving it on the encrypted disk).

17.3.5 iCloud and Continuity

Like Windows, a Mac can store files on local drives, but cloud storage offers a more secure option and simplifies data synchronization across devices.

iCloud is Apple's cloud storage solution, providing a central location for mail, contacts, calendar, photos, notes, reminders, and more across macOS and iOS devices. Users receive 5 GB of free storage by default, with options to upgrade for a monthly fee. This storage is shared across all iCloud components and devices.

FaceTime is a video and audio calling service that allows users to make calls over the internet to other Apple devices. It seamlessly integrates with iCloud to sync call history and contacts, enabling users to start a call on one device and continue it on another.

iMessage is Apple's messaging service that allows users to send texts, photos, videos, and more between Apple devices. It uses iCloud to sync messages across devices, ensuring that conversations are up-to-date and accessible from any Apple device.

iCloud Drive allows users to store and access files from any device connected to their iCloud account, enhancing productivity and accessibility by providing a unified file storage solution.

Figure 1. Using the Apple ID to configure iCloud synchronization options



Screenshot reprinted with permission from Apple Inc.

Description

The Apple ID from the left menu is selected. The horizontal bar on the right shows the storage. The options listed under save to iCloud are Photos, Drive, Passwords, Notes, Messages, and Mail. The options under the iCloud plus features

are Family, Private Relay, Hide My Email, and Custom Email. The advanced data protection is off. The toggle to access iCloud data on the Web is on.

Continuity

Continuity is a set of features in macOS and iOS that allows seamless integration and interaction between Apple devices. It enhances the user experience by enabling tasks to be started on one device and continued on another. Key Continuity features include:

- **Handoff**: Allows you to start a task on one Apple device (like writing an email or browsing a webpage) and continue it on another device.
- **Universal Clipboard**: Lets you copy content (text, images, etc.) on one Apple device and paste it on another.
- **Continuity Camera**: Enables you to take a photo or scan a document with your iPhone or iPad and have it appear instantly on your Mac.
- **Phone Calls and Text Messages**: Allows you to make and receive phone calls and send and receive SMS/MMS messages on your Mac using your iPhone.
- **Instant Hotspot**: Lets your Mac connect to the internet using the cellular connection of your iPhone or iPad without requiring a password.
- **Auto Unlock**: Allows you to unlock your Mac automatically when you're wearing an authenticated Apple Watch.
- **AirDrop**: Facilitates easy sharing of files between Apple devices without the need for email or messaging.

These features require devices to be signed in to the same Apple ID and connected to the same Wi-Fi network, with Bluetooth enabled.

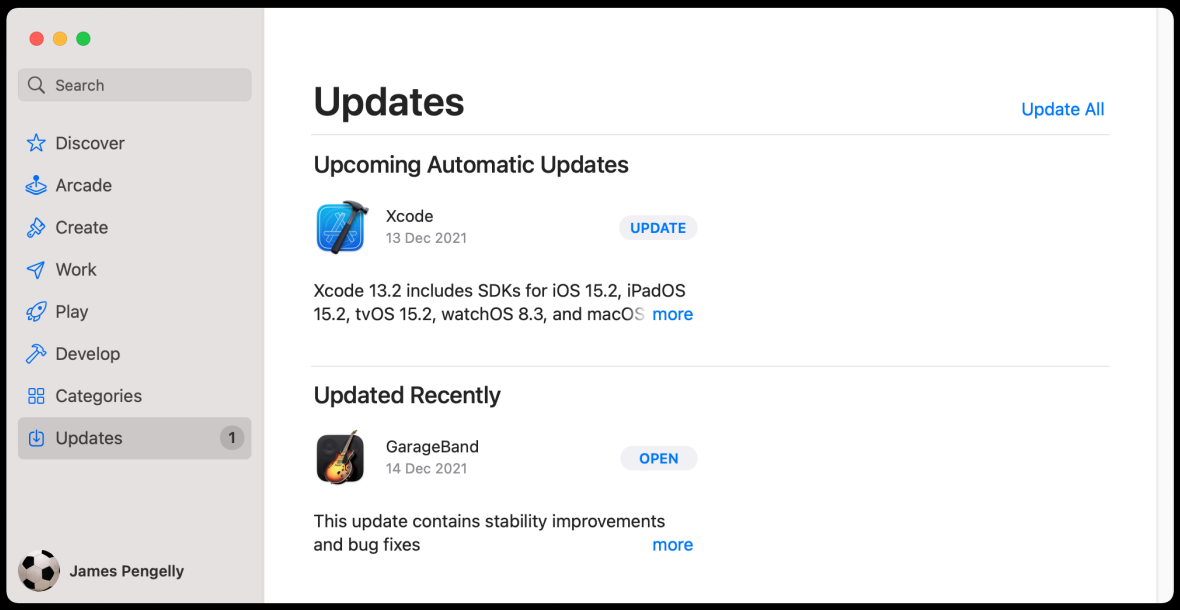
17.3.6 App Installation and Management

macOS apps are distributed mainly through the App Store and direct downloads.

Installation from the App Store

The **App Store** is a central platform for distributing free and paid software, as well as macOS updates and new releases. Access requires an Apple ID.

Figure 1. Monitoring the App Store for available updates



Description

The left sidebar contains categories such as Discover, Arcade, Create, Work, Play, Develop, and Updates. Update is selected. Below, recently updated apps are shown, including GarageBand, which received stability improvements and bug fixes.

Installation of Downloaded Apps

Some apps, like Adobe Creative Cloud and Skype, are not available in the App Store. Download these from the vendor's website, ensuring you select the macOS version. Drag the downloaded app to the Applications folder to install it.

By default, macOS allows app installations only from the App Store and identified developers. To change this, go to **System Settings**> **Security & Privacy**, click the padlock, and enter the Administrator password to adjust settings.

macOS Package Installer File Types:

- **DMG (.dmg)**: Used for simple installs where disk image contents are copied to the Applications folder.
- **PKG (.pkg)**: Used for installs requiring additional actions, like running services or writing files to multiple folders.

Installed apps are placed in a directory with an **APP** extension (.app) in the Applications folder.

Note: App installs might be restricted to the app store as a security setting.

App Uninstallation Process

To uninstall an app, use **Finder** to delete the .APP directory. Dragging an app to the Trash is unreliable for a complete uninstallation because it often leaves behind associated or cached files.

Antivirus

Like any software, macOS is vulnerable to security threats and advisories, some of which could allow an unprivileged user to gain root access. It's crucial to patch macOS systems against known vulnerabilities. While infections by conventional viruses or worms are relatively rare, new threats can still emerge. macOS is susceptible to malware like fake security alerts and Trojans. Additionally, a macOS host can transmit Windows viruses to others via email or file transfer. If a Windows boot partition is present, it can also become infected with a virus.

To protect a macOS computer from infection, follow these steps:

- **Download Trusted Apps**: By default, macOS allows app installations only from the App Store. If you change this setting, ensure you download apps from trusted websites.
- **Download Trusted Content**: Always obtain media and other content from reliable sources.
- **Use Antivirus Software**: Consider using free antivirus packages for Mac, such as Avira, Avast, or Sophos, to detect macOS malware and Windows viruses, preventing their spread via email or file sharing.
- **Protect Windows Partitions**: If you have a bootable Windows partition (Boot Camp), treat it like a standalone Windows computer. Use antivirus software and follow standard security practices to protect it.

Corporate Restrictions

macOS can be enrolled in a mobile device/endpoint management suite, allowing restrictions on app installation and uninstallation. Corporate apps can be pushed via the Business Manager portal. For more information, refer to Apple's Platform Deployment guide at support.apple.com/guide/deployment/welcome/web.

17.3.7 OS and App Updates

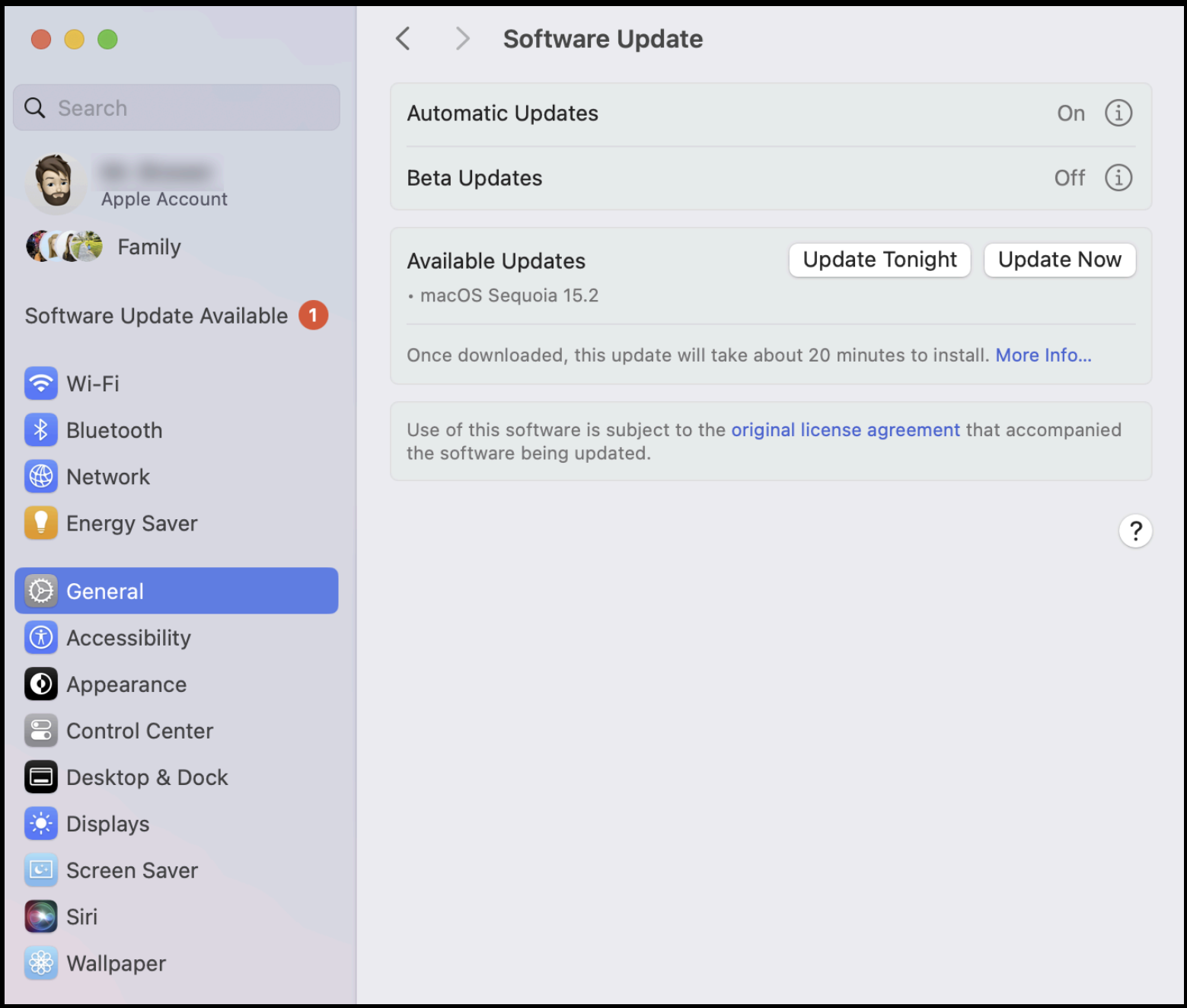
In macOS, the App Store checks daily for **updates and patches** for installed apps. If a new version is available, a notification appears on the App Store icon in the Dock.

Following best practices, it is recommended to select the "Update All" button to ensure all apps and macOS updates are current. Keeping your system and apps up-to-date is a key best practice for maintaining security and performance.

To enable automatic app updates on macOS:

- **For App Store updates**:
  - Go to **App Store** and enable options to automatically download and install App Store updates.
- **For macOS updates**:
  - Go to **System Settings > General > Software Update** and configure automatic download and installation of macOS updates.

Figure 1. Software Update showing that a macOS version upgrade is available



Most third-party apps downloaded outside the App Store will check for updates when launched, prompting you to update or cancel. As a best practice, you should manually check for updates within the app, typically by selecting **"Check for Updates"** in the app's menu.

Rapid Security Response (RSR)

Rapid Security Response (RSR) in macOS delivers important security updates faster than traditional software updates. It addresses vulnerabilities and threats without needing a full operating system update, ensuring users receive critical patches promptly to protect against exploits. RSR updates are smaller and quicker to install, minimizing user disruption. They can be applied automatically or manually, based on user settings.

17.3.8 Network and Device Settings

Various options in System Preferences allow you to add and configure hardware devices.

Network

Manage network settings from the **Status** menu on the right-hand side of the menu bar or via System Preferences.

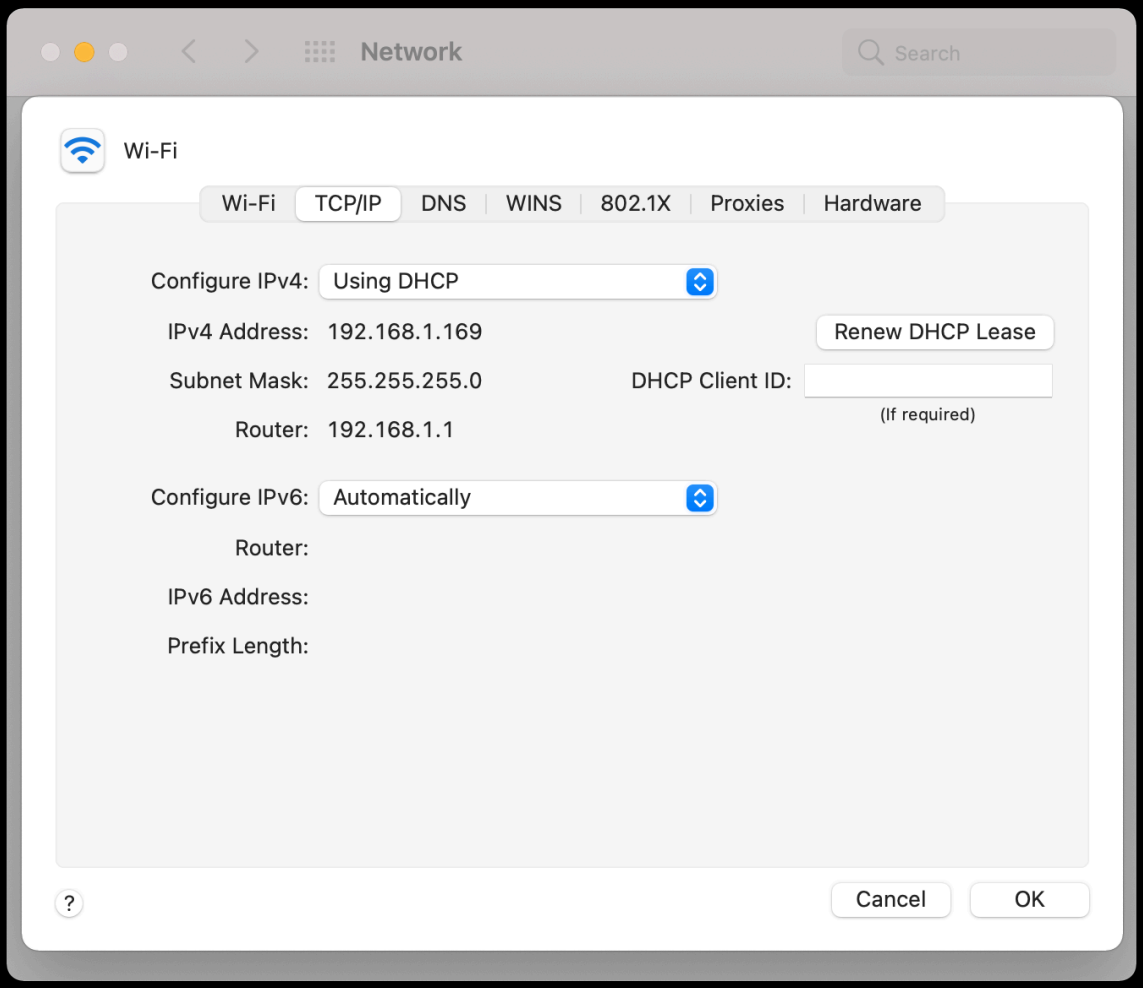
Figure 1. Status menus in the Menu bar



Screenshot reprinted with permission from Apple Inc.

Use the "Advanced" button to configure IP properties, proxy settings, and other network options.

Figure 2. Select the Advanced button in the Network prefpane to configure Wi-Fi options, IP and DNS settings, and proxy settings.



Description

The configurations are set to D H C P, with fields displaying I P address, subnet mask, router address, and D H C P lease options.

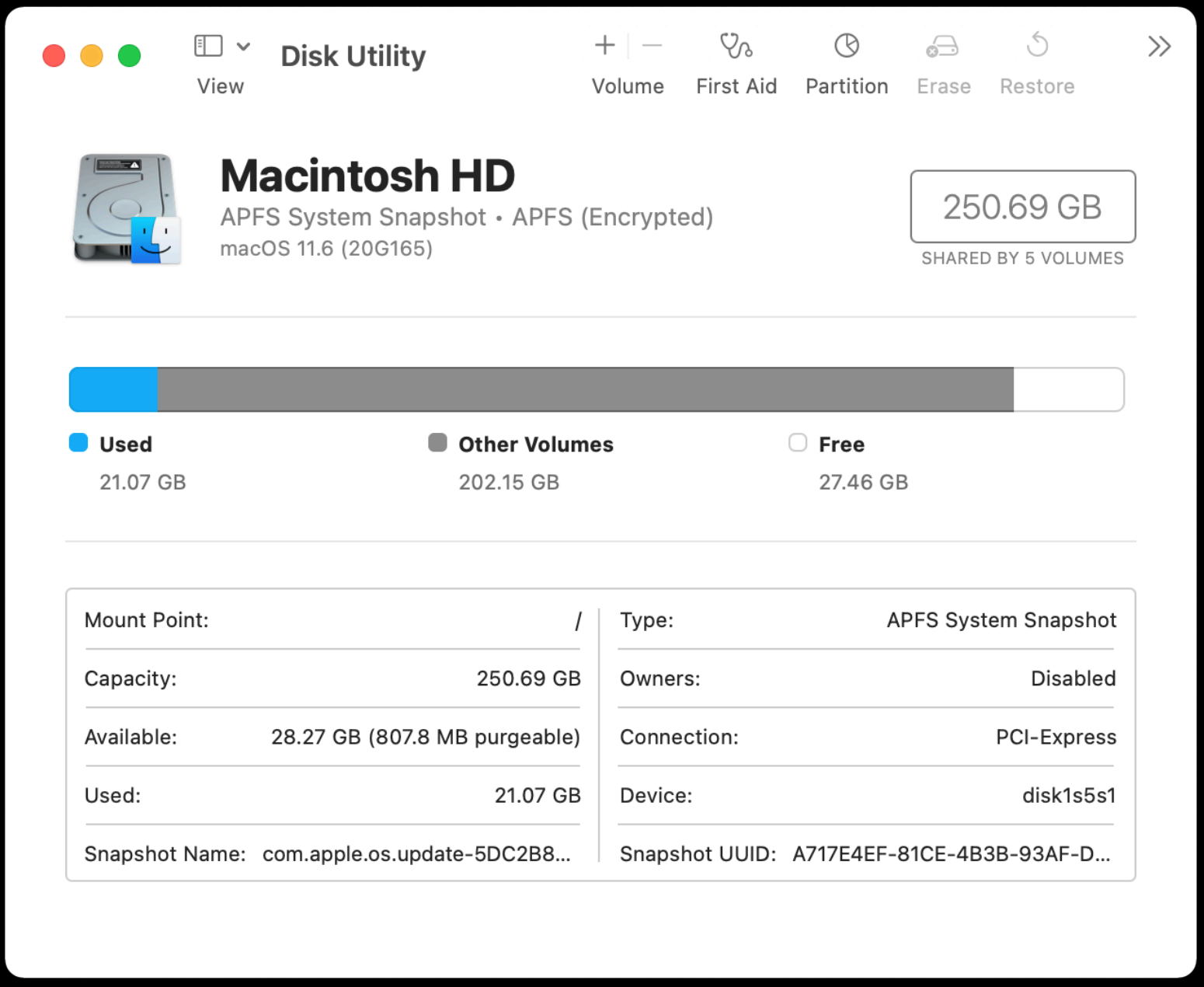
Printers & Scanners

Use the **Printers & Scanners** prefpane to add and manage print and scan devices.

Disk Utility

The **Disk Utility** app can verify or repair a disk or file system and erase a disk with security options if you are selling or passing on a Mac.

Figure 3. Use the Disk Utility to report storage status and configure and format volumes

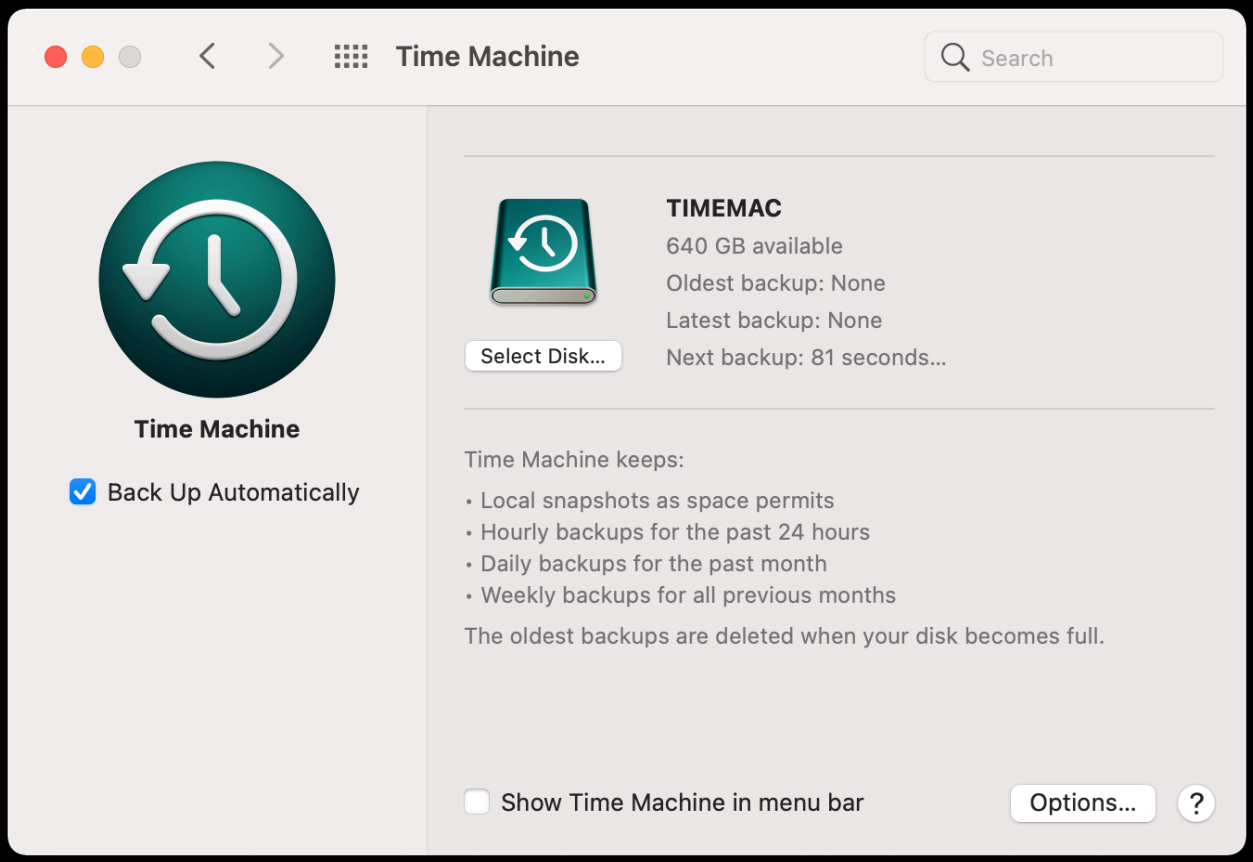


Regular defragmentation is not necessary for Mac hard drives, and defragmentation is rarely needed.

17.3.9 Time Machine Backup

The **Time Machine** preferences pane allows you to **back up** data to an external drive or partition formatted with APFS or macOS's older extended file system (HFS+). By default, Time Machine keeps hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for all previous months. When the backup drive becomes full, Time Machine automatically deletes the oldest backups to free up space.

Figure 1. Configuring Time Machine.



To restore files from Time Machine, use the timeline on the right side of the screen to view available backups. In the **Time Machine Finder** window, locate the folder with the file(s) you want to restore, and slide the timeline back to the desired date/time.

Note:

Time Machine also stores backups as local snapshots on the internal drive. If the backup drive is not connected, you may still be able to restore a file or version from these local snapshots. If a tick mark next to an item in the timeline is dimmed, the backup drive must be connected to restore that item.

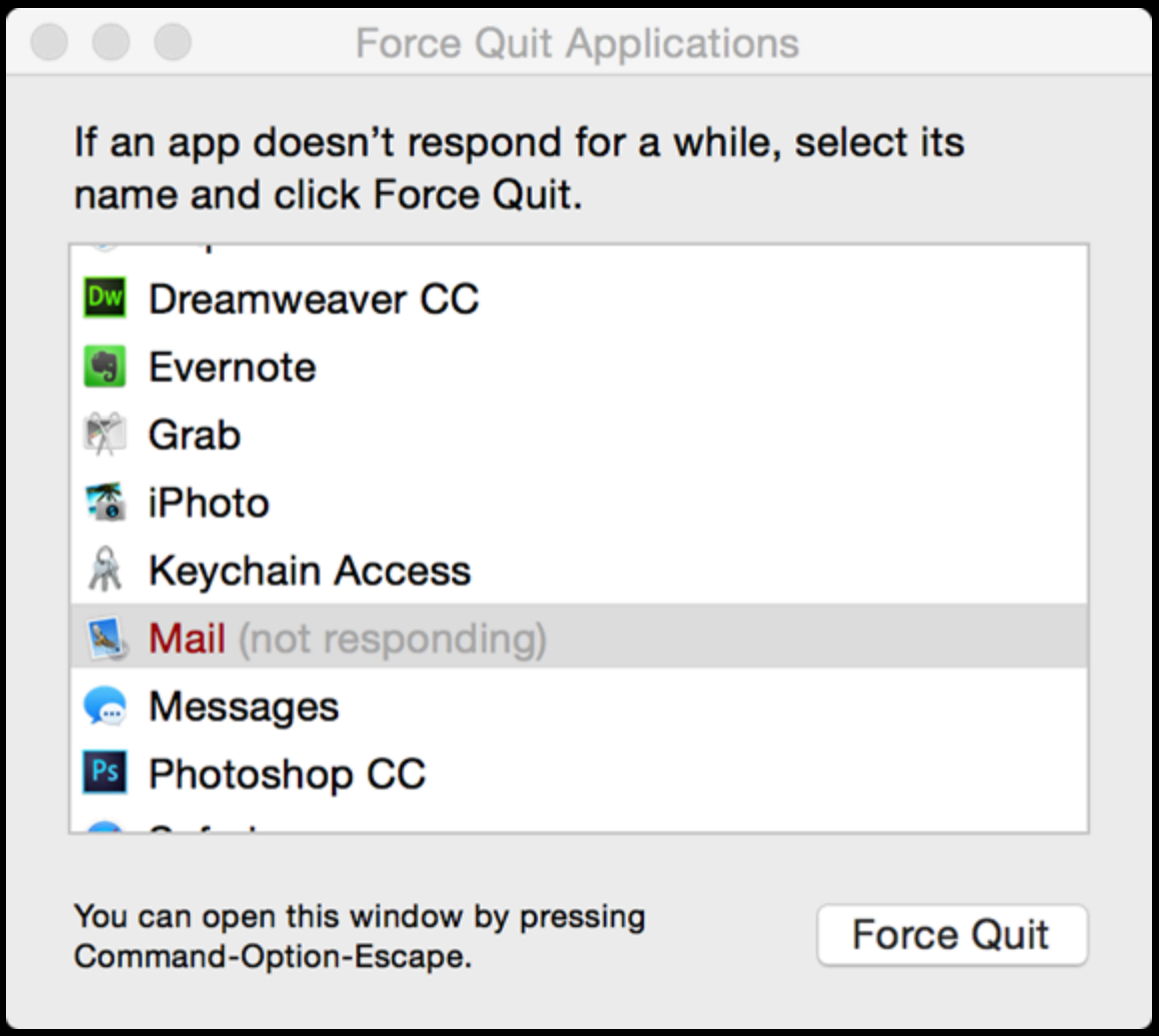
17.3.10 Troubleshoot Crashes and Boot Issues

macOS comes with several tools to troubleshoot app, OS, and data issues.

App Crashes and Force Quit

When an app is busy or processing a complex request, the **spinning wait cursor** may appear. If it remains visible for an extended period, the app might be unresponsive. To close and restart the app without rebooting the computer, use **Force Quit** from the **Apple** menu or press **COMMAND+OPTION+ESC**.

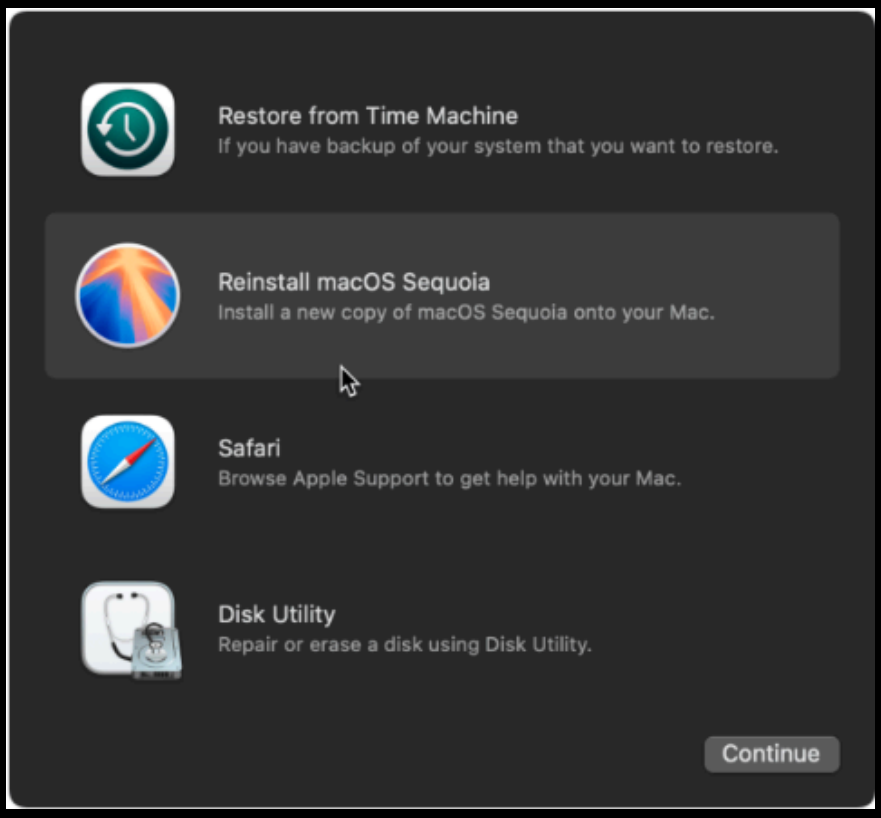
Figure 1. Using Force Quit to stop an app that is not responding



Recovery Menu

macOS includes utilities to restore a Mac from a Time Machine backup, reinstall macOS, or reformat and repair the system disk. To access the **Recovery** menu, hold down the **COMMAND+R** keys while powering up the Mac until you see the Apple logo. After selecting your language, macOS Recovery will launch, allowing you to choose from various recovery options.

Figure 2. macOS Recovery menu



Screenshot reprinted with permission from Apple Inc.

If an Apple Mac's startup drive is unavailable, it may boot into Internet Recovery Mode if connected to the Internet. This mode downloads a minimal recovery system from Apple's servers, allowing you to reinstall macOS or perform recovery tasks.

To restore a Mac to a specific point in time, such as after replacing or reformatting the hard drive, use a Time Machine backup. Time Machine lets you restore the entire system or specific files to a previous state, aiding in data recovery and system restoration.

18.0 Configuring SOHO Network Security

As a CompTIA A+ technician, you are in a position to identify potential security issues before they become big problems. By identifying security threats and vulnerabilities, as well as some of the controls that can counteract them, you can help keep your organization's computing resources safe from unauthorized access. In this lesson, you will identify security threats and vulnerabilities, plus some of the logical and physical controls used to mitigate them on SOHO networks.

Prepare for A+ Core 2 by:

- Explaining attacks, threats, and vulnerabilities.
- Comparing wireless security protocols.
- Configuring SOHO router security.
- Summarizing security measures.

18.1 Attacks, Threats, and Vulnerabilities

Core 2 Exam Objectives Covered

- 2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities.

In your new role as a Junior Security Technician, you have been tasked with identifying potential vulnerabilities that exist within the company. This includes both technology-related and physical security issues. Before you begin analyzing the company's security systems, you need to refresh your knowledge of potential threats.

In this lesson, you will learn the different types of vulnerabilities, including those that exist within the computer and network systems, social engineering, and encryption concepts.

Learning Outcomes

As you study this lesson, answer the following questions:

- What makes a zero-day vulnerability so unique?
- Why is having a system that is beyond its End of Life a security vulnerability?
- Why would someone go dumpster diving?
- What encryption method uses the same key to encrypt and decrypt data?
- What are digital signatures used for?

18.1.1 Vulnerabilities

A **vulnerability** is some fault or weakness in a system that could be exploited by a threat actor. Vulnerabilities can arise due to a very wide range of causes. Some of these causes include improperly configured or installed hardware or software, delays in applying and testing software and firmware patches, untested software and firmware patches, the misuse of software or communication protocols, poorly designed network architecture, inadequate physical security, insecure password usage, and design flaws in software or operating systems, such as unchecked user input.

These vulnerabilities can lead to many types of attacks including social engineering exploits such as phishing attacks, exploiting weak passwords, or allowing malware onto unprotected systems.

Non-compliant Systems

A configuration baseline is a set of recommendations for deploying a computer in a hardened configuration to minimize the risk that there could be vulnerabilities. There are baselines for different operating systems and different server and client roles. For example, a web server would have a different configuration baseline than a file server would have. The basic principle of a configuration baseline is to reduce the system's attack surface. The attack surface is all the points a threat actor could try to use to infiltrate or disrupt the system.

A **non-compliant system** is one that has drifted from its hardened configuration. A vulnerability scanner is a class of software designed to detect non-compliant systems.

Unprotected Systems

A baseline will recommend specific technical security controls to ensure a secure configuration. Examples of these controls include antivirus scanners, network and personal firewalls, and intrusion detection systems. An **unprotected system** is one where at least one of these controls is either missing or improperly configured. This increases the system's attack surface and potentially exposes more vulnerabilities.

When a system is unprotected, it becomes extremely vulnerable to attacks. For example, a simple phishing email tricks the user into clicking a link. This link then downloads malware into the system which opens a backdoor for the attacker to gain full control over the system and access secure information. Having appropriate protections in place will help prevent this type of attack from occurring.

Software and Zero-day Vulnerabilities

A software vulnerability is a fault in design or in code that can cause an application security system to be circumvented or that will cause the application to crash. The most serious vulnerabilities allow the attacker to execute arbitrary code on the system, which could allow the installation of malware. Malicious code that can use a vulnerability to compromise a host is called an **exploit**.

Most software vulnerabilities are discovered by software and security researchers, who notify the vendor to give them time to patch the vulnerability before releasing details to the wider public. A vulnerability that is exploited before the developer knows about it or can release a patch is called a **zero-day**. These can be extremely destructive, as it can take the vendor a lot of time to develop a patch, leaving systems vulnerable for days, weeks, or even years.

Note:

The term zero-day is usually applied to the vulnerability itself but can also refer to an attack or malware that exploits it.

The biggest concern with the zero-day attack is that it is an unknown threat. This vulnerability can exist and be exploited for a long time before anyone becomes aware of it. This means there is no protection against it. Once the threat becomes known, patches can be released to close the threat.

Known threats on the other hand can still be dangerous, but these threats usually work because the system has not been properly patched and hardened.

Unpatched and End of Life Operating Systems

While zero-day exploits can be extremely destructive, they are relatively rare events. A greater threat is the large number of unpatched or legacy systems in use.

- An unpatched system is one that its owner has not updated with OS and application patches.

- A legacy or **end of life (EOL)** system is one where the software vendor no longer provides support or fixes for problems.
  Note:
  These issues do not just affect PC operating systems and applications. Any type of code running on a network appliance or device can also be vulnerable to exploits. The risks to embedded systems have become more obvious and the risks posed by unpatched and EOL mobile devices and the Internet of Things are growing.

Bring Your Own Device Vulnerabilities

Bring your own device is a provisioning model that allows employees to use personal mobile devices to access corporate systems and data. In this scenario, it is very difficult for the security team to identify secure configuration

baselines for each type of device and mobile OS version, and even more challenging to ensure compliance with those baselines. BYOD is another example of increasing the network attack surface.

18.1.2 Social Engineering

Threat actors can use a diverse range of techniques to compromise a security system. A prerequisite of many types of attacks is to obtain information about the network and its security controls. **Social engineering**—or hacking the human—refers to techniques that persuade or intimidate people into revealing this kind of confidential information or allowing some sort of access to the organization that should not have been authorized.

Preventing social engineering attacks requires an awareness of the most common forms of social engineering exploits.

Impersonation

Impersonation means that the social engineer develops a pretext scenario to allow himself or herself an opportunity to interact with an employee. A classic impersonation pretext is for the threat actor to phone into a department pretending to be calling from IT support, claim something must be adjusted on the user's system remotely, and persuade the user to reveal his or her password. For this type of **pretexting** attack to succeed, the social engineer must gain the employee's trust or use intimidation or hoaxes to frighten the employee into complying.

One example of this type of attack is Business Email Compromise (BEC). In this attack, the attacker gains access to an email account in the company. This email account is then used to impersonate a trusted individual and attempts to trick employees into perform a specified task, such as sending money or divulging information.

Figure 1. Do you really know who's on the other end of the line?



Photo by Uros Jovicic on Unsplash.

Dumpster Diving

To make a pretext seem genuine, the threat actor must obtain privileged information about the organization or an individual. For example, an impersonation pretext is much more effective if the attacker knows the user's name. As most companies are set up toward customer service rather than security, this information is typically easy to come by. Information that might seem innocuous, such as department employee lists, job titles, phone numbers, diary appointments, invoices, or purchase orders, can help an attacker penetrate an organization through impersonation.

Another way to obtain information that will help to make a social engineering attack credible is by obtaining documents that the company has thrown away. **Dumpster diving** refers to combing through an organization's (or individual's) garbage to try to find useful documents. Attackers may even find files stored on discarded removable media.

Note:

A threat actor might stage multiple attacks as part of a campaign. Initial attacks may only aim at compromising low-level information and user accounts, but this low-level information can be used to attack more sensitive and confidential data and better protected management and administrative accounts.

Shoulder Surfing

A **shoulder surfing** attack means that the threat actor learns a password or PIN (or other secure information) by watching the user type it. Despite the name, the attacker may not have to be in proximity to the target—they could use high-powered binoculars or CCTV to directly observe the target remotely, for instance.

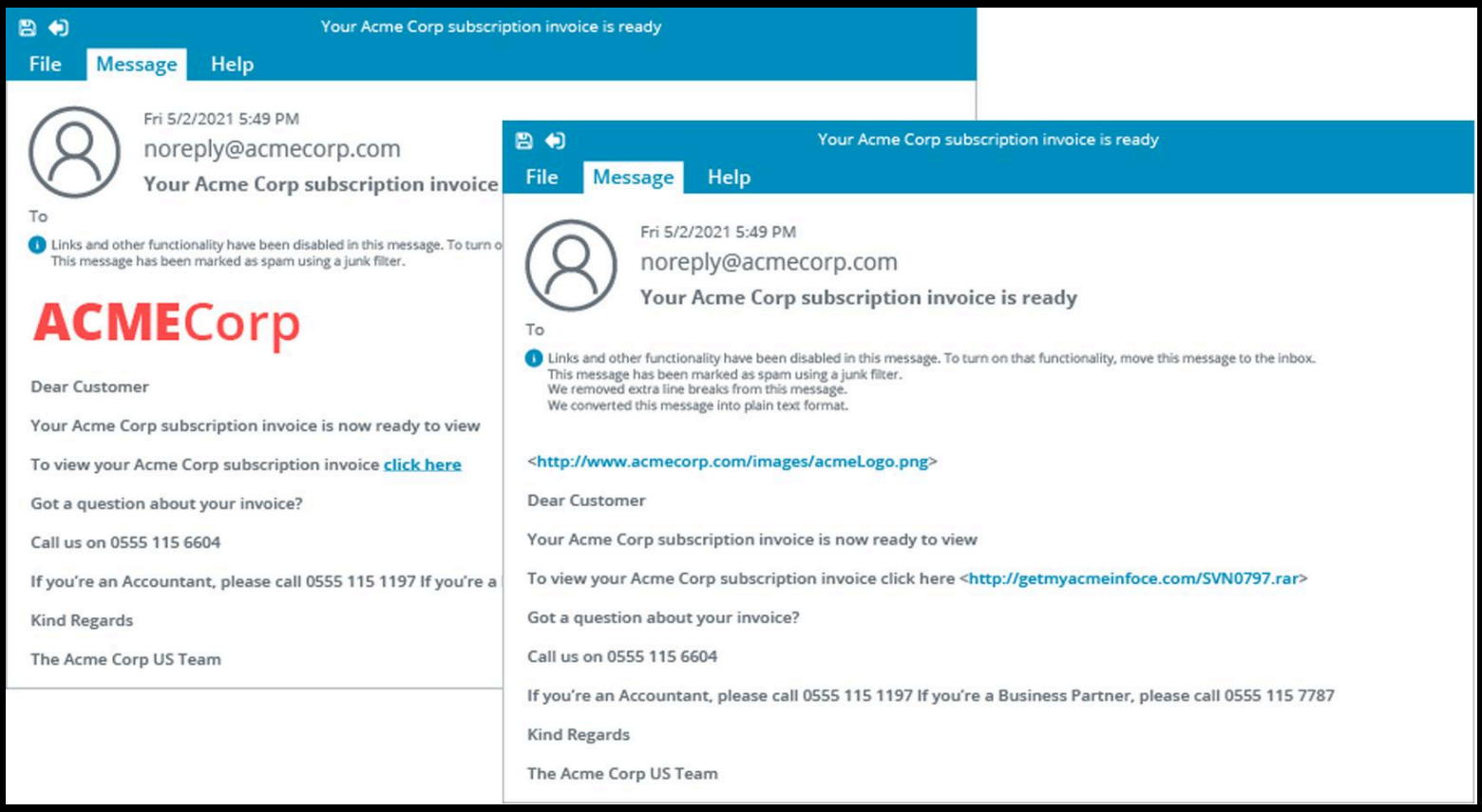
Tailgating and Piggybacking

Tailgaiting is a means of entering a secure area without authorization by following closely behind the person who has been allowed to open the door or checkpoint. **Piggybacking** is a similar situation but means that the attacker enters a secure area with an employee's permission. For instance, an attacker might impersonate a member of the cleaning crew and request that an employee hold the door open while the attacker brings in a cleaning cart or mop bucket. Another technique is to persuade someone to hold a door open, using an excuse such as "I've forgotten my badge (or key)."

18.1.4 Phishing and Evil Twins

Phishing uses social engineering techniques to make spoofed electronic communications seem authentic to the victim. A phishing message might try to convince the user to perform some action, such as installing malware disguised as an antivirus program or allowing a threat actor posing as a support technician to establish a remote access connection. Other types of phishing campaigns use a spoof website set up to imitate a bank or e-commerce site or some other web resource that should be trusted by the target. The attacker then emails users of the genuine website, informing them that their account must be updated. Or, with some sort of hoax alert or alarm, the attacker supplies a disguised link that leads to the spoofed site. When users authenticate with the spoofed site, their login credentials are captured.

Figure 1. Example of a phishing email



Screenshot courtesy of CompTIA.

Some phishing variants are referred to by specific names:

- **Spear-phishing** occurs when the attacker has some information that makes the target more likely to be fooled by the attack. The threat actor might know the name of a document that the target is editing, for instance, and send a malicious copy, or the phishing email might show that the attacker knows the recipient's full name, job title, telephone number, or other details that help to convince the target that the communication is genuine.
- **Whaling** is an attack directed specifically against upper levels of management in the organization (CEOs and other "big catches"). Upper management may also be more vulnerable to ordinary phishing attacks because of their reluctance to learn basic security procedures.
- **Vishing** is conducted through a voice channel (telephone or VoIP, for instance). For example, targets could be called by someone purporting to represent their bank asking them to verify a recent credit card transaction and requesting their security details. It can be much more difficult for someone to refuse a request made in a phone call compared to one made in an email. The growth of AI has allowed attackers to utilize AI to impersonate voices which can increase the chances of a user falling victim to this attack.
- Smishing is an attack performed through SMS text messages. In this attack, the target will receive a text message that looks like it's from a legitimate source, such as their bank. The message will typically have a sense of urgency and encourage the target to click a link that redirects to a fake website or even a phone number to call and speak with someone. The website or person will attempt to have the target enter their login credentials and reveal personal information.

- QR code phishing (Quishing) uses malicious QR codes to trick targets into visiting a fake website to enter their credentials and reveal personal information. QR codes are essentially shortcuts to websites and downloads. If the attacker can get a target to scan the QR code, the target is redirected to the malicious site or prompted to download malware to their system.

An **evil twin** attack is similar to phishing but instead of an email, the attacker uses a rogue wireless access point to try to harvest credentials. An evil twin might have a similar network name (SSID) to the legitimate one, or the attacker might use some denial of service (DoS) technique to overcome the legitimate AP. The evil twin might be able to harvest authentication information from users entering their credentials by mistake. For example, the evil twin might allow devices to connect via open authentication and then redirect users' web browsers to a spoofed captive portal that prompts them for their network password.

18.1.5 Threat Types

Historically, cybersecurity techniques were highly dependent on the identification of "static" known **threats**, such as computer viruses. This type of threat leaves a programming code signature in the file that it infects that is relatively straightforward to identify with automated scanning software. Unfortunately, adversaries were able to develop means of circumventing this type of signature-based scanning.

The sophisticated nature of modern cybersecurity threats means that it is important to be able to describe and analyze behaviors. This behavioral analysis involves identifying the attributes of threat actors in terms of location, intent, and capability.

External versus Internal Threats

An external threat actor is one who has no account or authorized access to the target system. A malicious external threat actor must infiltrate the security system using malware and/or social engineering. Note that an external actor may perpetrate an attack remotely or on-premises (by breaking into the company's headquarters, for instance). It is the threat actor who is defined as external, rather than the attack method.

One example of an attack that can be carried out by an external threat is a supply chain or pipeline attack. In this attack, instead of attacking the company directly, the attacker focuses on gaining unauthorized access to weaker links in the chain, such as vendors, suppliers, or service providers. This access can then be used to gain access to the company's resources. Instead of attacks like a denial-of-service which targets the victim directly, these attacks are more indirect, but can still be extremely damaging.

Conversely, an **insider threat** actor is one who has been granted permissions on the system. This typically means an employee, but insider threats can also arise from contractors and business partners. It is important to realize that insider threats can be either malicious or non-malicious. An example of a malicious insider threat is a disgruntled or corrupt employee trying to damage or steal confidential company data. An example of a non-malicious insider threat is a technician setting up a Minecraft server on one of the company's computers, exposing it to unnecessary risk.

Because external threats are not supposed to be in the network or systems, they can be easier to detect. If an attacker is moving through the network and targeting multiple systems, bypassing firewalls and other security features, this will most likely raise some flags and alert security to the threat. On the other hand, the internal threat is already in the network and is using their credentials and knowledge to gain access to the systems. These threats are much more difficult to detect until after the damage has already been done.

Footprinting Threats

Footprinting is an information-gathering threat in which the attacker attempts to learn about the configuration of the network and security systems. A threat actor will perform reconnaissance and research about the target, gathering publicly available information, scanning network ports and websites, and using social engineering techniques to try to discover vulnerabilities and ways to exploit the target.

Spoofing Threats

A **spoofing** threat is any type of attack where the threat actor can masquerade as a trusted user or computer. Spoofing can mean cloning a valid MAC or IP address, using a false digital certificate, creating an email message that imitates a legitimate one, or performing social engineering by pretending to be someone else.

Spoofing can also be performed by obtaining a logical token or software token. A logical token is assigned to a user or computer during authentication to some service. A token might be implemented as a web cookie, for instance. If an attacker can steal the token and the authorization system has not been designed well, the attacker may be able to present the token again and impersonate the original user. This type of spoofing is also called a replay attack.

While many types of attacks will disrupt system operations, spoofing is typically a more stealthy type of attack and should not cause system disruptions.

On-path Attacks

An **on-path attack** is a specific type of spoofing where the threat actor can covertly intercept traffic between two hosts or networks. This allows the threat actor to read and possibly modify the packets. An on-path attack is often designed to try to recover password hashes. An evil twin is one example of an on-path attack. In this attack, the attacker sets up a fake wireless network that is spoofed to look like a legitimate network. When a victim connects to the spoofed network, the attacker can monitor and intercept their data.

Note:

On-path attack is the updated terminology for man-in-the-middle (MitM). Non-inclusive terminology that uses this kind of weak or vague metaphor is deprecated in most modern documentation and research. The terms adversary-in-the-middle (AitM) and machine-in-the-middle (MitM) are also used today.

Denial of Service Attack

A **denial of service attack** attack causes a service at a given host to fail or to become unavailable to legitimate users. Typically, a DoS attack tries to overload a service by bombarding it with spoofed requests. It is also possible for DoS attacks to exploit design failures or other vulnerabilities in application software to cause it to crash. Physical DoS refers to cutting the power to a computer or cutting a network cable.

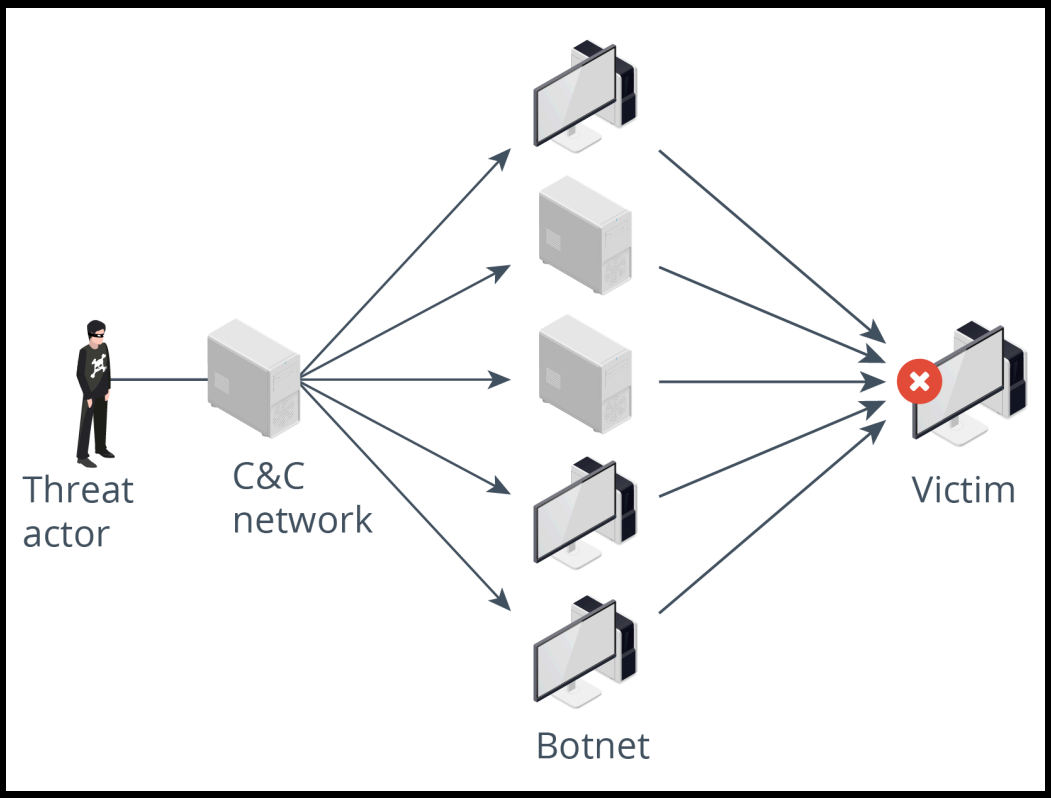
DoS attacks may simply be motivated by the malicious desire to cause trouble. DoS is also often used to mask a different type of attack. For example, a DoS attack against a web server might be used to occupy the security team when the threat actor's real goal is stealing information from a database server.

Compared to other attacks, a DoS attack can be extremely devastating as it can take down services for an extended period of time and cause massive service disruptions.

Distributed DoS Attacks and Botnets

Network-based DoS attacks are normally accomplished by flooding the server with bogus requests. They rely on the attacker having access to greater bandwidth than the target or on the target being required to devote more resources to each connection than the attacker. This type of bandwidth-directed DoS attack is usually perpetrated as **distributed denial-of-service**. Most networks and systems today can handle a lot of bandwidth so a single system can't produce enough bandwidth by itself to take down the target. This is where the distributed denial-of-service attack comes in.

DDoS means that the attacks are launched from multiple compromised systems, referred to as a **botnet**. To establish a botnet, the threat actor will first compromise one or two machines to use as a command & control (C&C) server. The C&C servers are used to compromise hundreds or thousands of devices by installing bots on them via automated exploits or successful phishing attacks. A bot establishes a persistent remote-control channel with the C&C hosts. This allows the threat actor to launch coordinated attacks using all the devices in the botnet. Figure 1. Using a command & control (C&C) network to operate a botnet of compromised hosts and coordinate a DDoS attack.

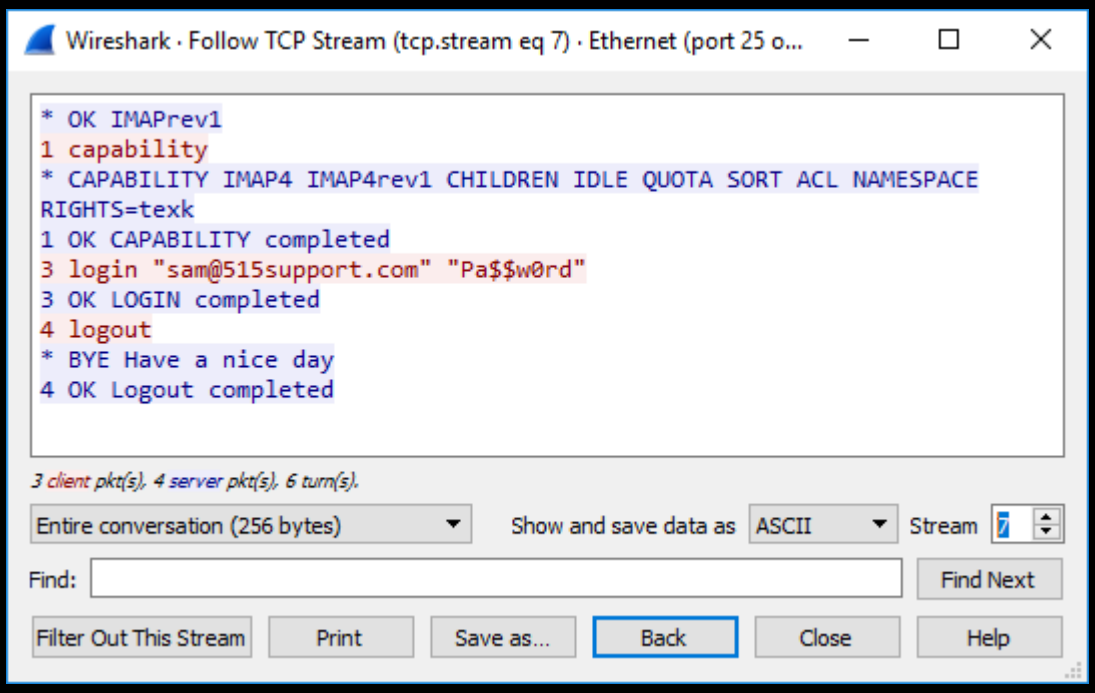


18.1.6 Password Attacks

On-path and malware attacks can be difficult to perpetrate. Many network intrusions occur because a threat actor simply obtains credentials to access the network. Also, when threat actors gain some sort of access via an on-path or malware attack, they are likely to attempt to escalate privileges to gain access to other targets on the network by harvesting credentials for administrative accounts.

A plaintext **password** can be captured by obtaining a password file or by sniffing unencrypted traffic on the network. If the protocol does not use encryption, then the threat actor can simply read the password string from the captured frames.

Figure 1. Wireshark TCP Stream



Screenshot courtesy of Wireshark.

In most cases, a password is stored and transmitted more securely by making a cryptographic hash of the string entered by the user. A cryptographic hash algorithm produces a fixed-length string from a variable-length string using a one-way function. This means that, in theory, no one except the user (not even the system administrator) knows the password because the plaintext should not be recoverable from the hash.

Note:

A password might be sent in an encoded form, such as Base64, which is simply an ASCII representation of binary data. This is not the same as cryptographic hashing. The password value can easily be derived from the Base64 string.

A threat actor might obtain a database of password hashes from the local system. Common password hash files and databases include `%SystemRoot%\System32\config\SAM`, `%SystemRoot%\NTDS\NTDS.DIT` (the Active Directory credential store), and `/etc/shadow` (Linux machines). The threat actor could also use an on-path attack to capture a password hash transmitted during user authentication.

While the original string is not supposed to be recoverable, password-cracking software can be used to try to identify the password from the cryptographic hash. A password cracker uses two basic techniques:

- **Dictionary** - The software matches the hash to those produced by ordinary words found in a dictionary. This dictionary could include information such as user and company names, pet names, significant dates, or any other data that people might naively use as passwords. Enforcing strict password requirements and educating users on password protocols, such as not using any personal information, will help protect against these attacks. It is also recommended to use passphrases instead of passwords.
- **Brute force** - The software tries to match the hash against one of every possible combination it could be. If the password is short (under eight characters) and non-complex (using only lower-case letters, for instance), a password might be cracked in minutes. Longer and more complex passwords increase the amount of time the attack takes to run. The longer and more complex the password is, the computational power needed to crack it increases exponentially. The attacker can use any information they know about the password (such as exact length, known characters, etc) as masks to help speed up the cracking process. Figure 2. Hashcat password cracking utility

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Type........: NetNTLMv2
Hash.Target......: ADMINISTRATOR::515support:2f8cbd19fd1bfac9:881c5503...000000
Time.Started.....: Mon Jan  6 11:25:16 2020 (1 min, 38 secs)
Time.Estimated...: Sat Jan 11 07:49:57 2020 (4 days, 20 hours)
Guess.Mask.......: ?1?1?1?1?1?1?1?1 [8]
Guess.Charset....: -1 pPaAsSwWoOrRdD0123456789$, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   364.1 kH/s (11.09ms) @ Accel:128 Loops:32 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 34233472/152587890625 (0.02%)
Rejected.........: 0/34233472 (0.00%)
Restore.Point....: 2176/9765625 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:1824-1856 Iteration:0-32
Candidates.#1....: $87r8678 -> dSDoRS12
```

18.1.7 Cross-site Scripting Attacks

Many network services are now deployed as web applications. The HTTP/HTTPS web protocol is based on servers responding to client requests. A developer can extend the basic protocol with software code and information stored in databases to implement a dynamic web app, rather than simply returning static pages and graphics. A web application can use two methods of running code:

- Server-side code is run on the web server to process the request and build the response before it is sent to the client.
- Client-side code runs within the web browser software on the client machine to modify the web page before it is displayed to the user or to modify requests made to the server.

Most applications depend on user input. One of the most widespread vulnerabilities in web apps is failure to validate this input properly. For example, the user might need to sign in using an email address and password, so the web app presents two text-box fields for the user to input those values. If a threat actor can send a script via the username field and make the server or client execute that code, the web app has an input validation vulnerability.

Ensuring that the web app sanitizes user input, converts special characters into safe format before displaying it (output encoding), and implementing a Content Security Policy (CSP) will help prevent XSS attacks.

A **cross-site scripting** (XSS) attack exploits the fact that the browser is likely to trust scripts that appear to come from a site the user has chosen to visit. XSS attacks insert a malicious script that appears to be part of the trusted site. A non-persistent type of XSS attack would proceed as follows:

1. The attacker identifies an input validation vulnerability in the trusted site.
2. The attacker crafts a URL to perform code injection against the trusted site.
   This could be coded in a link to the attacker's site from the trusted site or a link in a phishing email message.

3. When the user opens the link, the trusted site returns a page containing the malicious code injected by the attacker.
   As the browser is likely to be configured to allow the site to run scripts, the malicious code will execute.

4. The malicious code could be used to deface the trusted site (by adding any sort of arbitrary HTML code), steal data from the user's cookies, try to intercept information entered in a form, or try to install malware.
   The crucial point is that the malicious code runs in the client's browser with the same permission level as the trusted site.
   This type of XSS attack is non-persistent because at no point is data on the web server changed. A stored/persistent XSS attack aims to insert code into a back-end database or content management system used by the trusted site. The threat actor may submit a post to a bulletin board with a malicious script embedded in the message, for instance. When other users view the message, the malicious script is executed.
   For example, with no input sanitization, a threat actor could type the following into a new post-text field:
   Check out this amazing website<script src="https://badsite.foo/hook.js"></script>
   Users viewing the post will have the malicious `script hook.js` execute in their browser.

18.1.8 SQL Injection Attacks

A web application is likely to use Structured Query Language (SQL) to read and write information from a database. SQL statements perform operations such as selecting data (SELECT), inserting data (INSERT), deleting data (DELETE), and updating data (UPDATE). In a **SQL injection** attack, the threat actor modifies one or more of these four basic functions by adding code to some input accepted by the app, causing it to execute the attacker's own set of SQL queries or parameters. If successful, this could allow the attacker to extract or insert information into the database or execute arbitrary code on the remote system using the same privileges as the database application.

For example, consider a web form that is supposed to take a name as input. If the user enters "Bob", the application runs the following query:

```
SELECT * FROM tbl_user WHERE username = 'Bob'
```

If a threat actor enters the string `' or 1=1--` and this input is not sanitized, the following malicious query will be executed:

```
SELECT * FROM tbl_user WHERE username = '' or 1=1--
```

The logical statement `1=1` is always true, and the `--` string turns the rest of the statement into a comment, making it more likely that the web application will parse this modified version and dump a list of all users.

The following techniques can be implemented to help prevent SQL Injection attacks:

- Input sanitization - removing special characters that can be used to manipulate SQL queries.
- Parameterized queries - User input is treated as data input and not executable code.
- Stored procedures - Pre-compiled SQL code that is stored on the server.

18.2 Wireless Security Protocols

Core 2 Exam Objectives Covered

- 2.3 Compare and contrast wireless security protocols and authentication methods.

After refreshing your knowledge of security threats and vulnerabilities, you were able to identify some potential issues in the company network. You have now been tasked with looking at the wireless networks employed at the company and identifying if there are any security threats and if so, mitigating them.

In this lesson, you will learn the different methods of securing the wireless network including data encryption methods, authentication methods, and enterprise-level wireless authentication methods.

Learning Outcomes

As you study this lesson, answer the following questions:

- Which wireless encryption method should be used with WPA2 and WPA3?
- What protocol is typically deployed with AES?
- What protocol replaced the 4-way handshake in WPA3?
- Which enterprise authentication method is typically used with wireless networks?

18.2.1 Wi-Fi Protected Access

Wireless LANs require careful configuration to make the connection and transmissions over the link secure. The main problem with wireless is that because it is unguided, there is no way to prevent anything within range from listening to the signals. If the wireless traffic is unencrypted, this could allow the interception of data or the unauthorized use of the network.

Temporal Key Integrity Protocol

The first version of Wi-Fi Protected Access was designed to fix critical vulnerabilities in the earlier wired equivalent privacy (WEP) standard. Like WEP, version 1 of WPA uses the RC4 symmetric cipher to encrypt traffic but adds a mechanism called the Temporal Key Integrity Protocol to try to mitigate the various attacks against WEP that had been developed.

TKIP helped to address the vulnerabilities in WEP, but TKIP was found to have its own share of vulnerabilities and has since been deprecated and replaced by the Advanced Encryption Standard (AES).

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is an encryption method that uses symmetric keys and block ciphers to encrypt data. This means that the data is divided into blocks of 128-bits and each block is encrypted independently.

AES replaced TKIP and is used to secure Wi-Fi networks including those using WPA2 and WPA3.

WPA2

Neither WEP nor the original WPA version is considered secure enough for continued use. Even with TKIP, WPA is vulnerable to various types of replay attacks that aim to recover the encryption key. WPA2 uses the advanced encryption standard (AES) cipher deployed within the Counter Mode with Block Chaining Message Authentication Code Protocol (CCMP). AES replaces RC4 and CCMP replaces TKIP. CCMP provides authenticated encryption, which is designed to make replay attacks harder.

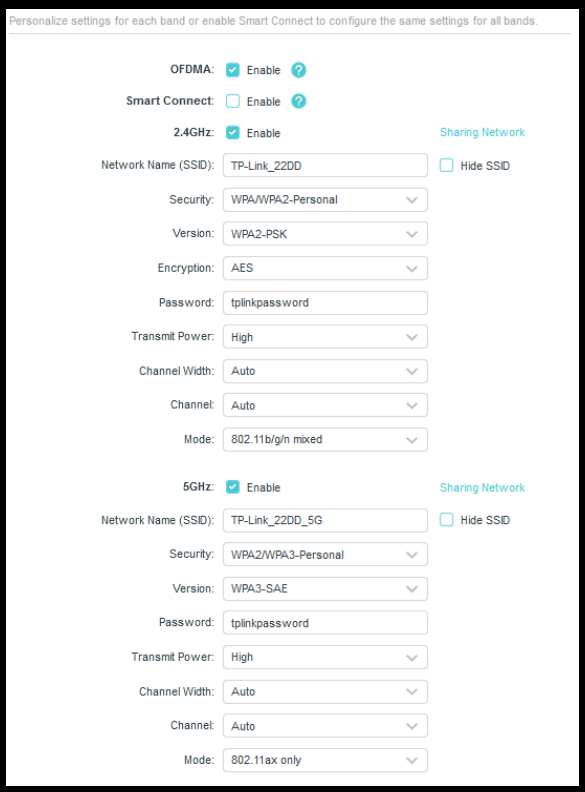
Note:

Some access points allow WPA2 to be used in WPA2-TKIP or WPA2-TKIP+AES compatibility mode. This provides support for legacy clients at the expense of weakening the security. It is better to select WPA2-AES.

WPA3

Weaknesses have also been found in WPA2, however, which has led to its intended replacement by WPA3. The main features of WPA3 are as follows:

- **Simultaneous Authentication of Equals (SAE) - WPA2 personal authentication uses a 4-way handshake with a preshared key (PSK) to allow a station to associate with an access point, authenticate its credential, and exchange a key to use for data encryption. The WPA2-PSK mechanism is vulnerable to manipulations that allow a threat actor to recover the key. WPA3 replaces WPA2-PSK with the more secure WPA3-SAE mechanism.**
- **Updated cryptographic protocols - WPA3 replaces AES CCMP with the stronger AES Galois Counter Mode Protocol (GCMP) mode of operation.**
- **Protected management frames - Management frames are used for association and authentication and disassociation and deauthentication messages between stations and access points as devices join and leave the network. These frames can be spoofed and misused in various ways under WPA and WPA2. WPA3 mandates use of encryption for these frames to protect against key recovery attacks and DoS attacks that force stations to disconnect.**
- **Wi-Fi Enhanced Open - An open Wi-Fi network is one with no passphrase. Any station can join the network. In WPA2, this also means that all traffic is unencrypted. WPA3 encrypts this traffic. This means that any station can still join the network, but traffic is protected against sniffing. Figure 1. Configuring a TP-LINK SOHO access point with wireless encryption and authentication settings**



Screenshot courtesy of TP-Link.

18.2.2 Wi-Fi Authentication Methods

Wi-Fi authentication comes in three types: open, personal, and enterprise. Within the personal authentication category, there are two methods: WPA2 pre-shared key (PSK) authentication and WPA3 Simultaneous Authentication of Equals.

WPA2 Pre-Shared Key Authentication

In WPA2, pre-shared key authentication uses a passphrase to generate the key that is used to encrypt communications. It is also referred to as group authentication because a group of users shares the same passphrase. When the access point is set to WPA2-PSK mode, the administrator configures a passphrase consisting of 8 to 63 characters. This is converted to a type of hash value, referred to as the pairwise master key (PMK). The same secret must be configured on each station that joins the network. The PMK is used as part of WPA2's 4-way handshake to derive various session keys.

All types of PSK authentication have been shown to be vulnerable to attacks that attempt to recover the passphrase. The passphrase must be at least 14 characters long to try to mitigate risks from cracking.

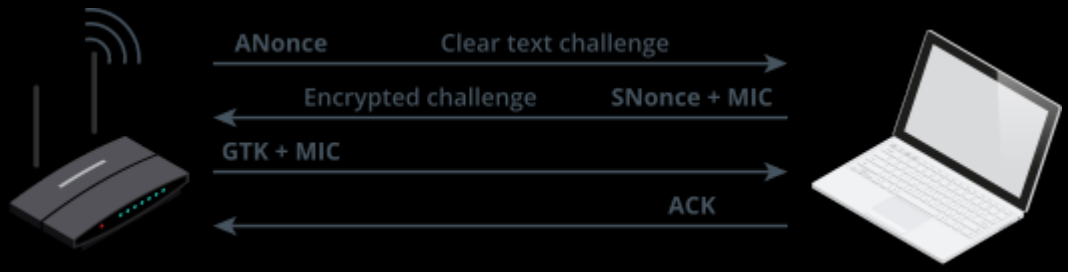


Figure 1. WPA2 4-Way Handshake

Description

WPA3 Personal Authentication

While WPA3 still uses passphrase-based group authentication of stations in personal mode, it changes the method by which this secret is used to agree session keys. In WPA3, the simultaneous authentication of equals (SAE) protocol replaces the PSK mechanism.

SAE uses a 128-bit key and perfect forward secrecy to authenticate. Perfect forward secrecy is a cryptography method that generates a new key for every transmission. This makes the handshake much more secure from hackers because if the hacker intercepts and cracks one of the messages, they still won't be able to crack the keys.

The configuration interfaces for access points can use different labels for these methods. You might see WPA2-Personal and WPA3-SAE rather than WPA2-PSK and WPA3-Personal, for example. Additionally, an access point can be configured for WPA3 only or with support for legacy WPA2 (WPA3-Personal Transition mode). Enabling compatibility supports legacy clients at the expense of weakening security.

18.2.3 Enterprise Authentication Protocols

The main problems with personal modes of authentication are that the distribution of the passphrase cannot be secured properly and that the access point administrator may choose an insecure passphrase. Personal authentication also fails to provide accounting because all users share the same credentials.

As an alternative to personal authentication, WPA's 802.1X enterprise authentication method implements the Extensible Authentication Protocol. EAP allows the use of different mechanisms to authenticate against a network directory. 802.1X defines the use of EAP over Wireless (EAPoW) to allow an access point to forward authentication data without allowing any other type of network access. It is configured by selecting WPA2-Enterprise or WPA3-Enterprise as the security method on the access point.

Enterprise authentication uses the following general workflow:

1. When a wireless station (a supplicant) requests an association, the AP enables the channel for EAPoW traffic only.
2. It passes the credentials submitted by the supplicant to an authentication, authorization, and accounting server on the wired network for validation. The AAA server (not the access point) determines whether to accept the credential.
3. When the user has been authenticated, the AAA server transmits a master key (MK) to the wireless PC or laptop. The wireless station and authentication server then derive the same pairwise master key (PMK) from the MK.
4. The AAA server transmits the PMK to the access point. The wireless station and access point use the PMK to derive session keys.

The enterprise authentication method means that the access point does not need to store any user accounts or credentials. They can be held in a more secure location on the AAA server. Another advantage of EAP is support for more advanced authentication methods than simple usernames and passwords. Strong EAP methods use a digital certificate on the server and/or client machines. These certificates allow the machines to establish a trust relationship and create a secure tunnel to transmit the user credential or to perform smart card authentication without a user password. This means the system is using strong multifactor authentication.

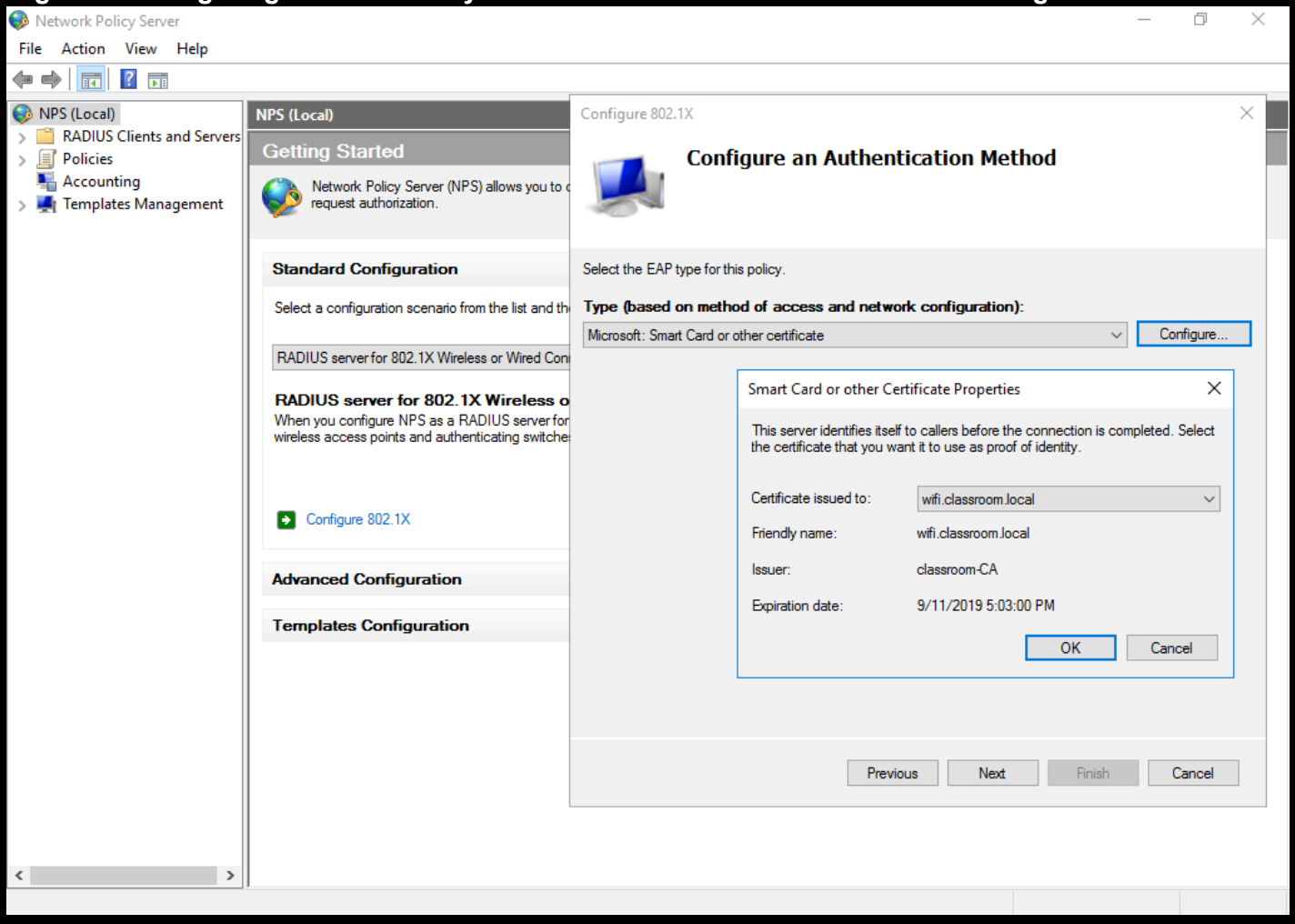
For example, EAP with Transport Layer Security (EAP-TLS) is one of the strongest types of multifactor authentication:

1. Both the server and the wireless supplicant are issued with an encryption key pair and digital certificate.
2. On the wireless device, the private key is stored securely in a trusted platform module (TPM) or USB key.
   The user must authenticate with the device using a PIN, password, or bio gesture to allow use of the key. This is the first factor.

3. When the device associates with the network and starts an EAP session, the server sends a digital signature handshake and its certificate.
4. The supplicant validates the signature and certificate and if trusted, sends its own handshake and certificate.
   This is the second factor.

5. The server checks the supplicant's handshake and certificate and authenticates it if trusted.

Figure 1. Configuring Network Policy Server to authenticate wireless clients using 802.1X EAP-TLS



Note:

Other methods of EAP use a certificate on the AAA server only. The AAA server uses the certificate to create an encrypted tunnel for the supplicant to send a username/password credential securely.

18.2.5 RADIUS, TACACS+, and Kerberos

Enterprise authentication uses an AAA server and network directory. These components can be implemented by several different protocols.

RADIUS

Remote Authentication Dial-in User Service is one way of implementing the AAA server when configuring enterprise authentication. The wireless access point is configured as a client of the RADIUS server. Rather than storing and validating user credentials directly, it forwards this data between the RADIUS server and the supplicant without being able to read it. The wireless access point must be configured with the host name or IP address of the RADIUS server and a shared secret. The shared secret allows the RADIUS server and access point to trust one another.

TACACS+

Terminal Access Controller Access Control System Plus is another way of implementing AAA. TACACS+ was developed by Cisco but is also supported on many third-party implementations. Where RADIUS is often used to authenticate connections by wireless and VPN users, TACACS+ is often used in authenticating administrative access to routers, switches, and access points.

Kerberos

In theory, an access point could allow a user to authenticate directly to a directory server using the Kerberos protocol. On Windows networks, Kerberos allows a user account to authenticate to a domain controller (DC) over a trusted local cabled segment. Kerberos facilitates single sign-on (SSO). As well as authenticating the user on the network, the Kerberos server issues authorization tickets that give the user account rights and permissions on compatible application servers.

In practice, there are no access points with direct support for Kerberos. Access points use RADIUS or TACACS+ and EAP to tunnel the credentials and tokens that allow a domain user connecting via a wireless client to authenticate to a DC and use SSO authorizations.

18.3 SOHO Router Security

Core 2 Exam Objectives Covered

- **2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.**

The company you work for is opening a small remote office. Since this office will only employ about 5 employees, it will only need a smaller SOHO network setup. You have been tasked with researching the best options to configure and secure the new SOHO network.

In this lesson, you will learn the key components of a SOHO network and how to secure these networks. This includes securing access to the management console, configuring the firewall, port-forwarding, and screening subnets.

Learning Outcomes

As you study this lesson, answer the following questions:

- **Typically, where should a SOHO router be physically placed?**
- **What are some of the key steps that should be taken when securing access to the router management interface?**
- **What is the purpose of the SSID?**
- **In what situation would you configure port-forwarding?**
- **What type of devices would typically be placed in a screened subnet?**

18.3.1 Home Router Setup

A small office home office (SOHO) LAN uses a single Internet appliance to provide connectivity. This appliance combines the functions of an Internet router, DSL/cable modem, Ethernet switch, and Wi-Fi access point. It can variously be described as a wireless router, SOHO router, or home router.

Physical Placement/Secure Locations

Ideally, the physical placement of any type of router or network appliance should be made to a secure location. A non-malicious threat actor could damage or power off an appliance by accident. A malicious threat actor could use physical access to tamper with an appliance or attach unauthorized devices to network or USB ports or use the factory reset mechanism and log on with the default password. On an enterprise network, such appliances are deployed in a locked equipment room and may also be protected by lockable cabinets.

In a home environment, however, the router must be placed near the minimum point of entry for the service provider's cabling. There is not always a great deal of flexibility in choosing a location that will make the router physically inaccessible to anyone other than the administrator. The home router will also usually implement the wireless network and therefore cannot be locked in a cabinet because clients would suffer from reduced signal strength.

If the user is experiencing weak signals throughout the site, Wi-Fi extenders can be used to mitigate the reduced signal strength.

Home Router Setup

To set up a new home router, first connect it to the Internet provider using the WAN port. This port is typically a different color or will be labeled as the WAN port. The port may use an RJ45 port for a full fiber connection, an RJ11 port for DSL, or an F-connector coax port for cable. Alternatively, the home router might need to be connected to an external digital modem. This connection will use a dual-purpose RJ45 port on the router labeled WAN/LAN. Many ISPs will provide a wireless router that has the modem built in as well.

Power on the router. Connect a computer to an RJ45 LAN port to start the home router setup process. The LAN ports will be a different color than the WAN port. Make sure the computer is set to obtain an IP address automatically. Wait for the Dynamic Host Configuration Protocol (DHCP) server running on the router to allocate a valid IP address to the computer.

Use a browser to open the device's management URL, as listed in the documentation. This could be an IP address or a host/domain name, such as http://192.168.0.1 or http://www.routerlogin.com. If you cannot connect, check that the computer's IP address is in the same range as the router's IP. You may need to manually configure the computer's IP address so it's in the same range.

Once you have accessed the router management interface, it is important to secure this access. If an unauthorized user can access the router's management interface, they can change all the settings and lock users out of the network.

The router management access should use HTTPS rather than unencrypted HTTP. If it is not, there should be a setting to enable this. Enabling remote access allows the router management to be accessed remotely while connected to the LAN (internal) side of the wireless network. There may also be a setting to allow remote access from the WAN (outside the network) side using SSH. If using remote access, you need to ensure that a secure protocol is being used.

The home router management software will prompt you to change the default password to secure the administrator account. Enter the default password (as listed in the documentation or printed on a sticker accompanying the router/modem). Choose a new, strong password of 12 characters or more. If there is also an option to change the default username of the administrator account, this is also a little bit more secure than leaving the default configured.

Internet Access and Static Wide Area Network IP

Most routers will use a wizard-based setup to connect to the Internet via the service provider's network. The WAN link parameters (full fiber, DSL, or cable) are normally self-configuring. You might need to supply a username and password. If manual configuration is required, obtain the settings from your ISP.

The router’s public interface IPv4 address is determined by the ISP. This must be an address from a valid public range. This is normally auto-configured by the ISP’s DHCP service.

Some Internet access packages assign a static IP or offer an option to pay for a static address. A static address might also be auto-configured as a DHCP reservation, but if manual configuration is required, follow the service provider’s instructions to configure the correct address on the router’s WAN interface.

When the Internet interface is fully configured, use the router’s status page to verify that the Internet link is up.

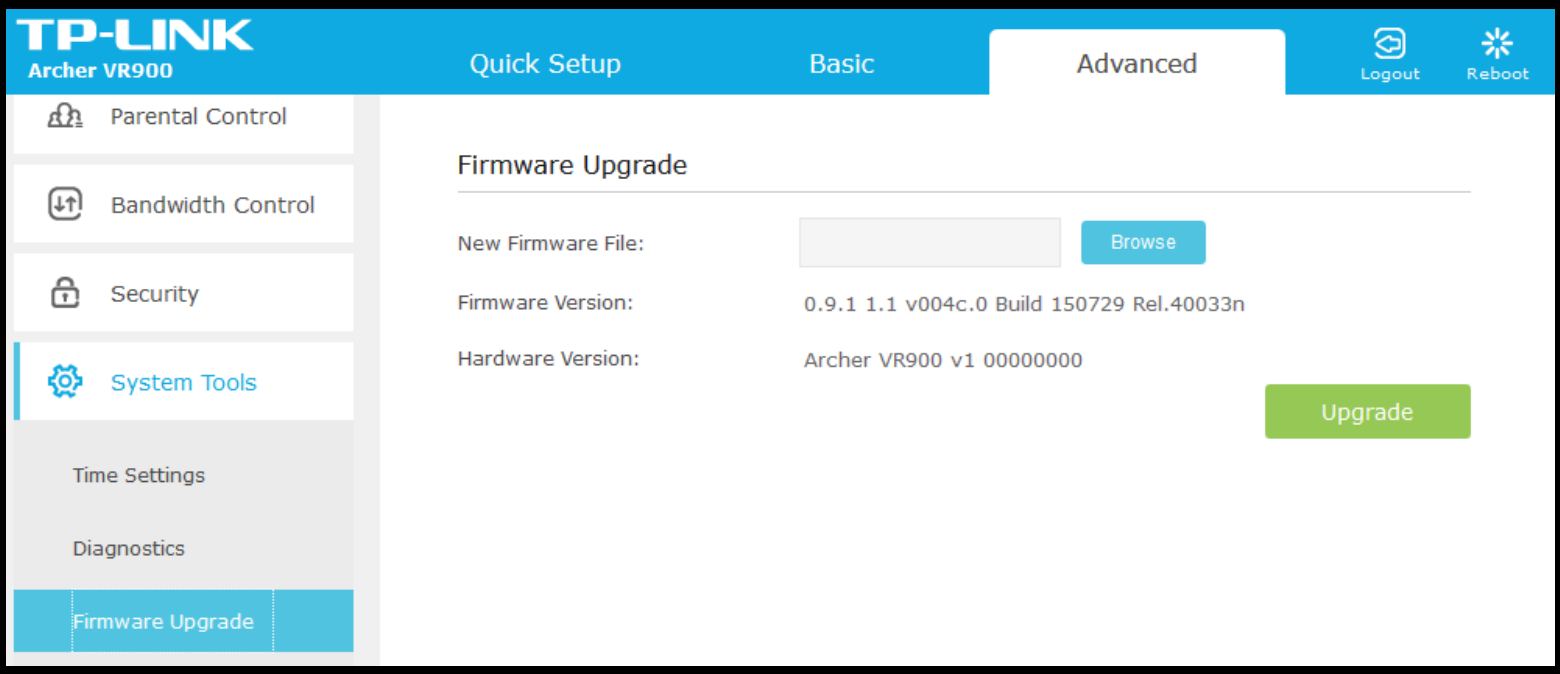
18.3.3 Firmware Update

You should keep the firmware and driver for the home router up to date with the latest patches. This is important because it allows you to fix security holes and support the latest security standards, such as WPA3. To perform a firmware update, download the update from the vendor's website, taking care to select the correct patch for your device make and model. In the management app, select the Firmware Upgrade option and browse for the firmware file you downloaded.

Many routers have the option to automatically download and install firmware updates which can simplify the process. If manually downloading and installing firmware updates, it is important to make sure that the firmware is only downloaded from the official website.

Make sure that power to the device is not interrupted during the update process.

Figure 1. Upgrading device firmware on a TP-LINK home router



Screenshot courtesy of TP-Link.

18.3.4 Home Router LAN and WLAN Configuration

A home router provides a one-box solution for networking. The WAN port facilitates Internet access. Client devices can connect to the local network via the RJ45 LAN ports or the appliance's access point functionality.

Service Set ID

The service set identifier is a simple, case-sensitive name by which users identify the WLAN. The factory configuration uses a default SSID that is typically based on the device brand or model. You should change it to something that your users will recognize and not confuse with nearby networks. Given that, on a residential network, you should not use an SSID that reveals personal information, such as an address or surname. Similarly, on a business network, you may not want to use a meaningful name. For example, an SSID such as "Accounts" could be a tempting target for an evil twin attack.

Wi-Fi analyzer tools can be used to identify nearby networks to avoid SSID conflicts and heavy congestion.

Disabling broadcast of the SSID prevents any stations not manually configured to connect to the name you specify from seeing the network. This provides a margin of privacy at the expense of configuration complexity.

Note:

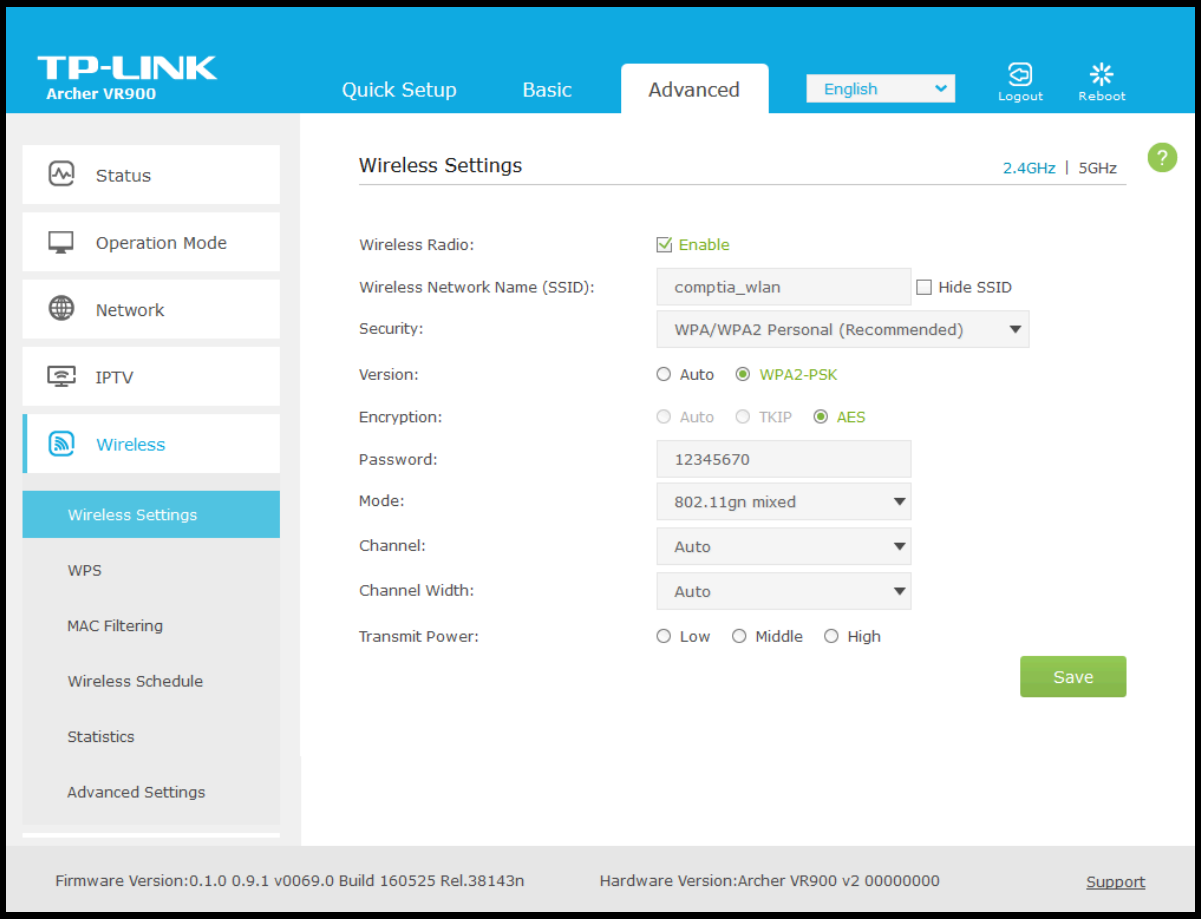
Hiding the SSID does not secure the network; you must enable encryption. Even when broadcast is disabled, the SSID can still be detected using packet sniffing tools and Wi-Fi analyzers.

Encryption Settings

The encryption or security option allows you to set the authentication mode. You should set the highest standard supported by the client devices that need to connect.

- Ideally, select WPA3. If necessary, enable compatibility support for WPA2 (AES/CCMP) or even WPA2 (TKIP). Remember that enabling compatibility weakens the security because it allows malicious stations to request a downgraded security type.

- Assuming personal authentication, enter a strong passphrase to use to generate the network key.
Figure 1. Configuring security settings on a TP-LINK home router



Screenshot courtesy of TP-Link.

Disabling Guest Access

Most home routers automatically configure and enable a guest wireless network which will allow clients to connect to the network and use the Internet. The guest network is usually isolated from the other local devices though. Use the option to disable guest access if appropriate.

Changing Channels

For each radio frequency band (2.4 GHz, 5 GHz, and 6 GHz), there will be an option to auto-configure or select the operating channel. If set to auto-detect, the access point will select the channel that seems least

congested. As the environment changes, you may find that this channel selection is not the optimum one. You can use a Wi-Fi analyzer to identify which channel within the access point's range is least congested.

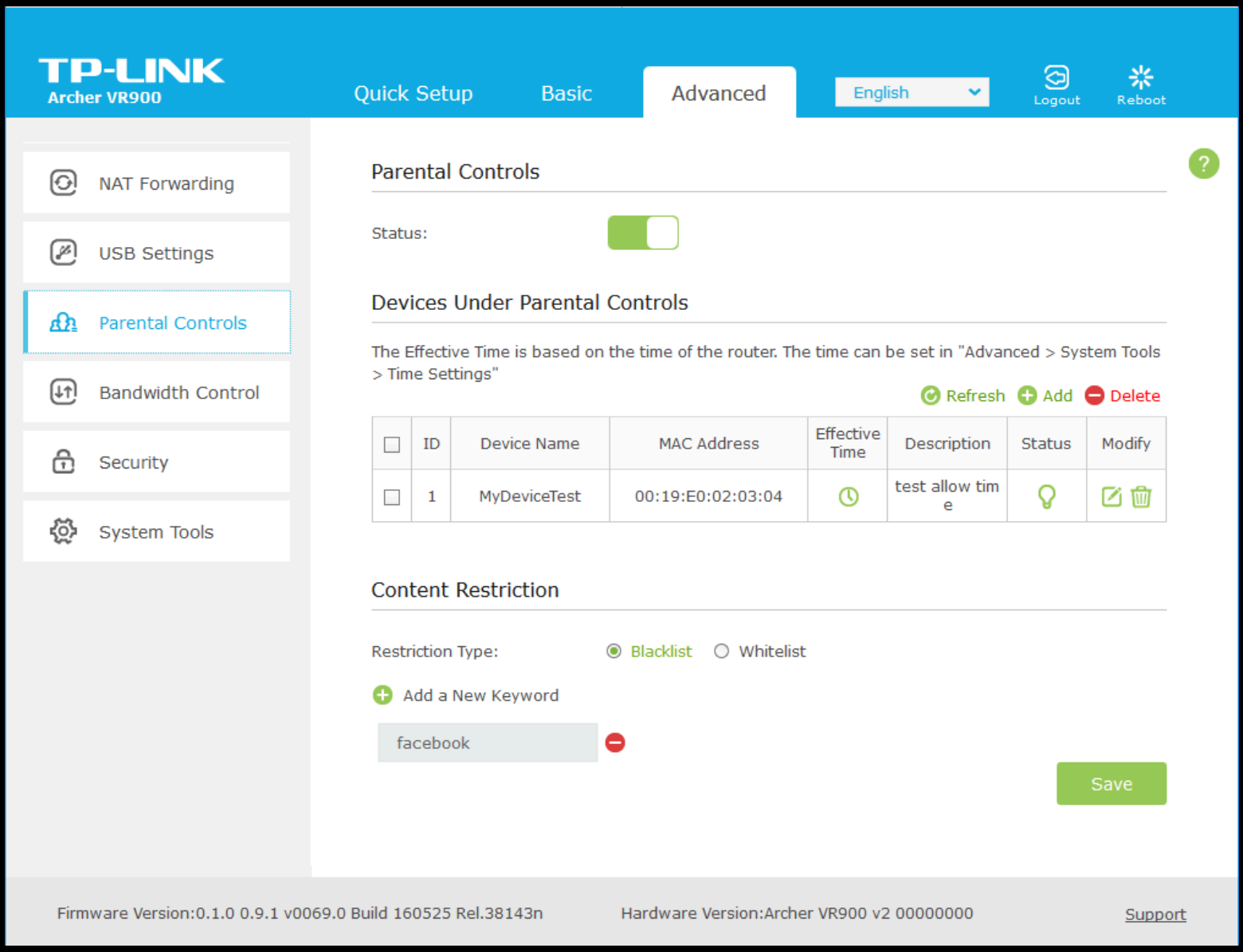
18.3.5 Home Router Firewall Configuration

All home routers come with at least a basic firewall, and some allow advanced filtering rules. Any firewall operates two types of filtering:

- **Inbound filtering determines whether remote hosts can connect to given TCP/UDP ports on internal hosts. On a home router, all inbound ports are blocked by default. Exceptions to this default block are configured via port forwarding.**
- **Outbound filtering determines the hosts and sites on the Internet that internal hosts are permitted to connect to. On a home router, outbound connections are allowed by default but can be selectively restricted via a content filter.**

Any packet-filtering firewall can allow or block traffic based on source and destination IP address filtering. Identifying which IP address ranges should be allowed or blocked and keeping those lists up to date is a complex task, however. Most home router firewalls implement content filtering instead. Content filtering means that the firewall downloads curated reputation databases that associate IP address ranges, FQDNs, and URL web addresses with sites known to host various categories of content and those associated with malware, spam, or other threats. The filters can also block URLs or search terms using keywords and phrases. There will be separate blocklists for different types of content that users might want to block.

Figure 1. Configuring parental control content-filtering to restrict when certain devices can access the network on a TP-LINK home router



Screenshot courtesy of TP-Link.

Another content-filtering option is to restrict the times at which the Internet is accessible. These are configured in conjunction with services offered by the ISP.

18.3.6 Home Router Port Forwarding Configuration

Where content filtering mediates outgoing access to the Internet, port forwarding allows Internet hosts to connect to computers on the local network. This is usually configured to support multiplayer games, but some home users might want to allow remote access to home computers or even run a web server.

Static IP Addresses and DHCP Reservations

To create a port-forwarding rule, you must identify the destination computer by IP address. This is not easy if the computer obtains its IP configuration via a normal DHCP lease. You could configure the host to use static addressing, but this can be difficult to manage.

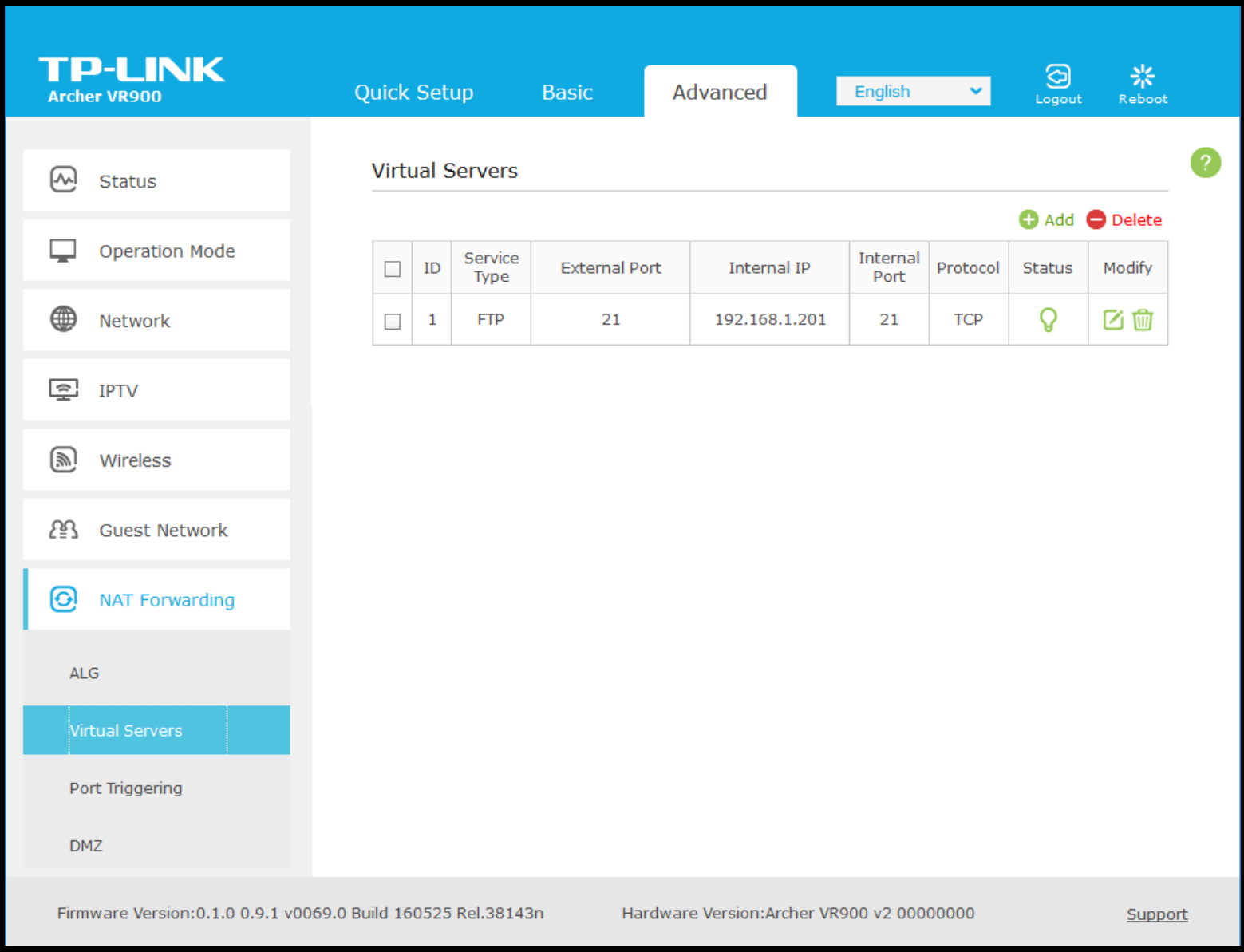
Another option is to create a dynamic host configuration protocol reservation for the device on the DHCP server. This means that the DHCP server always assigns the same IP address to the host. You can usually choose which IP address this should be. You need to input the MAC address of the computer in the reservation so that the DHCP server can recognize the host when it connects.

Configuring Port-Forwarding and Port-Triggering Rules

Hosts on the Internet can only "see" the router's WAN interface and its public IP address. Hosts on the local network are protected by the default block rule on the firewall. If you want to run some sort of server application from your network and make it accessible to the Internet, you must configure a port forwarding rule.

Port forwarding means that the router takes a request from an Internet host for a particular service (for example, the TCP port 25565 associated with a Minecraft server) and sends the request to a designated host on the LAN. The request could also be sent to a different port, so this feature is often also called port mapping. For example, the Internet host could request Minecraft on port 25565, but the LAN server might run its Minecraft server on port 8181.

Figure 1. Configuring port forwarding for FTP on a TP-LINK home router via its Virtual Servers feature



Screenshot courtesy of TP-Link.

Port-triggering is used to set up applications that require more than one port, such as file transfer protocol (FTP) servers. When the firewall detects activity on outbound port A destined for a given external IP address, it opens inbound access for the external IP address on port B for a set period.

Any changes to port forwarding rules should be documented so they can be changed back when they are no longer needed.

Disabling Unused Ports

One of the basic principles of hardened configuration is only to enable services that must be enabled. If a service is unused, then it should not be accessible in any way.

A home router operates a default block that stops any Internet host from opening a connection to a local port. Exceptions to this default block are configured as port-forwarding exceptions. If a port-forwarding rule is no longer required, it should either be disabled or deleted completely.

Some of the worst security vulnerabilities are caused by simple oversights. For example, you might enable a rule for a particular situation and then forget about it. Make sure you review the configuration of a home router every month.

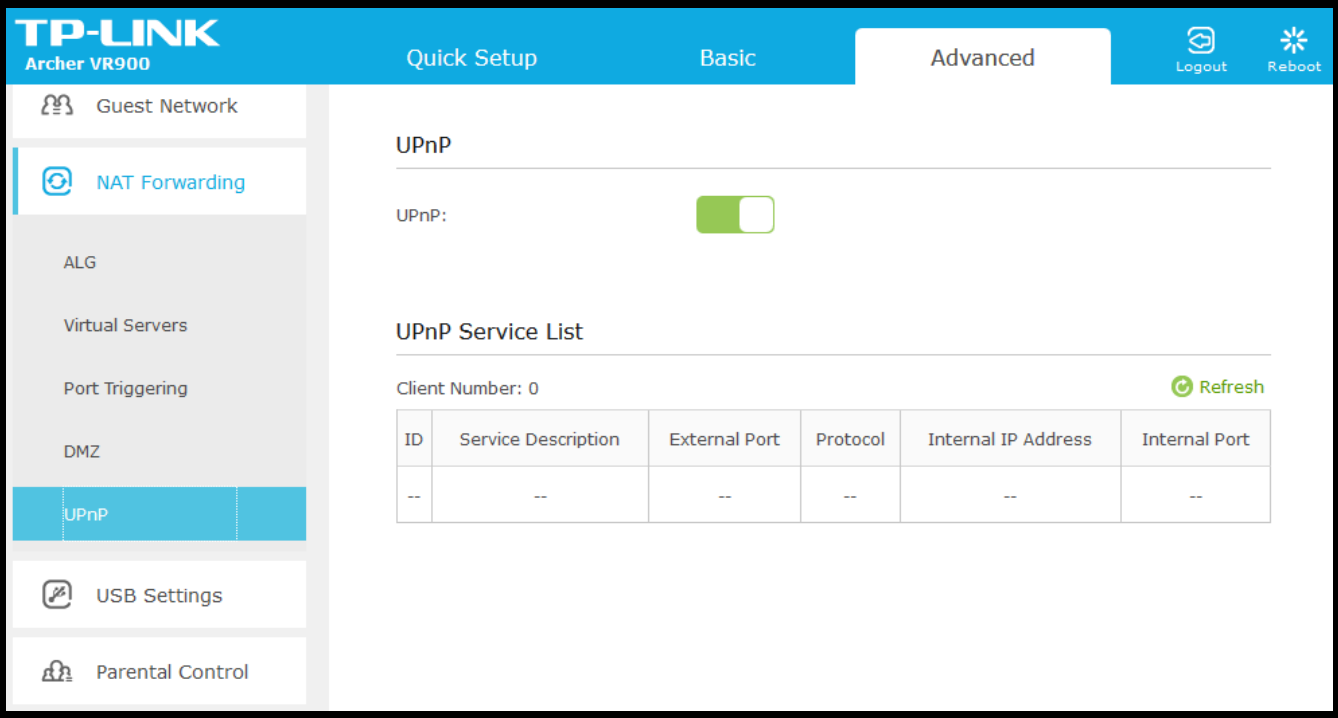
If supported by the home router, the outbound link can be made more secure by changing to a default block and allowing only a limited selection of ports. This involves considerable configuration complexity, however.

18.3.7 Universal Plug-and-Play

Port forwarding/port triggering is challenging for end users to configure correctly. Many users would simply resort to turning the firewall off to get a particular application to work. As a means of mitigating this attitude, services that require complex firewall configuration can use the Universal Plug-and-Play framework to send instructions to the firewall with the correct configuration parameters.

On the firewall, check the box to enable UPnP. A client UPnP device, such as an Xbox, PlayStation, or voice-over-IP handset, will be able to configure the firewall automatically to open the IP addresses and ports necessary to play an online game or place and receive VoIP calls.

Figure 1. There is nothing to configure when enabling UPnP, but when client devices use the service, the rules they have configured on the firewall are shown in the service list.



UPnP is associated with many security vulnerabilities and is best disabled if not required. You should ensure that the router does not accept UPnP configuration requests from the external (Internet) interface. If using UPnP, keep up to date with any security advisories or firmware updates from the router manufacturer.

Note:

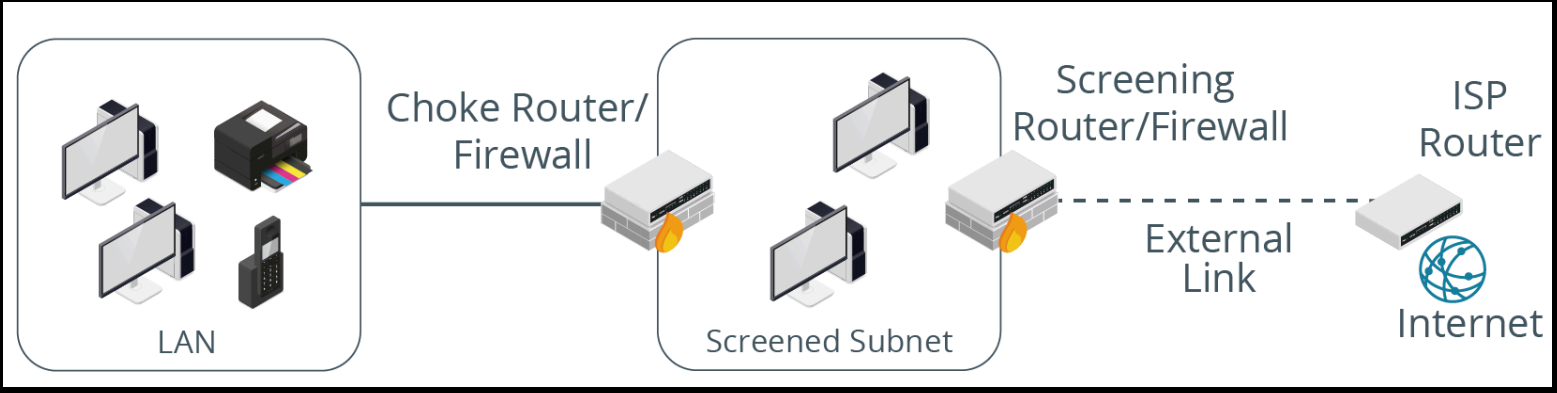
Also, make sure that UPnP is disabled on client devices unless you have confirmed that the implementation is secure. As well as game consoles, vulnerabilities have been found in UPnP running on devices such as printers and webcams.

18.3.8 Screened Subnets

When making a server accessible on the Internet, careful thought needs to be given to the security of the local network. If the server target of a port-forwarding rule is compromised, because it is on the local network there is the possibility that other LAN hosts can be attacked from it or that the attacker could examine traffic passing over the LAN.

In an enterprise network, a screened subnet is a means of establishing a more secure configuration. A screened subnet can also be referred to by the deprecated terminology demilitarized zone (DMZ). The idea of a screened subnet is that some hosts are placed in a separate network segment with a different IP subnet address range than the rest of the LAN. This configuration uses either two firewalls or a firewall that can route between at least three interfaces. Separate rules and filters apply to traffic between the screened subnet and the Internet, between the Internet and the LAN, and between the LAN and the screened subnet.

Figure 1. A screened subnet topology

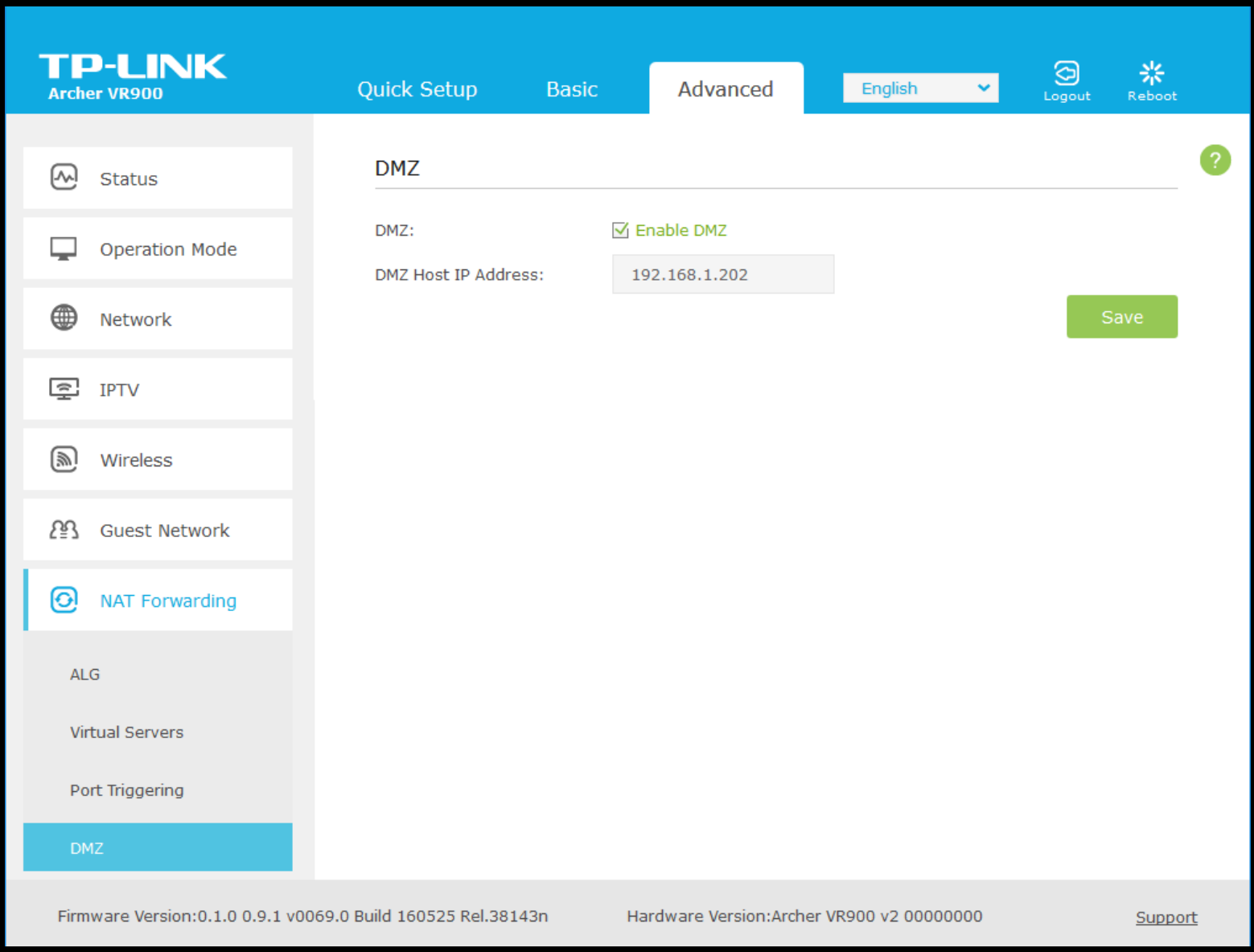


Images © 123RF.com.

Most home routers come with only basic firewall functionality. The firewall in a typical home router screens the local network rather than establishing a screened subnet.

However, you should be aware of the way that many home router vendors use the term DMZ. On a home router, a "DMZ" or "DMZ host" configuration is likely to refer to a computer on the LAN that is configured to receive communications for any ports that have not been forwarded to other hosts. When DMZ is used in this sense, it means "not protected by the firewall" as the host is fully accessible to other Internet hosts (though it could be installed with a host firewall instead). A computer should only be placed in the screened subnet if it has robust host-level security measures since it will not be protected by the firewall.

Figure 2. Configuring a home-router version of a DMZ—the host 192.168.1.202 will not be protected by the firewall



Screenshot courtesy of TP-Link.

18.4 Additional Security Measures

Core 2 Exam Objectives Covered

- **2.1 Summarize various security measures and their purposes**

You have impressed management with your grasp of network and wireless security. You have now been tasked with identifying any other potential security measures that should be taken.

In this lesson, you will learn the different types of physical access control, door locks, and alarm systems.

Learning Objectives

As you study this lesson, answer the following questions:

- **What security measures should be implemented to prevent tailgating or piggybacking?**
- **What type of door lock uses a user's physical characteristics to unlock the door?**
- **What type of lock is typically used to secure a laptop to a table?**
- **Which alarm system uses RFID tags?**

18.4.1 Physical Access Control

Physical security measures control who can access a building or a secure area of a building, such as a server room.

Perimeter Security

Perimeter security uses barricades, fences, lighting, and surveillance to control and monitor who can approach the building or campus. Sites where there is a risk of a terrorist attack will use barricades such as bollards (short vertical posts that are used to prevent vehicles from getting close to a building or sensitive area) and security posts to prevent vehicles from crashing into the building or exploding a bomb near it.

Security fencing needs to be transparent (so that guards can see any attempt to penetrate it), robust (so that it is difficult to cut), and secure against climbing (which is generally achieved by making it tall and possibly by using razor wire). Fencing is generally effective, but the drawback is that it gives a building an intimidating appearance. Buildings that are used by companies to welcome customers or the public may use more discreet security methods.

Access Control Vestibules

From the site perimeter, people should enter and leave the building through defined entry and exit points. There may be a single entrance or separate entrances for visitors and for staff. The main problem with a simple door as an entry mechanism is that it cannot accurately record who has entered or left an area. More than one person may pass through the gateway at the same time; a user may hold a door open for the next person; an unauthorized visitor may tailgate behind an authorized employee.

This risk may be mitigated by installing a turnstile or an access control vestibule. An access control vestibule is where one gateway leads to an enclosed space protected by another barrier. This restricts access to one person at a time.

Magnetometers

Surveillance at the building entrance might be enhanced by deploying a walk-through or handheld magnetometer. This type of metal detector is often deployed at airports and in public buildings to identify concealed weapons or other items.

Security Guards

Human security guards can be placed in front of and around a location to protect it. They can monitor critical checkpoints and verify identification, allow or disallow access, and log physical entry occurrences. They also

provide a visual deterrent and can apply their own knowledge and intuition to mitigate potential security breaches.

18.4.3 Lock Types

A door lock controls entry and exit from a building, room, or another area without necessarily needing a guard, depending on the risk of tailgating and piggybacking being an issue.

Door Lock Types

Door locks can be categorized as follows:

- **Key operated - A conventional lock prevents the door handle from being operated without the use of a key.**
- **Electronic - Rather than a key, the lock is operated by entering a PIN on an electronic keypad.**
- **Badge reader - Some types of electronic locks work with a hardware token rather than a PIN. The token might be a basic magnetic swipe card. A more advanced type of lock works with a cryptographic contactless smart card or key fob . These are much more difficult to clone than ordinary swipe cards.**
- **Mobile digital key - Instead of a physical key, this is a virtual key that resides on the user's smartphone. The door lock will use a technology such as Bluetooth or NFC to communicate with the user's device. Typically, the user will open an app on the smartphone and when in range, they can send the command to open the lock.**

Biometric Door Locks

Some types of electronic locks use a biometric scanner so that the lock can be activated by a bio gesture:

- **Fingerprint reader - This is usually implemented as a small capacitive cell that can detect the unique pattern of ridges making up the fingerprint. The technology is also nonintrusive and relatively simple to use, although moisture or dirt can prevent readings, and there are hygiene issues at shared-use gateways.**
- **Palmprint scanner - This is a contactless type of camera-based scanner that uses visible and/or infrared light to record and validate the unique pattern of veins and other features in a person's hand. Unlike facial recognition, the user must make an intentional gesture to authenticate.**
- **Retina scanner - An infrared light is shone into the eye to identify the pattern of blood vessels. The arrangement of these blood vessels is highly complex and typically does not change from birth to death, except in the event of certain diseases or injuries. Retinal scanning is therefore one of the most accurate forms of biometrics. Retinal patterns are very secure, but the equipment required is expensive and the process is relatively intrusive and complex. False negatives can be produced by diseases such as cataracts.**
- **Facial Recognition - When the user approaches the door, a built-in camera captures their image. This image is then compared with stored templates that were previously enrolled. If the match is found, the door will unlock. This type of biometrics is extremely secure, fast, and accurate, but is costly to implement.**

- **Voice Recognition - Users program the door lock to open with a specific command which is recorded and analyzed to create a unique voiceprint. When the user approaches the door and speaks the command, the lock will unlock if the voiceprint matches. This method works great for users with limited mobility or when their hands are full. While voice recognition technology has gotten better, it can be affected by background noises, voice changes (such as the user having a cold), and malicious users mimicking a valid user's voice. To increase security, many of these systems will also require the user to speak a passcode along with the unlock command.**

Other general issues with biometrics include privacy issues with capturing and storing personal information and discriminatory issues involving people who cannot make the required bio gesture.

Equipment Locks

There are several types of equipment lock that act to prevent unauthorized physical access to servers and network appliances or prevent theft:

- **Kensington locks are used with a cable tie to secure a laptop or other device to a desk or pillar to prevent theft.**
- **Chassis locks and faceplates prevent the covers of server equipment from being opened. These can prevent access to external USB ports and prevent someone from accessing the internal fixed disks.**
- **Lockable rack cabinets control access to servers, switches, and routers installed in standard network racks. These can be supplied with key-operated or electronic locks.**

18.4.4 Alarms and Surveillance

When designing premises security, you must consider the security of entry points that could be misused, such as emergency exits, windows, hatches, grilles, and so on. These may be fitted with bars, locks, or alarms to prevent intrusion. Also consider pathways above and below, such as false ceilings and ducting. There are four main types of alarm system:

- Circuit - A circuit-based alarm sounds when the circuit is opened or closed, depending on the type of alarm. This could be caused by a door or window opening or by a fence being cut.
- Motion sensor - A motion-based alarm is linked to a detector triggered by movement within a room or other area. The sensors in these detectors are either microwave radio reflection (radar, for example) or passive infrared (PIR), which detects moving heat sources.
- Proximity - Radio frequency ID (RFID) tags and readers can be used to track the movement of tagged objects within an area. This can form the basis of an alarm system to detect whether someone is trying to remove equipment.
- Duress - This type of alarm is triggered manually by staff if they come under threat. A duress alarm could be implemented as a wireless pendant, concealed sensor or trigger, or call contact. Some electronic entry locks can also be programmed with a duress code that is different from the ordinary access code. This will open the gateway but also alert security personnel that the lock has been operated under threat.

Video surveillance is typically a second layer of security designed to improve the resilience of perimeter gateways. Surveillance may be focused on perimeter areas or within security zones themselves. This type of surveillance can be implemented with older-style CCTV (closed-circuit television) or with IP cameras. The surveillance system may be able to use motion detection or even facial recognition to alert staff to intrusion attempts.

Security lighting is important in contributing to the perception that a building is safe and secure at night. Well-designed lighting helps to make people feel safe, especially in public areas or enclosed spaces, such as parking garages. Security lighting also acts as a deterrent by making intrusion more difficult and surveillance (whether by camera or guard) easier. The lighting design needs to account for overall light levels, the lighting of particular surfaces or areas (allowing cameras to perform facial recognition, for instance), and avoiding areas of shadow and glare.

19.0 Managing Security Settings

Firewalls provide a security border around a network, but this secure border is not sufficient to protect against insider threats, advanced malware, or sophisticated threat-actor tactics and techniques. Most organizations deploy defense in depth controls to ensure that each endpoint—computer, laptop, smartphone, or tablet—is deployed in a hardened configuration in terms of both the OS and the web browser software.

Despite best efforts to assess risks and deploy countermeasures, most networks will suffer from security incidents. As an IT specialist, you will need to be able to use best practice methods and tools to identify and eliminate malware and other intrusions to minimize the impact of these incidents.

Prepare for A+ Core 2 by:

- **Configuring workstation security.**
- **Configuring browser security.**
- **Troubleshooting workstation security issues.**

19.1 Account Security

Core 2 Exam Objectives Covered

- **2.7 Given a scenario, apply workstation security options and hardening techniques.**

Security of your accounts is critical to ensure your personal information is kept safe from unauthorized access. This is also true when it comes to corporate-owned data and information. Ensuring your accounts are protected using best practices for passwords and the use of strong encryption are fundamentals of the security sector of IT. Let's think about the information you store on your smartphone or computer. Personal emails, photos, and even financial information are readily available for you to access when necessary. Now let's say an unauthorized user was to get a hold of that device, what information and data would they have access to? How could the unauthorized access or potential disclosure of your information affect your life? This lesson will examine several basic security principles that apply to both personal and corporate accounts.

Learning Objectives

As you study this lesson, answer the following questions:

- **What considerations should be made when selecting a password?**
- **How does encryption of your data make it more difficult to access?**
- **What best practices should be enabled on your personal accounts? Are they the same for corporate accounts?**
- **What methods can be used to restrict access to the system and the data it contains?**
- **What applications manage security policies in an Active Directory environment?**

19.1.1 Password Best Practices

One of the first pillars of workstation security is ensuring that only authorized users can operate the computers connected to the network. Effective user security depends on strong credential management, effective account policies, and best practice end-user behavior.

Password-based authentication systems have a long history of vulnerability. Some of this ineffectiveness is due to inadequate technologies and some is due to poor user password practice. As not all companies can make the switch to multifactor sign-in, password best practice is still a key security requirement.

The biggest vulnerability of knowledge factor authentication to cyberattacks is the use of weak passwords. A threat actor might use dictionary files containing popular words and phrases or strings from breached password databases to compromise account credentials. Once a threat actor obtains a password, she or he can gain access to a system posing as that person.

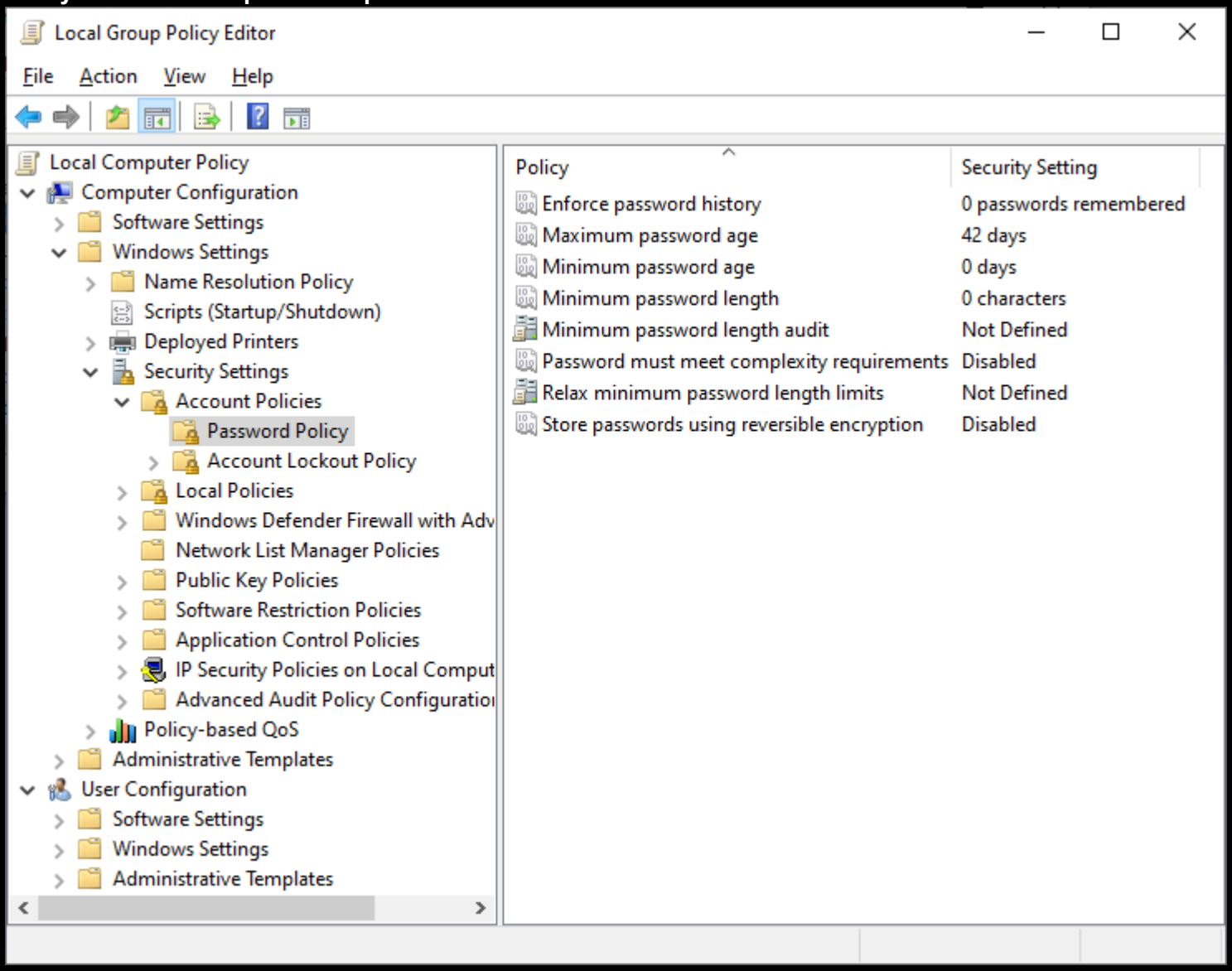
Password Rules

The following rules are easy for users to apply and make passwords more difficult to crack:

- **Make the password sufficiently long—12+ character length is suitable for an ordinary user account. Administrative accounts should have longer passwords.**
- **Choose a memorable phrase, but do not use any personal information— Anything that a threat actor could discover or guess should not be used in a password. This includes things such as significant dates, family names, usernames, job titles, company names, pet names, quotations, and song lyrics. Set a unique password for each account you set up.**

Some password policies impose complexity requirements beyond minimum length. Rules might specify that the password must contain a given mix of character types: uppercase and lowercase letters, numbers, and symbols. A password policy may have an expiration requirement, which means that the user must change the password after a set period. This is sometimes referred to as password age. Figure 1. Using the local Group

Policy editor to view password policies



Screenshot courtesy of Microsoft.

Description

The password policy folder under the folders account policies and security settings is selected from the menu on the left. The table lists the policy and security setting.

Character complexity and expiration are deprecated by some standards bodies. These rules can make it harder for users to select good passwords and encourage poor practice, such as writing the password down.

19.1.3 End User Best Practices

Good password practice should be supplemented with secure use of the workstation. Some key principles are as follows:

- **Log off when not in use— A lunchtime attack is where a threat actor can access a computer that has been left unlocked. Policies can configure screensavers that lock the desktop after a period of inactivity. Users should not depend on these, however. In Windows, START+L locks the desktop. Users must develop the habit of doing this each time they leave a computer unattended.**
- **Secure/protect critical hardware (such as laptops)— Users must also be alert to the risk of physical theft of devices. Portable computers can be secured to a desk using a cable lock, sometimes known as a Kensington lock. When in public, users must keep laptop cases in sight.**
- **Secure personally identifiable information (PII) and passwords— Paper copies of personal and confidential data must not be left where they could be read or stolen. A clean desk policy ensures that all such information is not left in plain sight. Also, this type of information should not be entered into unprotected plain text files, word processing documents, or spreadsheets.**
- **Use password managers— Password managers are usually software applications that make it easy to store passwords on a device. Some password manager applications also can generate unique passwords when needed. This can make setting a password for a new account easier.**

  Note:

  Personal data is typically protected by regulations and legislation. Making any sort of unauthorized copy of this data is often illegal. It should only typically be stored and processed in systems that are configured and monitored by a data owner.

19.1.4 Restrict User Permissions

Account management policies are used to determine what rights and privileges each employee should be assigned. These policies should be guided by the principle of least privilege.

An operating system's access control system assigns two types of permissions to a user account:

- **File permissions control whether a user can read or modify a data file or folder, either on the local PC or across the network. Configuring file permissions is the responsibility of the data owner or file server administrator.**
- **Rights or privileges control what system configuration changes a user can make to a PC. Configuring rights is the responsibility of the network owner.**

Some networks have complex requirements for assigning rights, but the basic principle is that the number of accounts with administrator/superuser privileges should be as few as possible. These highly privileged accounts should be further protected by features such as UAC and sudo. For both file permissions and rights, a system of least privilege will be most effective in reducing risk. Users should be given sufficient access to complete their job tasking; nothing more, nothing less.

19.1.5 Change Default Administrator Account and Password

The root or superuser in Linux or the Administrator user account in Windows is the default system owner. These default accounts have no practical limitations and consequently are the ultimate target for threat actors. In many cases, these default accounts are disabled during the OS installation, and their privileges are exercised by named administrator accounts using tools such as UAC and sudo.

If the default administrator account cannot be disabled, it must never be left configured with a default password. The new password must be treated with the highest level of security available. Ideally, the password should be known by a limited number of people. Sharing administrative passwords is a security risk.

Any use of the default administrator account must be logged and accounted for. Using this account for sign-in should be an unusual event that generates an alert. For separation of duties, the person operating the default administrator account must not be able to disable this accounting.

19.1.6 Disable Guest Account

A guest account allows unauthenticated access to the computer and may provide some sort of network access too. In current versions of Windows, the Guest account is disabled by default and cannot be used to sign-in. It is only enabled to facilitate password-less file sharing in a Windows workgroup. You should monitor other operating systems and features such as guest Wi-Fi and disable them if they do not comply with security policies.

19.1.7 Account Policies

Account policies supplement best practice behavior by enforcing requirements as controls imposed by the OS. On a standalone workstation, password and account policies can be configured via the Local Security Policy snap-in (`secpol.msc`) or the Group Policy Editor snap-in (`gpedit.msc`). On a Windows domain network, settings can be defined as group policy objects (GPO) and applied to groups of user and computer accounts within domains and organizational units (OUs).

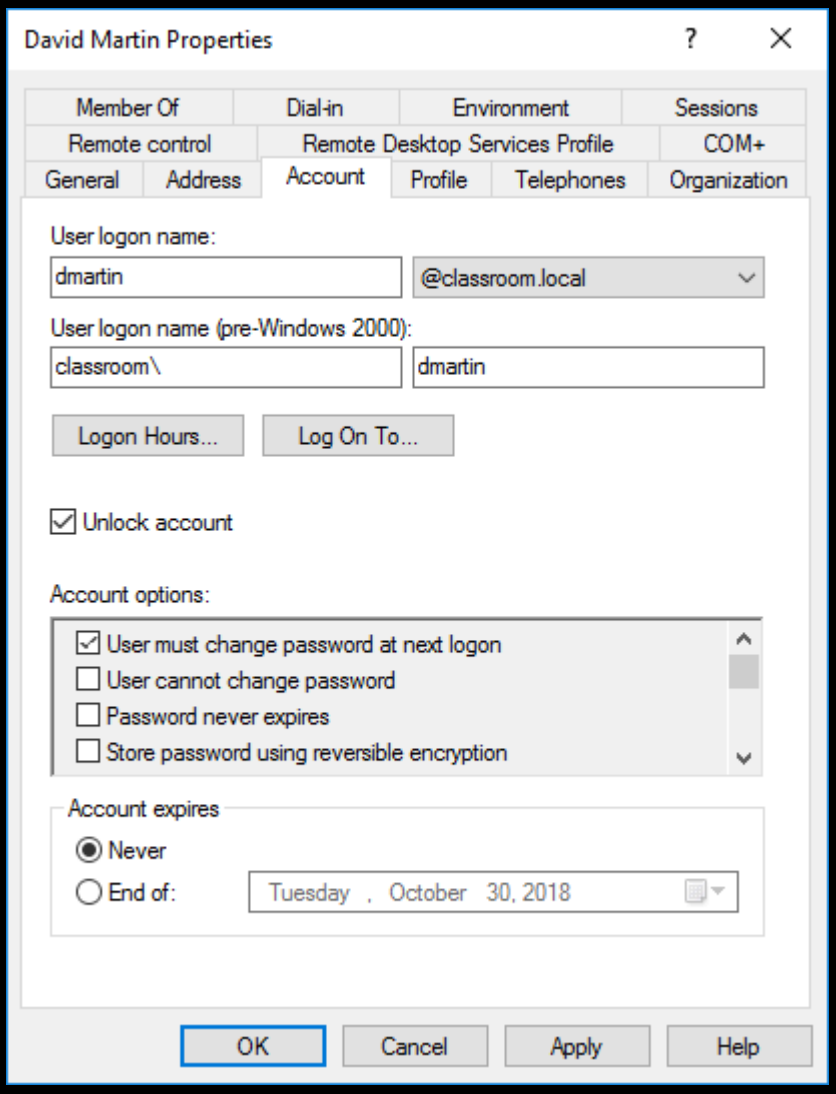
Note:

These tools are not available in the Home edition of Windows.

- **Restrict login times— This is typically used to prevent an account from logging in at an unusual time of the day or night or during the weekend. Periodically, the server checks whether the user has the right to continue using the network. If the user does not have the right, then an automatic logout procedure commences.**
- **Account expiration— You may also want to set an expiration date and time on accounts. This will automatically disable the account so it cannot be used beyond the timeframe allowed.**
- **Failed attempts lockout— This specifies a maximum number of incorrect sign-in attempts within a certain period. Once the maximum number of incorrect attempts has been reached, the account will be disabled. This mitigates the risk of threat actors gaining system access using lists of possible passwords.**
- **Concurrent logins— This sets a limit to the number of simultaneous sessions a user can open. Most users should only need to sign in to one computer at a time, so this sort of policy can help to prevent or detect misuse of an account.**
- **Use timeout/screen lock— This locks the desktop if the system detects no user-input device activity. This is a sensible, additional layer of protection. However, users should not rely on this and must lock the computer manually when leaving it unattended.**

If a user account violates a security policy, such as an incorrect password being entered repeatedly, it may be locked against further use. The account will be inaccessible until it is unlocked by setting the option in the Properties dialog box on the Account tab.

Figure 1. Using the Properties dialog box to unlock a user account



Screenshot courtesy of Microsoft.

If a user forgets a password, you can reset it by right-clicking the account and selecting Reset Password.

19.1.8 Unused Services

Services are used by the operating system and hardware to increase the functionality of the computer. Some services you may be familiar with may include update services, file and print services, and even network services like DHCP and DNS.

While some services are essential for the operation of the system, others may not need to be running on your system. For example, if you are not connecting to a Bluetooth or NFC device, you should disable those related services until you do need them. Another example is if you are not executing a file transfer, you should disable the file transfer services like FTP or SSH because they are not necessary.

On smartphones or tablets, you may want to turn off auto update services or remote connection services to prevent unauthorized access to your system through the Bluetooth or cellular connection. Only activate or enable services that are required when you need them.

19.2 Workstation Security

Core 2 Exam Objectives Covered

- **2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.**
- **2.7 Given a scenario, apply workstation security options and hardening techniques.**

Security of workstations can easily prevent unauthorized access issues for the data, information, and network the system is connected to. It goes beyond just ensuring no unauthorized persons are physically using the workstation and includes the logical use of the system and its resources as well. From ensuring the system is free from malware and the data and information on the hard drive are protected using encryption, the security of the workstation can easily be achieved by following best practices from the industry.

Learning Objectives

As you study this lesson, answer the following questions:

- **What protections does the Windows Defender application provide to a workstation?**
- **What type of firewall is Windows Defender Firewall?**
- **What encryption programs are available within the Windows operating system environment?**

19.2.1 Execution Control

Authentication and authorization policies give subjects the right to sign on to a computer and network and (potentially) to make changes to the system configuration. This places a certain amount of trust in the user to exercise those rights responsibly. Users can act maliciously, though, or could be tricked into an adverse action. Execution control refers to logical security technologies designed to prevent malicious software from running on a host regardless of what the user account privileges allow. Execution control can establish a security system that does not entirely depend on the good behavior of individual users.

Even when logged in as an administrator account, Windows requires a confirmation when making certain changes to a system. This is a part of the User Account Control system. When running an application, the application will be run as the user who is logged in. A user may need to execute a program by using the Run As Administrator option. Run As Administrator allows a standard user account to run a program or utility with administrative privileges. The user will be required to provide the administrative account password when the Run As Administrator option is selected. This assists with execution control of applications and making changes to the workstation.

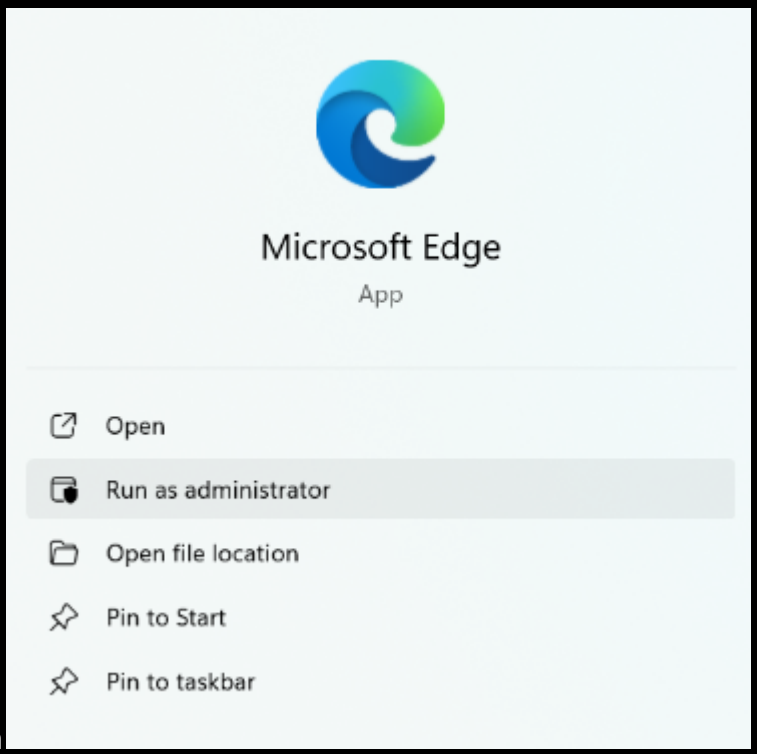


Figure 1. Run As Administrator menu option

Screenshot courtesy of Microsoft.

19.2.2 Trusted/Untrusted Software Sources

To prevent the spread of malware such as Trojans, it is necessary to restrict the ability of users to run unapproved program code, especially code that can modify the OS, such as an application installer. Windows uses the system of Administrator and Standard user accounts, along with User Account Control (UAC) and system policies, to enforce these restrictions.

Developers of Windows applications can use digital certificates to perform code signing and prove the authenticity and integrity of an installer package. Linux also prompts when you attempt to install untrusted software. Software is signed with a cryptographic key. Packages need the public key for the repository to install the software. When prompted that you are installing untrusted software, you can either respond that you want to install it anyway or cancel the installation.

Mobile OS vendors use this "walled garden" model of software distribution as well. Apps are distributed from an approved store, such as Apple's App Store or the Windows Store. The vendor's store policies and procedures are supposed to prevent any Trojan-like apps from being published.

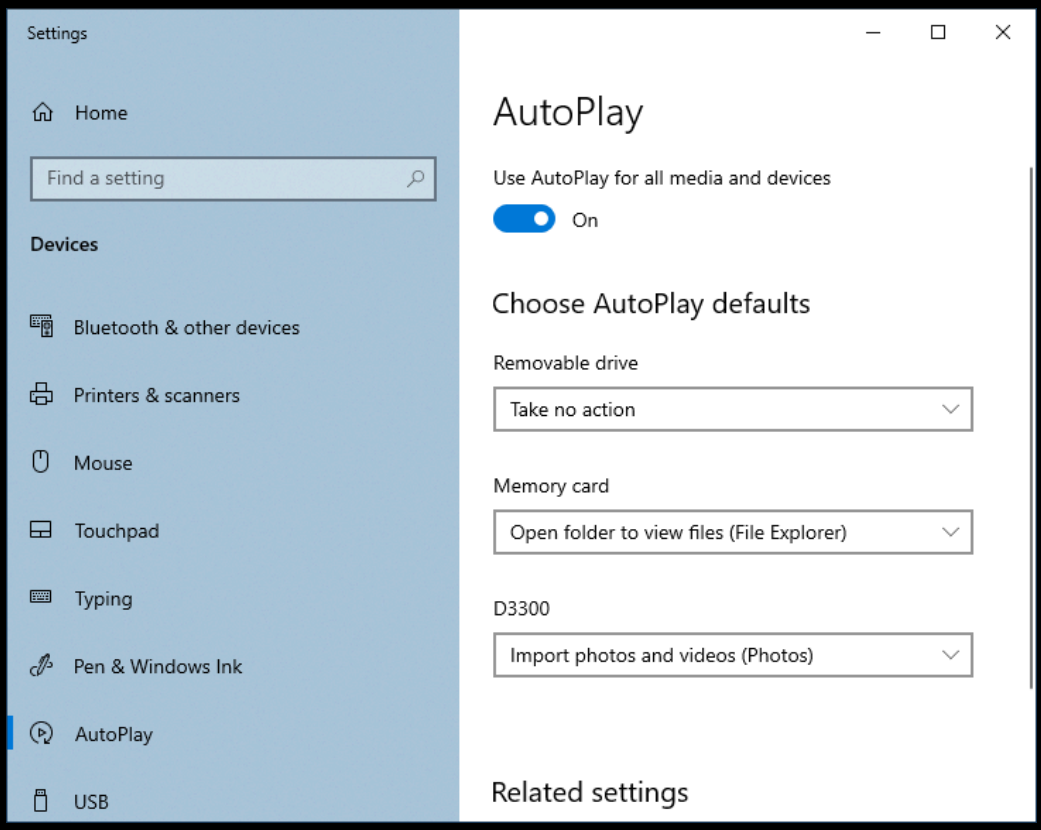
There are also third-party network management suites to enforce application control. This means configuring block lists of unapproved software (allowing anything else) or allow lists of approved software (denying anything else).

19.2.3 AutoRun and AutoPlay

One of the problems with legacy versions of Windows is that when an optical disc is inserted or a USB drive is attached, Windows would automatically run commands defined in an autorun.inf file stored in the root of the drive. A typical autorun.inf would define an icon for a disk and the path to a setup file. This could lead to malware being able to install itself automatically. Disabling the autorun/autoplay option would prevent this from occurring.

In modern versions of Windows, an AutoPlay dialog box is shown, prompting the user to take a particular action. AutoRun and AutoPlay settings can be configured via a drive's property dialog box. Also, UAC will require the user to explicitly allow any executable code to run. There is a Windows Settings page to configure default AutoPlay actions.

Figure 1. Configuring AutoPlay. D3300 is a digital camera that has been connected to the computer previously



Screenshot courtesy of Microsoft.

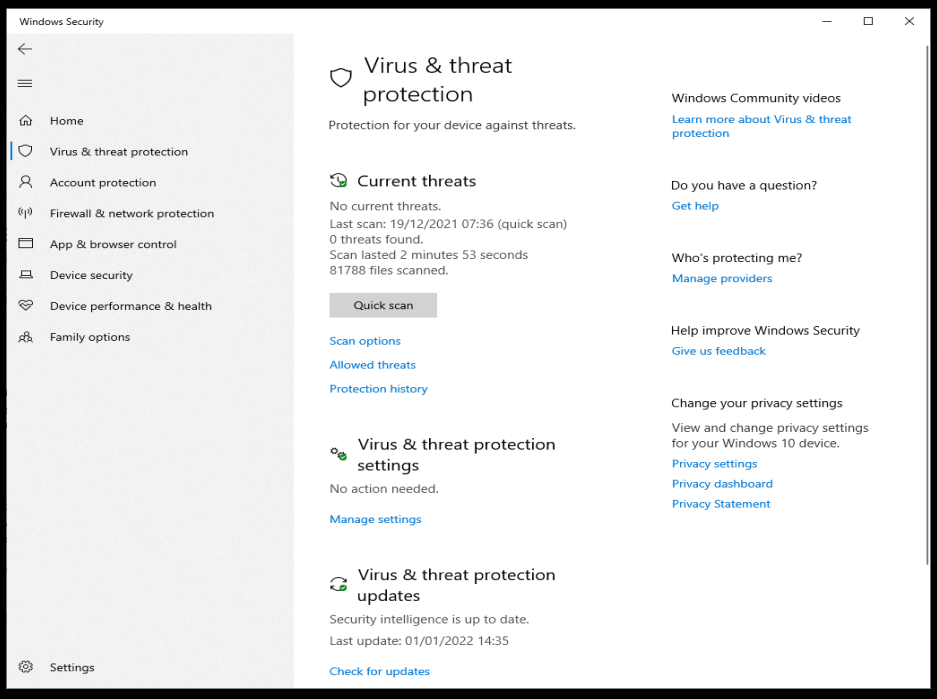
19.2.4 Windows Defender Antivirus

Even with UAC and execution control, there are still plenty of ways for malware to install onto a PC. A program might use particularly effective social engineering techniques to persuade the user to bypass the normal checks. The malware might exploit a vulnerability to execute without explicit consent. Malware might also not need to install itself to achieve threat-actor objectives, such as exfiltrating data, weakening the system configuration, or snooping around the network.

Antivirus (AV) is software that can detect malware and prevent it from executing. The primary means of detection is to use a database of known virus patterns called definitions, signatures, or patterns. Another technique is to use heuristic identification. "Heuristic" means that the software uses knowledge of the sort of things that viruses do to try to spot (and block) virus-like behavior. Most antivirus software is better described as anti-malware, as it can detect software threats that are not technically virus-like, including spyware, Trojans, rootkits, ransomware, and cryptominers.

The broad range of threats posed by different types of malware and vulnerability exploits means that an anti-malware software solution is a critical component of workstation security. Windows Defender Antivirus is a core component of all Windows editions. Windows Defender Antivirus is managed via the Windows Security Center.

Figure 1. Windows Defender Antivirus configuration page within the Windows Security app



Screenshot courtesy of Microsoft.

19.2.5 Windows Defender Antivirus Updated Definitions

It is particularly important that antivirus software be updated regularly. Two types of updates are generally necessary:

- **Definitions are information about new viruses or malware. These updates may be made available daily or even hourly.**
- **Scan engine/component updates fix problems or make improvements to the scan software itself.**

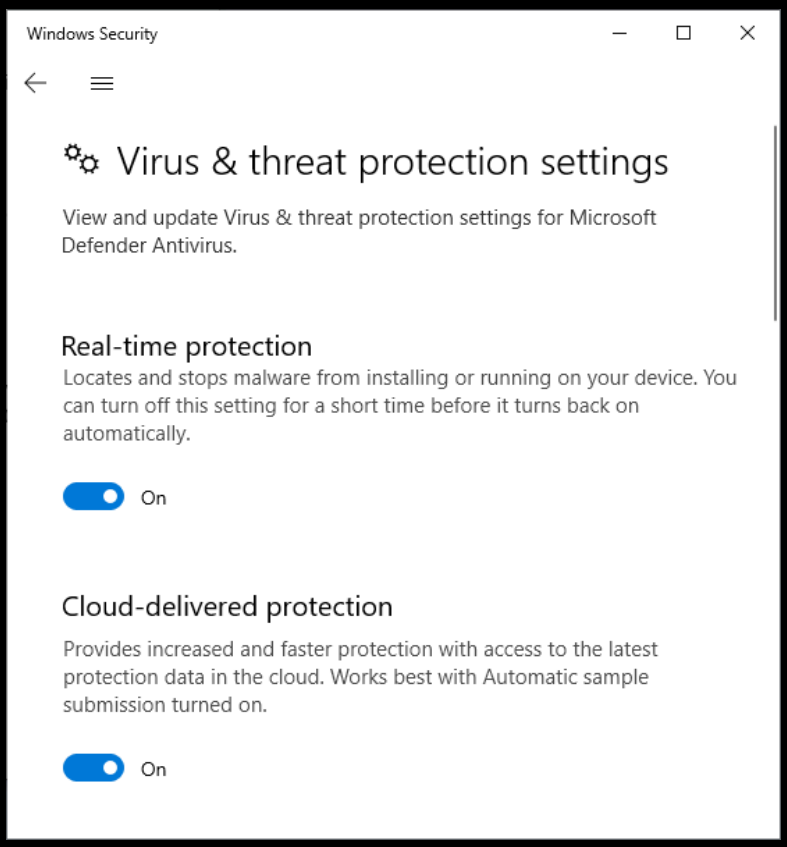
For Windows Defender Antivirus, these definitions and patches are delivered via Windows Update. Third-party software might also integrate its updates with Windows Update, or it might use its own updater.

19.2.6 Activating and Deactivating Windows Defender Antivirus

The nature of malware means that there should be no simple means of deactivating an antivirus product, or the malware could easily circumvent it. Defender Antivirus can be disabled temporarily by toggling the Real-time protection button. It will re-activate itself after a short period.

If a third-party antivirus product is installed, it will replace Windows Defender Antivirus. It can also be permanently disabled via group policy.

Figure 1. The Real-time protection setting can be toggled off to disable Windows Defender Antivirus temporarily



Screenshot courtesy of Microsoft.

It might be necessary to exclude folders from scanning. For example, scanning the disk images of virtual machines can cause performance problems. Also, some legitimate software or development code can trigger false-positive alerts. Folders containing this type of data can be excluded from scanning.

It is important to check the status of the antivirus product regularly to ensure that it is activated and up to date.

19.2.8 Windows Defender Firewall

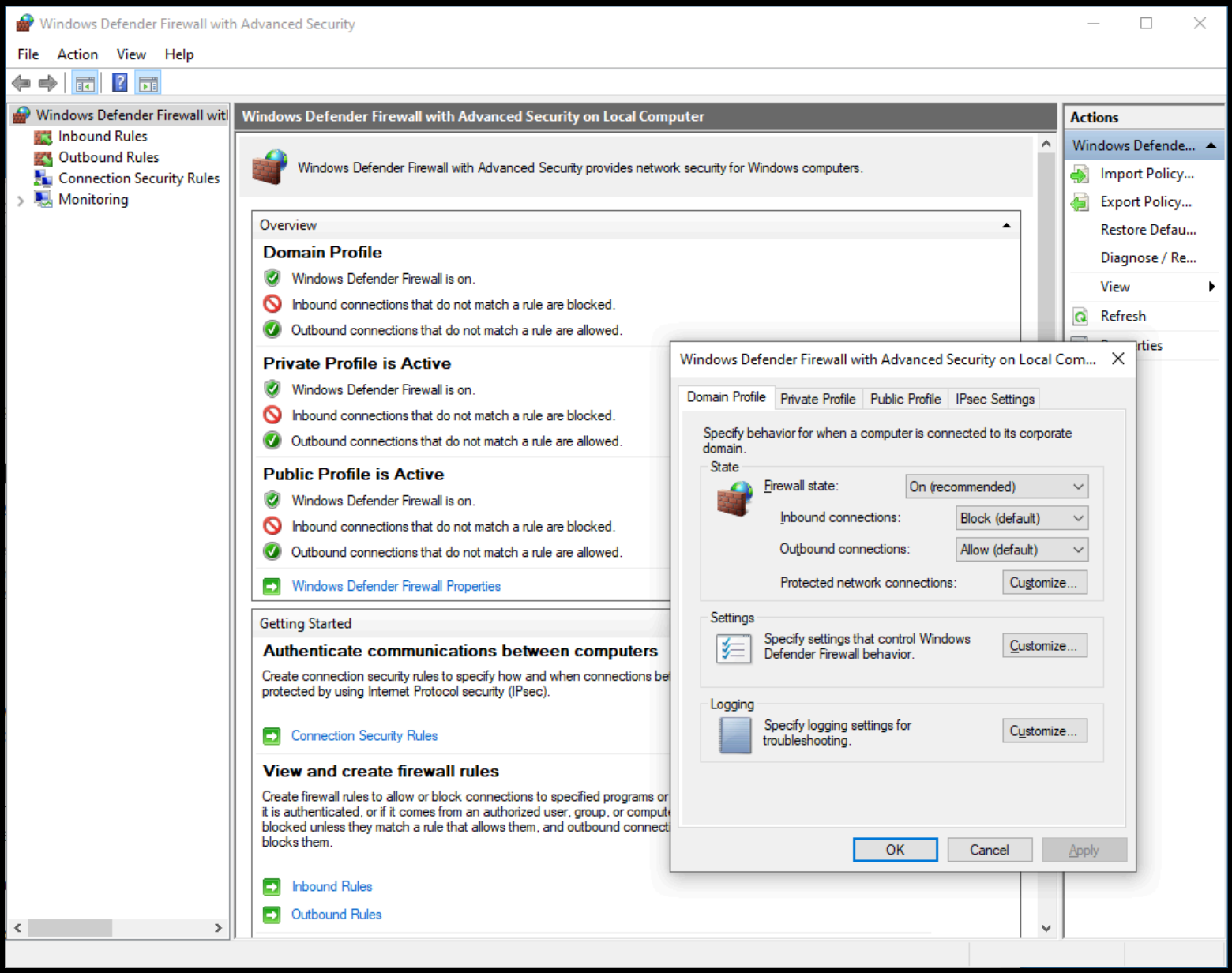
Where the antivirus product protects against threats in the file system, Windows Defender Firewall implements a personal/host firewall to filter inbound and outbound network traffic. The basic Settings app interface allows you to activate or deactivate the firewall for a given network profile and to add exceptions that allow a process to accept inbound connections.

The Windows Defender Firewall with Advanced Security console allows the configuration of custom inbound and outbound filtering rules. For each profile type, the default inbound and outbound policy can be set to block or allow. Each rule can be configured as a block or allow action to override the default policy for trigger ports, applications, and/or addresses:

- **Port security triggers are based on the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number used by the application protocol. For example, blocking TCP/80 prevents clients from connecting to the default port for a web server.**
- **Application security triggers are based on the process that listens for connections.**
- **Address triggers are based on the IP or FQDN of the server or client hosts.**

Windows Defender Firewall with Advanced Security can be configured through Group Policy on a domain. On a standalone PC or workgroup, open the wf.msc management console. On the status page, you can click Windows Defender Firewall properties to configure each profile. The firewall can be turned on or off, and you can switch the default policy for inbound and outbound traffic between Block and Allow.

Figure 1. Windows Defender Firewall with Advanced Security— Profile Settings



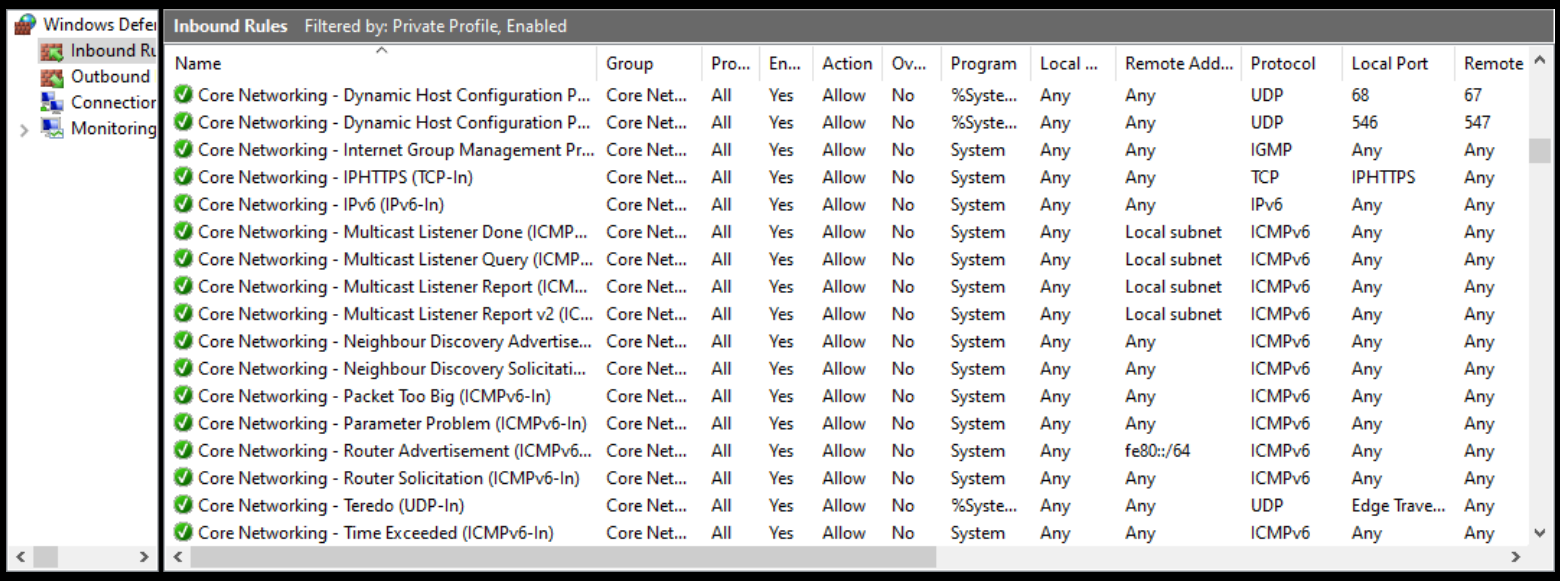
Screenshot courtesy of Microsoft.

Note:

Block stops traffic unless a specific rule allows it. Conversely, Allow accepts all traffic unless a specific rule blocks it. You can also use Block all connections to stop inbound connections regardless of the rules set up.

From the main Advanced Firewall console, you enable, disable, and configure rules by selecting in the Inbound Rules or Outbound Rules folder as appropriate.

Figure 2. Configuring inbound filtering rules in Windows Firewall with Advanced Security



Name	Group	Pro...	En...	Action	Ov...	Program	Local ...	Remote Add...	Protocol	Local Port	Remote
Core Networking - Dynamic Host Configuration P...	Core Net...	All	Yes	Allow	No	%Syste...	Any	Any	UDP	68	67
Core Networking - Dynamic Host Configuration P...	Core Net...	All	Yes	Allow	No	%Syste...	Any	Any	UDP	546	547
Core Networking - Internet Group Management Pr...	Core Net...	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any
Core Networking - IPHTTPS (TCP-In)	Core Net...	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any
Core Networking - IPv6 (IPv6-In)	Core Net...	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any
Core Networking - Multicast Listener Done (ICMP...	Core Net...	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Query (ICMP...	Core Net...	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Report (ICM...	Core Net...	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Report v2 (IC...	Core Net...	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Neighbour Discovery Advertise...	Core Net...	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Neighbour Discovery Solicitati...	Core Net...	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Packet Too Big (ICMPv6-In)	Core Net...	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Parameter Problem (ICMPv6-In)	Core Net...	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Router Advertisement (ICMPv6...	Core Net...	All	Yes	Allow	No	System	Any	fe80::/64	ICMPv6	Any	Any
Core Networking - Router Solicitation (ICMPv6-In)	Core Net...	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Teredo (UDP-In)	Core Net...	All	Yes	Allow	No	%Syste...	Any	Any	UDP	Edge Trave...	Any
Core Networking - Time Exceeded (ICMPv6-In)	Core Net...	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any

Screenshot courtesy of Microsoft.

19.2.10 Encrypting File System

When data is hosted on a file system, it can be protected by the operating system's security model. Each file or folder can be configured with an access control list (ACL), describing the permissions that principals have on the file. These permissions are enforced only when the OS mediates access to the device. If the disk is exposed to a different OS, the permissions could be overridden. Data on persistent storage— HDDs, SSDs, and thumb drives— is referred to as data-at-rest. To protect data-at-rest against these risks, the information stored on a disk can be encrypted.

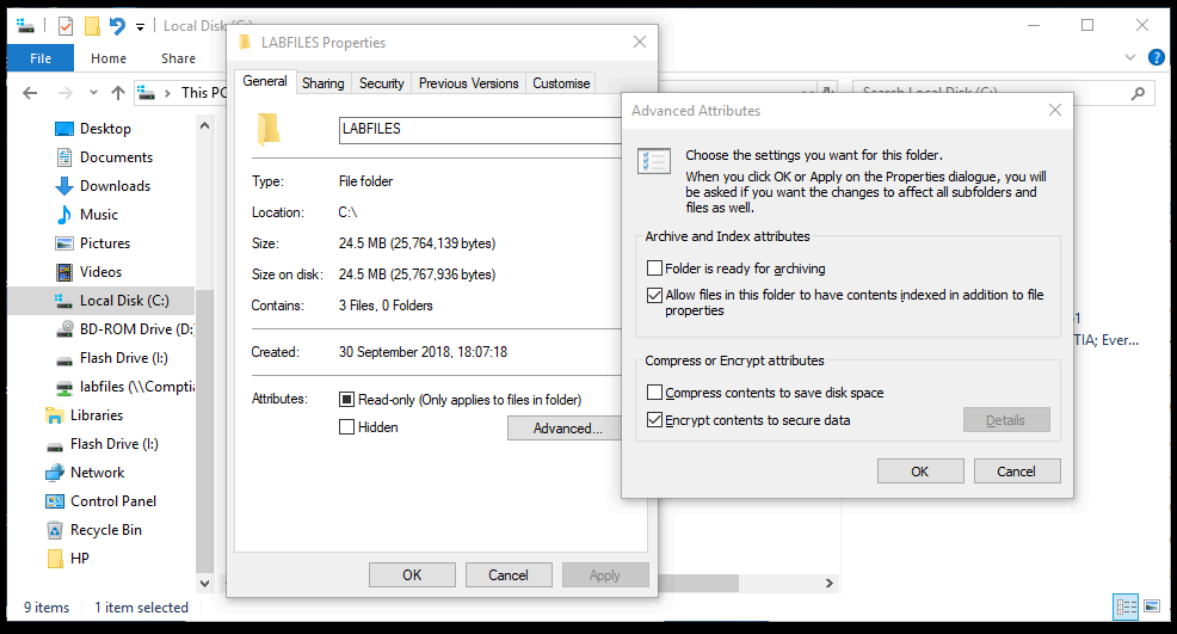
Note:

Data-at-rest contrasts with information sent over a network (data-in-transit) and information stored in nonpersistent CPU registers, cache, and system RAM (data-in-use).

One approach to protecting file system data is to apply encryption to individual files or folders. The Encrypting File System (EFS) feature of NTFS supports file and folder encryption. EFS is not available in the Home edition of Windows.

To apply encryption, open the file's or folder's property sheet and select the Advanced button. Check the Encrypt contents box, then confirm the dialogs.

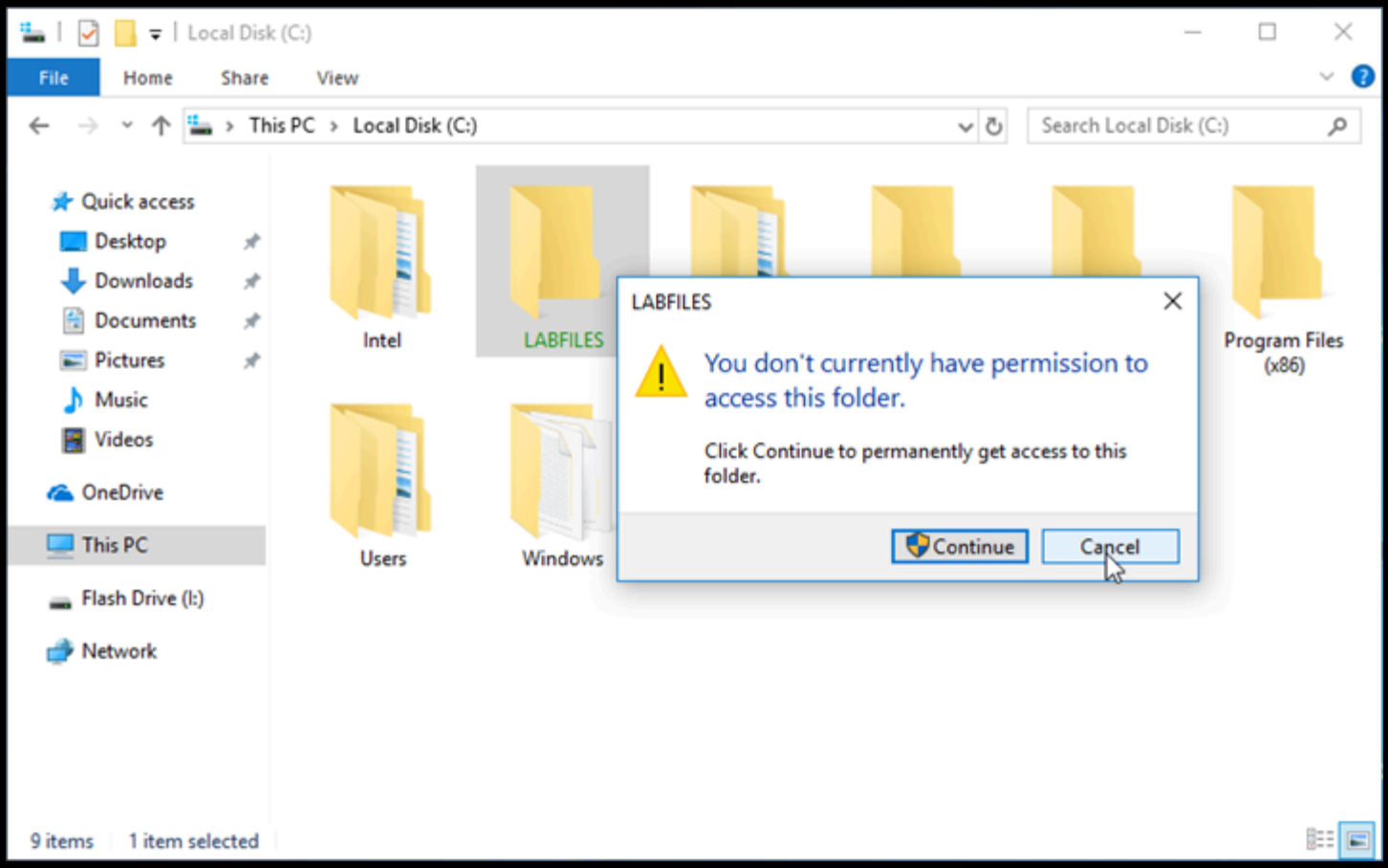
Figure 1. Applying encryption to a folder using EFS



Screenshot courtesy of Microsoft.

Folders and files that have been encrypted can be shown with green color coding in Explorer. Any user other than the one who encrypted the file will receive an "Access Denied" error when trying to browse, copy, or print the file.

Figure 2. A file that has been encrypted cannot be opened by other users—even administrators



Screenshot courtesy of Microsoft.

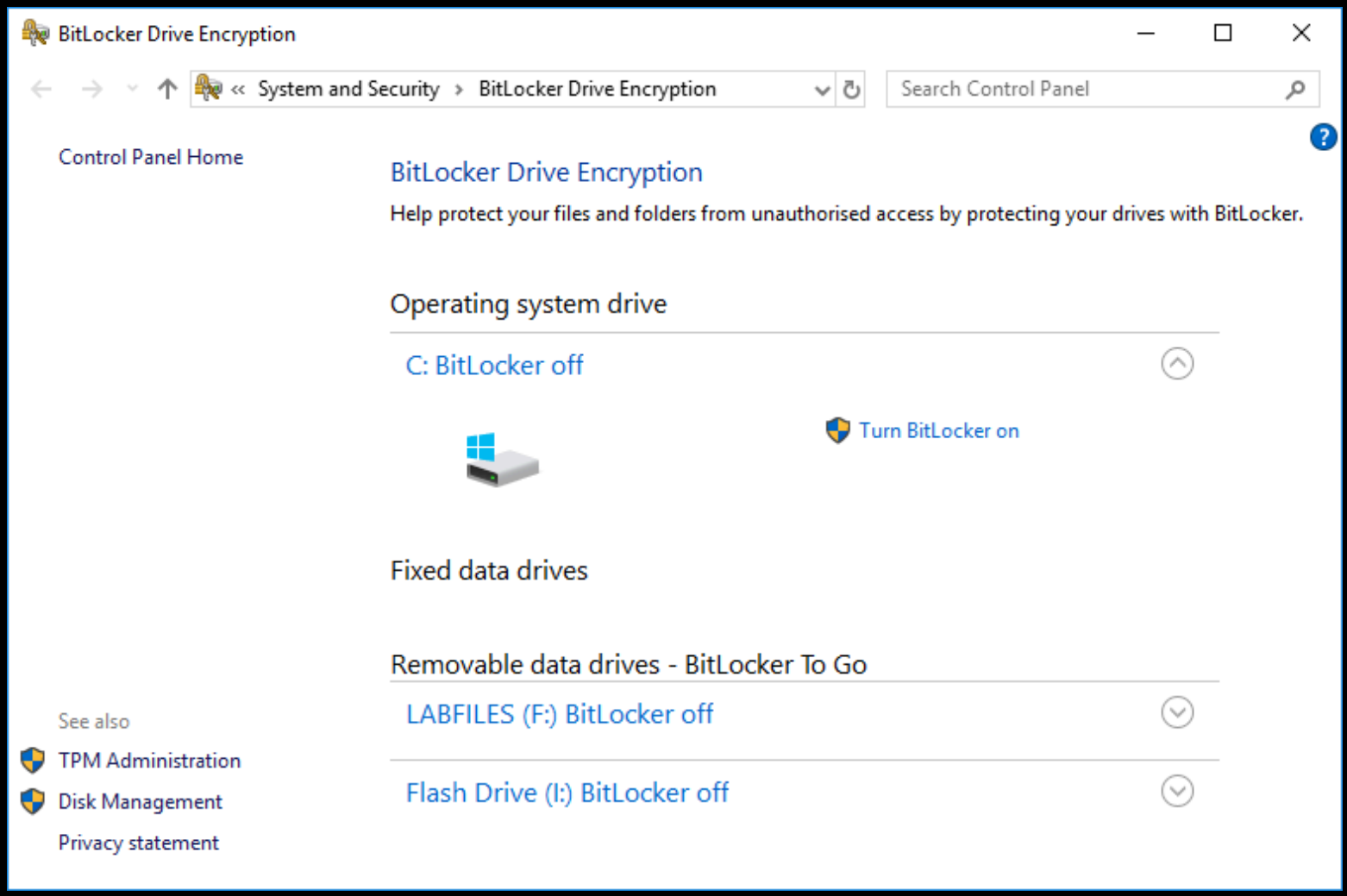
Without strong authentication, encrypted data is only as secure as the user account password. If the password can be compromised, then so can the data. The user's password grants access to the key that performs the file encryption and decryption. There is also the chance of data loss if the key is lost or damaged. This can happen if the user's profile is damaged, if the user's password is reset by an administrator, or if Windows is reinstalled. It is possible to back up the key (on a Windows domain) to set up recovery agents with the ability to decrypt data.

19.2.12 Windows BitLocker and BitLocker To Go

An alternative to file encryption is to use a full disk encryption (FDE) product. The Windows BitLocker disk encryption product is available with all editions of Windows except for the Home edition.

Full disk encryption carries a processing overhead, but modern computers usually have processing capacity to spare. The main advantage is that it does not depend on the user to remember to encrypt data. Disk encryption also encrypts the swap file, print queues, temporary files, and so on.

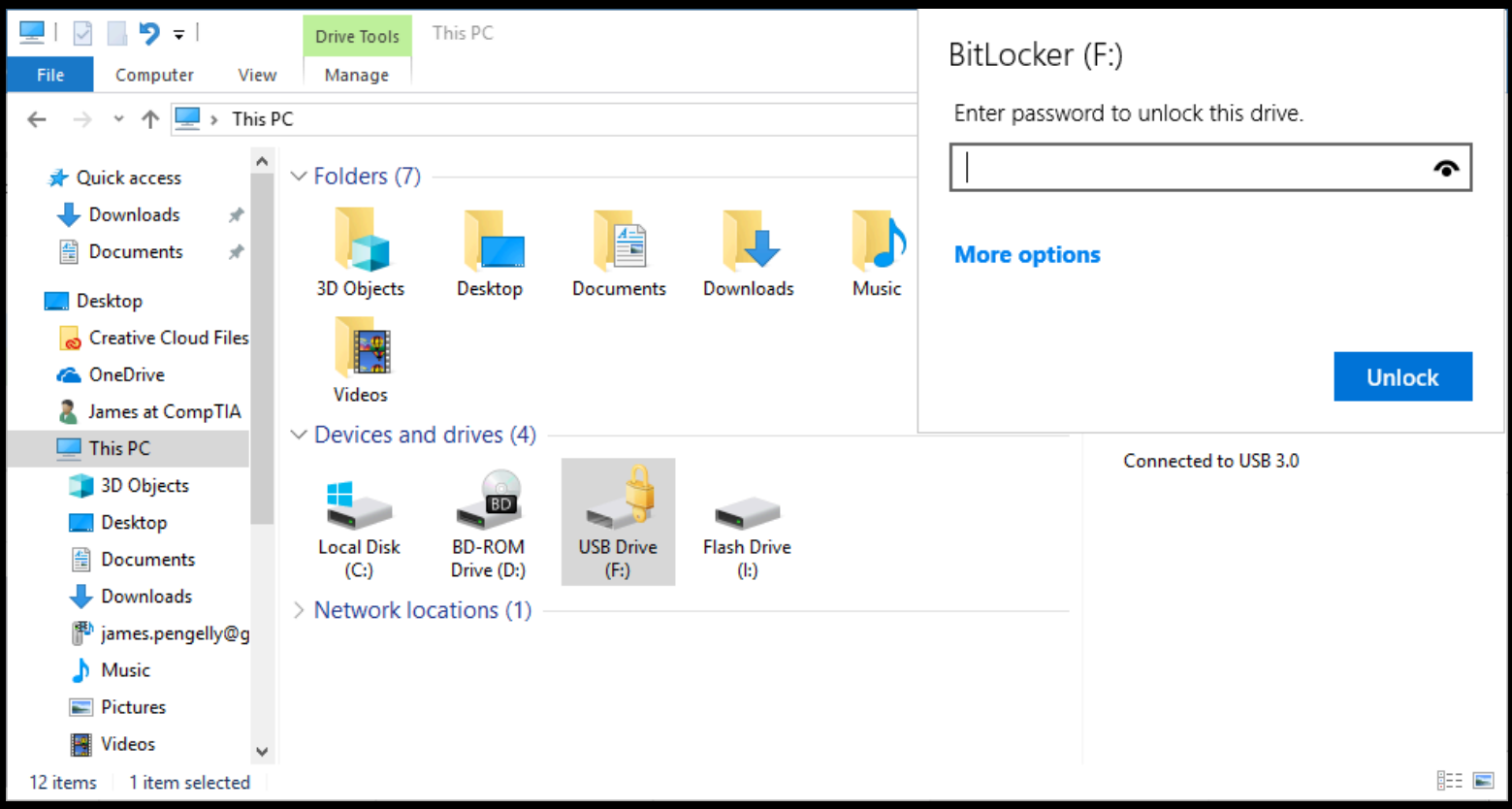
Figure 1. Configuring BitLocker and BitLocker To Go via the Control Panel



Screenshot courtesy of Microsoft.

BitLocker can be used with any volumes on fixed (internal) drives. It can also be used with removable drives in its BitLocker To Go form.

Figure 2. Removable drive protected with BitLocker To Go



Screenshot courtesy of Microsoft.

When the data is encrypted, the user must have access to the encryption key to access it. BitLocker can make use of a trusted platform module (TPM) chip in the computer to tie the use of a fixed disk to a particular motherboard. The TPM is used as a secure means of storing the encryption key and ensuring the integrity of the OS used to boot the machine. Alternatively, the key could be stored on a removable smart card or a USB stick. The computer's firmware must support booting from USB for the last option to work.

Note:

The TPM must be configured with an owner password (often the system password set in firmware). You can manage TPM settings from Windows using the TPM Management snap-in (select *TPM Administration* from the BitLocker applet).

During BitLocker setup, a recovery key is also generated. This should be stored on removable media (or written down) and stored securely (and separately from the computer). This key can be used to recover the encrypted drive if the startup key is lost.

Using PowerShell

BitLocker drive encryption can be configured using PowerShell. The `Enable-BitLocker` cmdlet is used to turn on BitLocker for a volume and specify how it should be encrypted and protected. Common switches used with this cmdlet include:

- **`-MountPoint "DriveLetter:"`: Specifies the drive you want to encrypt (for example, `"C:"`).**
- **`-EncryptionMethod MethodName`: Defines the encryption algorithm and strength to use (for example, `XtsAes128` or `XtsAes256`).**
- **`-UsedSpaceOnly:$option`: Controls whether BitLocker encrypts only the used space or the entire drive:**
  - **`$true`: Encrypt only the space currently in use.**
  - **`$false`: Encrypt the entire drive, including free space.**
- **`-RecoveryKeyPath "Path"`: Specifies a folder path where the recovery key file should be stored (for example, a network share or local path).**
- **`-RecoveryKeyProtector`: Adds a recovery key protector so the drive can be unlocked using a recovery key file if needed.**
- **`-TpmProtector`: Uses the Trusted Platform Module (TPM) on the system as a protector, so the drive can be automatically unlocked during boot if platform integrity checks succeed.**
- **`-SkipHardwareTest:$option`: Controls whether BitLocker performs a hardware test reboot before fully enabling encryption:**
  - **`$true`: Skips the hardware test and starts encryption immediately.**
  - **`$false`: Requires a restart to validate the BitLocker configuration before encryption begins.**

Example usage:

- `Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -UsedSpaceOnly:$false -RecoveryKeyPath "\\Server\Share" -RecoveryKeyProtector -TpmProtector -SkipHardwareTest:$true`

19.3 Browser Security

Core 2 Exam Objectives Covered

- **2.11 Given a scenario, configure relevant security settings in a browser.**

Web browsers provide access to a nearly endless repository of content available on the internet. The use of a browser is required to "browser" the internet to locate resources from across the globe. Ensuring that you are both safe and secure while connected to these remote resources will be key to maintaining a secure environment for your system. The security settings may also need to be changed so the computer can interact with an enterprise environment. Change to settings such as extensions and plug-ins or changing your profile sync settings may also be of use in both a professional or personal use environment.

Learning Objectives

As you study this lesson, answer the following questions:

- **How can you verify a downloaded browser has not been tampered with?**
- **Why might you consider using an untrusted source to download and install a plug-in or extension?**
- **Why might you consider clearing your cache and browsing data on a system?**
- **What does private-browsing mode mean?**

19.3.1 Browser Selection and Installation

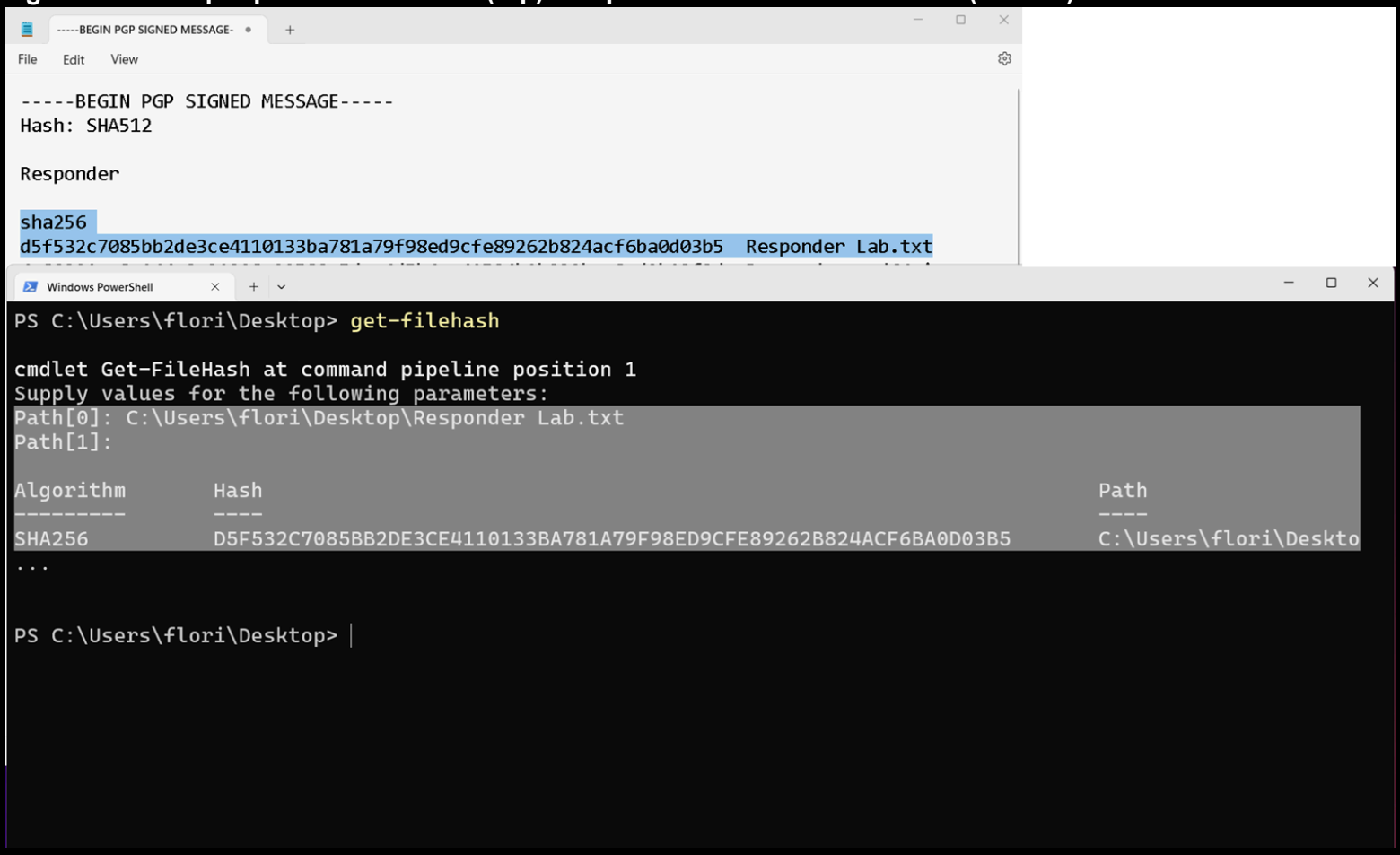
Microsoft’s Internet Explorer (IE) used to be dominant in the browser market, but alternatives such as Google's Chrome, Mozilla Firefox, and Opera have replaced it. IE itself is no longer supported. Edge, Microsoft’s replacement browser, now uses the same underlying Chromium codebase as Google Chrome. Apple’s Safari browser is tightly integrated within macOS and iOS/iPadOS.

In some scenarios, it might be appropriate to choose a browser that is different from these mainstream versions. Alternative browsers may claim to feature strong privacy controls, for instance.

Trusted Sources

As the browser is a security-critical type of software, it is particularly important to use a trusted source, such as an app store. If installed as a desktop application, care should be taken to use a reputable vendor. The integrity of the installer should also be verified, either by checking the vendor's code-signing certificate or by manually comparing the hash file published by the developer with one computed for the download file. When comparing a provided hash and self-generated hash, the same hash function must be used. For example, if the developer provides a SHA1 hash, when you calculate your own hash digest of the downloaded file, it also must be calculated with a SHA1 function.

Figure 1. Developer provided file hash (top) compared to user calculate hash (bottom)



Description

Untrusted Sources

Using a browser from an untrusted source where the publisher of the installer cannot be verified through a digital signature or hash is a security risk and likely to expose the user to unwanted adverts, search engines, and even spyware and redirection attacks. Some PC vendors bundle browsers that promote various types of adware. Though it is less common these days, such bloatware should be uninstalled as part of deploying a new PC. Adware browsers are also often bundled with other software, either covertly or as a checkable option. This type of potentially unwanted application (PUA) or Program (PUP) should also be removed from the computer.

Note:

Software that cannot definitively be classified as malicious but that does have increased privacy risks is often categorized as a potentially unwanted application (PUA).

19.3.3 Browser Settings

Each browser maintains its own settings that are accessed via its Meatball (…) or Hamburger (☰) menu button. Alternatively, you can open the internal URL, such as `chrome://settings`, `edge://settings`, or `about:preferences` (Firefox). The settings configure options such as startup and home pages, tab behavior, and choice of search engine and search behavior. Other features that can be enabled or disabled based on preference can include tabbed browsing behaviors and AI assistants like Microsoft's Copilot, which is enabled in the Edge browser by default.

Note:

The Internet Explorer browser functionality remains available as a compatibility mode in Microsoft Edge. The settings are configured via the Edge Settings and More menu.

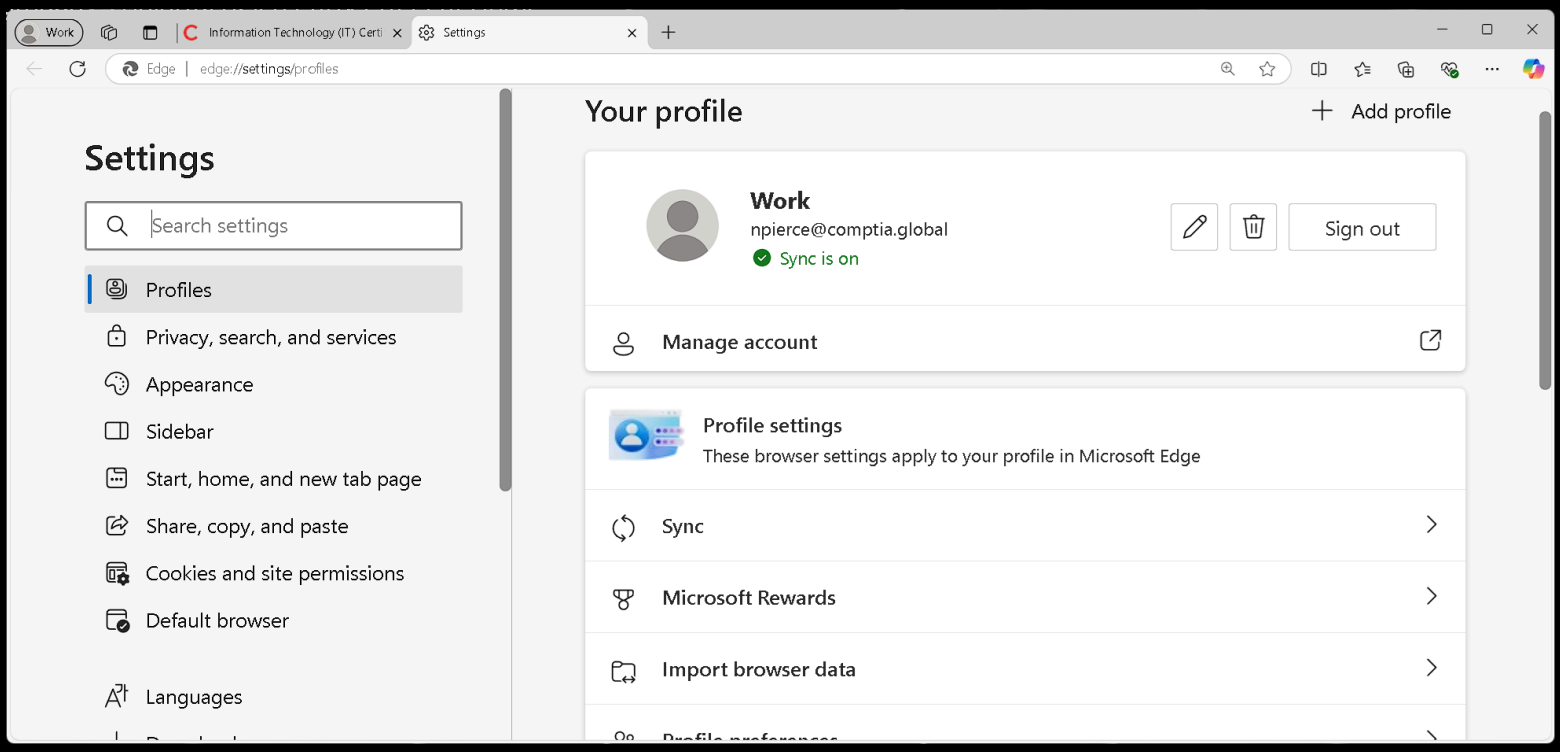
Browsers also have advanced settings that are accessed via a URL such as `chrome://flags` or `about:config`.

In enterprise environments, many of the browser settings can be managed for the entire environment through the use of group policy settings and configurations. This is accomplished using the Group Policy Management Console (GPMC) for Active Directory environments.

Sign-in and Browser Data Synchronization

A browser sign-in allows the user to synchronize settings between instances of the browser software on different devices. As well as the browser settings, items that can be synced include bookmarks, history, saved autofill entries, and passwords. Settings and data for specific applications are stored in the Windows AppData folder or for Linux, it is stored in the .config file of the Home directory.

Figure 1. Sync settings in a Microsoft Edge browser profile



Screenshot courtesy of Microsoft.

Description

Password Manager

A typical user might be faced with having to remember dozens of sign-ins for different services and resort to using the same password for each. This is insecure because just one site breach could result in the compromise of all the user's digital identities. Each major browser now supports password manager functionality and they may have an extension for the browser to make use of the third-party manager easier. This can suggest a strong password at each new account sign-up or credential reset and autofill this value when the user needs to authenticate to the site. If the user signs -in to the browser, the passwords will be available on each device.

One drawback of password managers is that not all sites present the sign-in form in a way that the password manager will recognize and trust as secure. Most of them allow you to copy and paste the string as a fallback mechanism.

19.3.5 Browser Extensions and Plug-ins

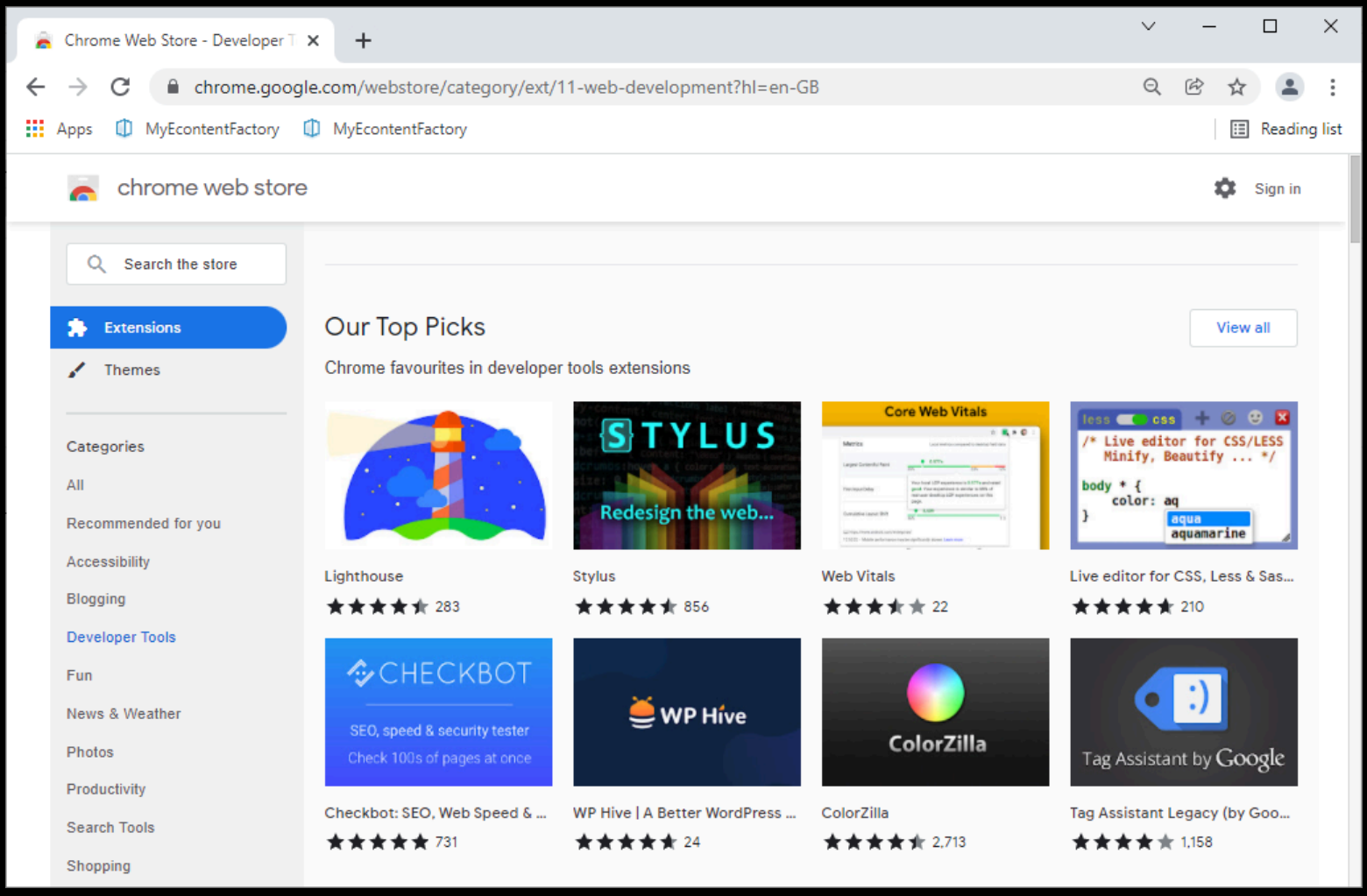
A browser add-on is some type of code that adds to the basic functionality of the software. Add-ons come in several different types:

- **Browser extensions add or change a browser feature via its application programming interface (API). For example, an extension might install a toolbar or change menu options. The extension must be granted specific permissions to make configuration changes. With sufficient permissions, they can run scripts to interact with the pages you are looking at. These scripts could compromise security or privacy, making it essential that only trusted extensions be installed. These are normally managed from the hamburger or meatball menu.**
- **Browser plug-ins play or show some sort of content embedded in a web page, such as Flash, Silverlight, or another video/multimedia format. The plug-in can only interact with the multimedia object placed on the page, so it is more limited than an extension, in theory. However, plug-ins have been associated with numerous vulnerabilities over the years and are now rarely used or supported. Dynamic and interactive content is now served using the improved functionality of HTML version 5.**
- **Apps support document editing in the context of the browser. They are essentially a means of opening a document within a cloud app version of a word processor or spreadsheet.**
- **Default search provider sets the site used to perform web searches directly from the address bar. The principal risk is that a malicious provider will redirect results to spoofed sites.**
- **Themes change the appearance of the browser using custom images and color schemes. The main risk from a malicious theme is that it could expose the browser to coding vulnerabilities via specially crafted image files.**

Any extension or plug-in could potentially pose a security and/or privacy risk. As with the browser software itself, you must distinguish between trusted and untrusted sources when deciding whether to install an add-on. Each browser vendor maintains a store of extensions, apps, and themes. This code should be subjected to a review process and use signing/hashing to ensure its integrity. There are instances of malicious extensions being included in stores, however.

You should disable extensions and plug-ins when not actively using them and enable them only when necessary. Some features can also be disabled if you do not need them.

Figure 1. The Google Chrome web store provides an official location for publishing extensions and themes



Screenshot courtesy of Google, a trademark of Google LLC.

19.3.6 Browser Patching

Maintaining a system that is up to date helps to ensure it remains protected against new threats. Just as you may update your operating system and other applications, your web browser should routinely be updated and patched using trusted sources.

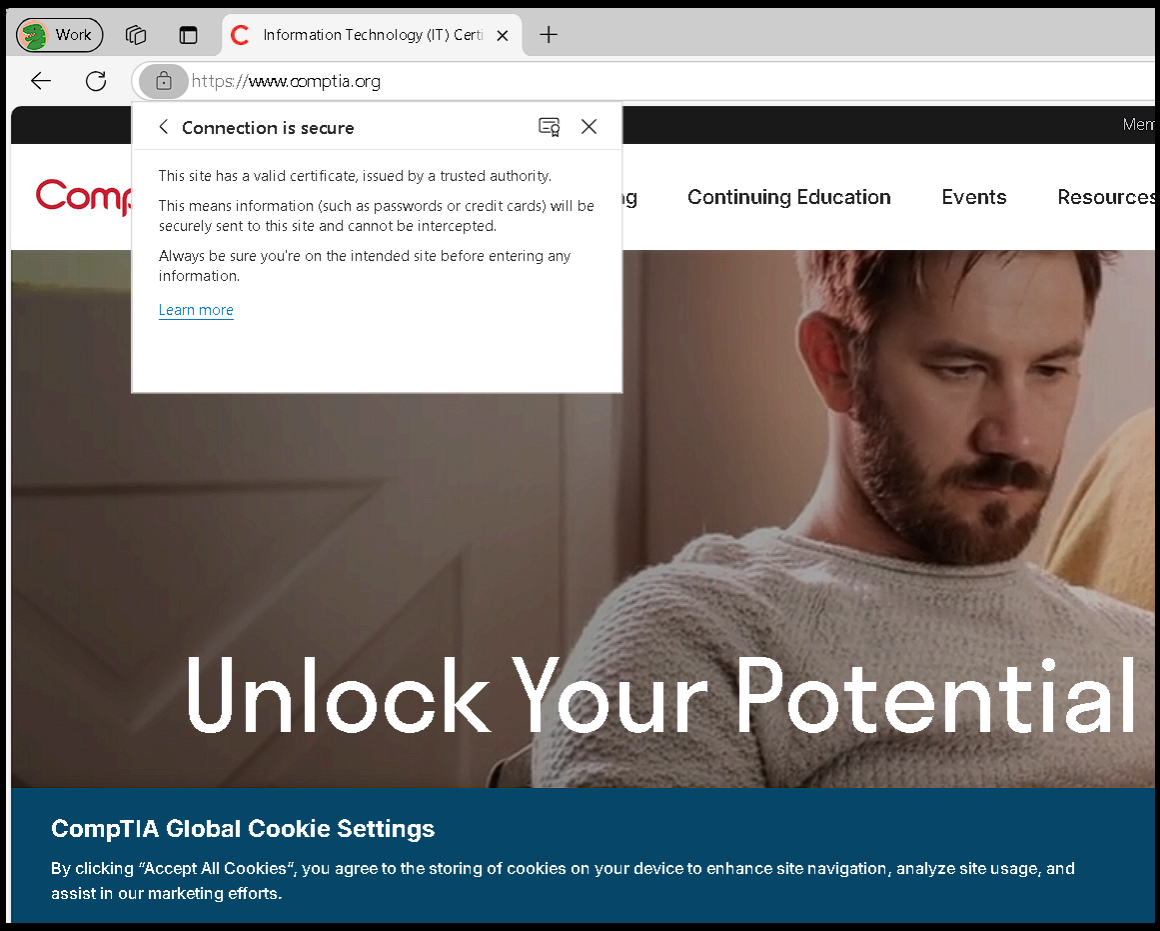
Edge is updated through its settings menu under the Help and Feedback menu option. Firefox and Chrome are set to check for updates each time the application starts by default. Safari from Apple is updated through the official App Store. For other browsers you may use, ensure the browser is routinely checking and applying update patches.

19.3.7 Secure Connections and Valid Certificates

The web uses Transport Layer Security (TLS) and digital certificate to implement a secure connection. A secure connection validates the identity of the host running a site and encrypts communications to protect against snooping. The identity of a web server computer for a given domain is validated by a certificate authority (CA), which issues the subject a digital certificate. The digital certificate contains a public key associated with the subject embedded in it. The certificate has also been signed by the CA, guaranteeing its validity. Therefore, if a client trusts the signing CA by installing its root certificate in a trusted store, the client can also trust the server presenting the certificate.

When you browse a site using an HTTPS URL, the browser displays the information about the certificate in the address bar.

Figure 1. Browsing CompTIA's home page in the Edge browser



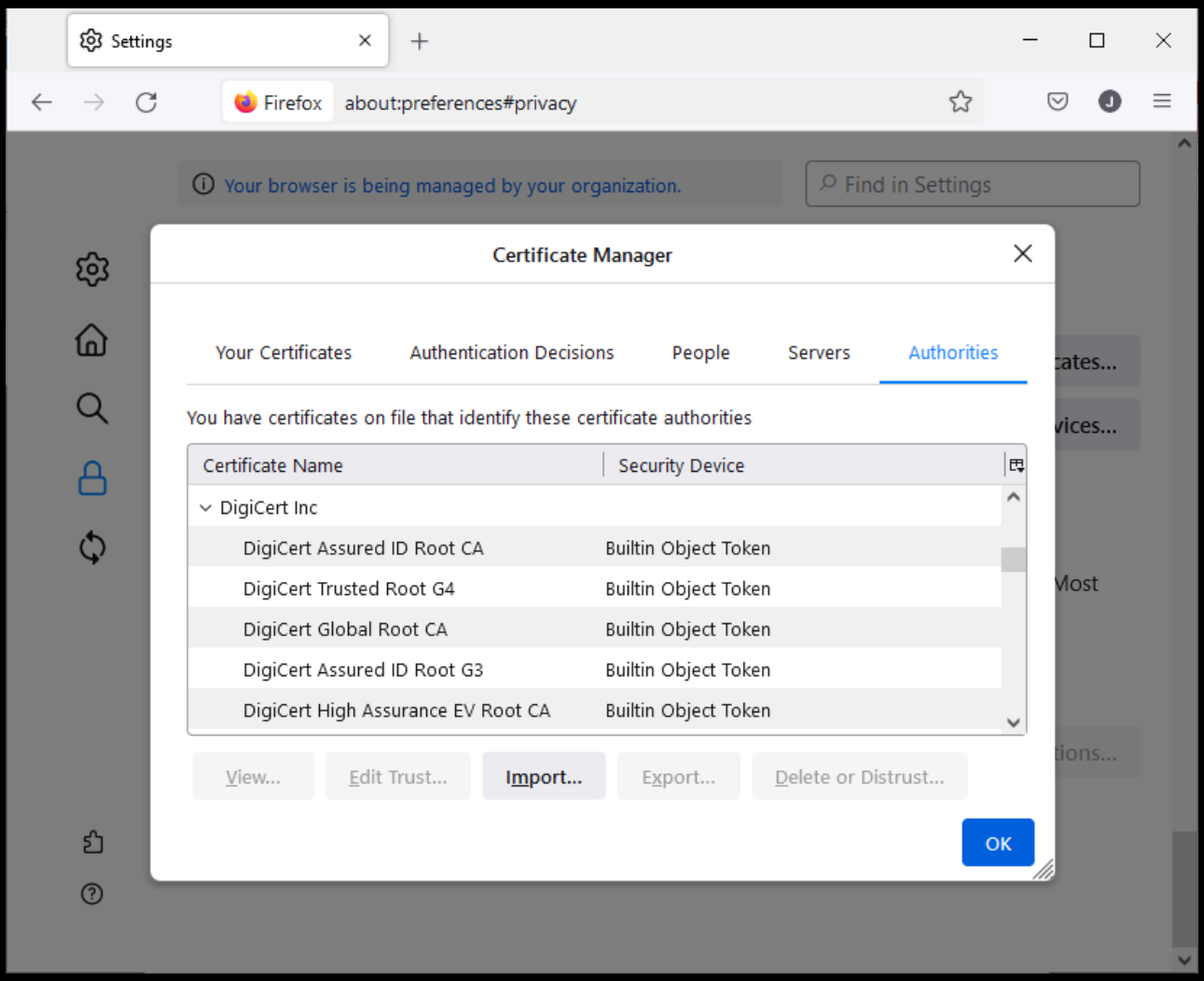
Screenshot courtesy of CompTIA and Edge.

If the certificate is valid and trusted, a padlock icon is shown. Select the icon to view information about the certificate and the CA guaranteeing it.

CA root certificates must be trusted implicitly, so it would be highly advantageous if a malicious user could install a bogus root certificate and become a trusted root CA. Installing a trusted root certificate requires administrative privileges. On a Windows PC, most root certificate updates are performed as part of Windows Update or installed by domain controllers or administrators as part of running Active Directory. There have been instances of stolen certificates and root certificates from CAs being exploited because of weaknesses in the key used in the certificate.

While Edge uses the Windows certificate store, third-party browsers maintain a separate store of trusted and personal certificates. When using enterprise certificates for internal sites and a third-party browser, you must ensure that the internal CA root certificate is added to the browser.

Figure 2. Mozilla Firefox's trusted certificate store showing the DigiCert root certificates that are trusted authorities

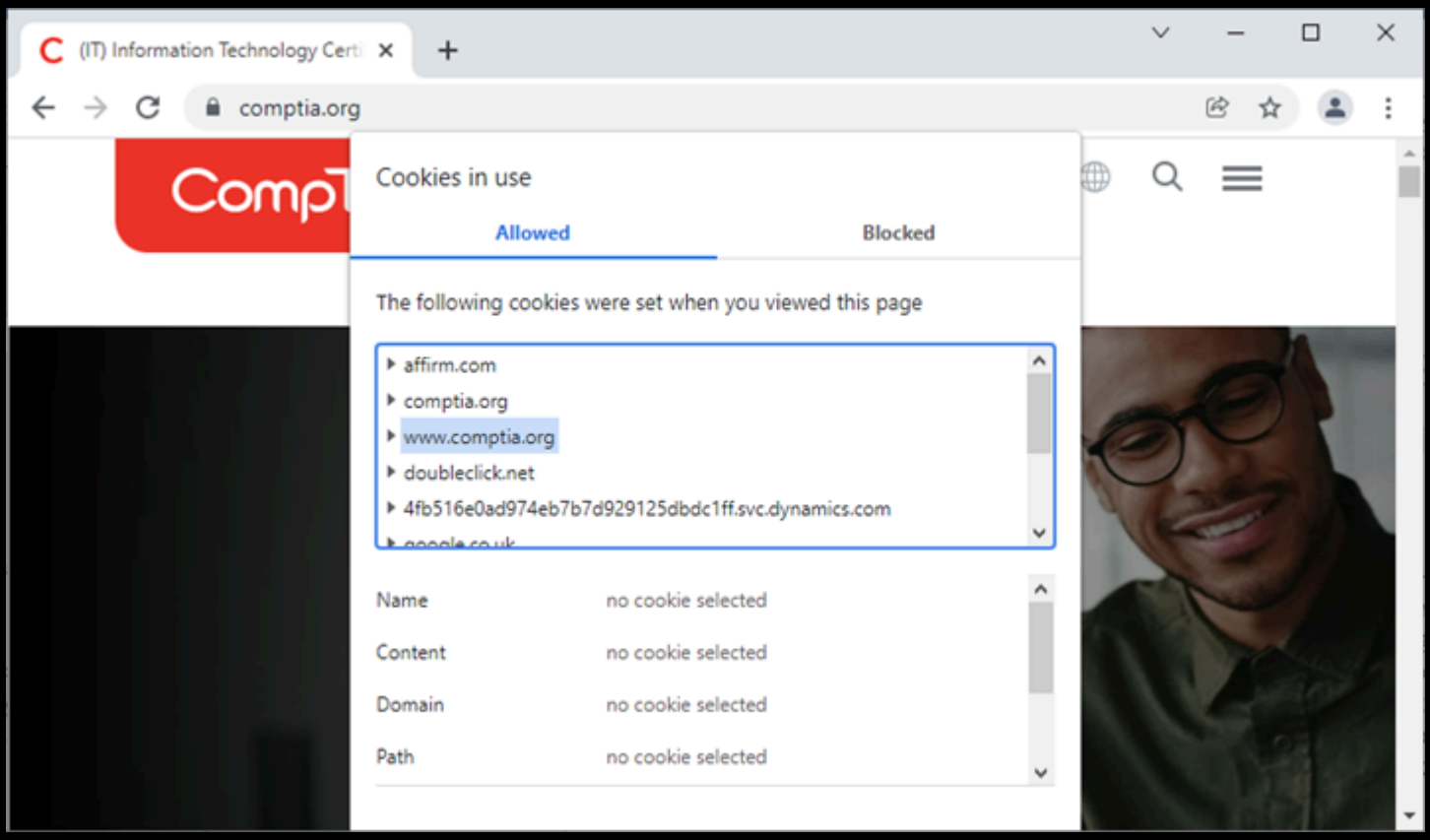


Screenshot courtesy of Mozilla.

19.3.8 Browser Privacy Settings

The marketing value of online advertising has created an entire industry focused on creating profiles of individual search and browsing habits. The main function of privacy controls is to govern sites' use of these tracking tools, such as cookies. A cookie is a text file used to store session data. For example, if you log on to a site, the site might use a cookie to remember who you are. A modern website is likely to use components from many different domains. These components might try to set third-party cookies that could create tracking information that is available to a different host than the site owner.

Figure 1. Viewing cookies set by visiting comptia.org's home page in Google's Chrome browser



Screenshot courtesy of CompTIA and Google, a trademark of Google, LLC.

The browser's privacy settings can be set to enable or disable all cookies or just third-party cookies and to configure exceptions to these rules for chosen sites. Most browsers also have a tracking protection feature that can be set to strict or standard/balanced modes.

As well as cookies, sites can use the header information submitted in requests plus scripted queries to perform browser fingerprinting and identify source IPs. Several other analytics techniques are available to track individuals as they visit different websites and use search engines. Tracking protection can mitigate some of these techniques but not all of them.

To supplement the cookie policy and tracking protection, the following features can be used to block unwanted content:

- **Pop-up blockers prevent a website from creating dialogs or additional windows. The pop-up technique was often used to show fake A-V and security warnings or other malicious and nuisance advertising.**
- **Ad Blockers use more sophisticated techniques to prevent the display of anything that doesn't seem to be part of the site's main content or functionality. No sites really use pop-up windows anymore as it is possible to achieve a similar effect using the standard web-page formatting tools. Ad blockers are better able to filter these page elements selectively. They often use databases of domains and IP addresses known to primarily serve ad content. An ad blocker must normally be installed as an extension. Exceptions can be configured on a site-by-site basis. Many sites detect ad blockers and do not display any content while the filtering is enabled.**
- **Proxy servers are commonly deployed as part of secure enterprise environments. Web connection requests are redirected to the proxy server first and then are forwarded to the internet by the proxy server. The proxy server can track web usage and use content and URL filters to control or even block access to certain content.**

- **Secure DNS settings allow the browser to authenticate DNS query responses through the use of digital signatures.**

Aside from the issue of being tracked by websites, there are privacy concerns about the data a browser might store on the device as you use it. This browsing history can be managed by two methods:

- **Clearing cache and browsing data options are used to delete browsing history. By default, the browser will maintain a history of pages visited, cache files to speed up browsing, and save text typed into form fields. On a public computer, it is best practice to clear the browsing history at the end of a session. You can configure the browser to do this automatically or do it manually.**
- **Private-browsing mode disables the caching features of the browser so that no cookies, browsing history, form fields, passwords, or temp files will be stored when the session is closed. This mode will also typically block third-party cookies and enable strict tracking protection, if available. Note that this mode does not guarantee that you are anonymous with respect to the sites you are browsing as the site will still be able to harvest data such as an IP address and use browser fingerprinting techniques.**

19.4 Troubleshoot Workstation Security

Core 2 Exam Objectives Covered

- **2.4 Summarize types of malware and tools/methods for detection, removal, and prevention.**
- **2.6 Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.**
- **3.4 Given a scenario, troubleshoot common PC security issues.**

Troubleshooting is a core job task requirement of an IT specialist. Being able to quickly and efficiently identify, evaluate, and provide an appropriate solution is not limited to hardware issues and outages. Logical problems within the operating system, applications, and browser can cause undesired operation, misuse of system resources, or even a massive outage of the system.

Learning Objectives

As you study this lesson, answer the following questions:

- **How does a malware vector differ from malware payloads?**
- **What is ransomware?**
- **What are best practices to combat malware and its undesired side effects?**
- **What steps should be taken to troubleshoot security issues within a workstation?**

19.4.1 Malware Vectors

Malware is usually simply defined as software that does something bad, from the perspective of the system owner. The more detailed classification of different malware types helps to identify the likely source and impact of a security incident. Some malware classifications focus on the vector used by the malware. The vector is the method by which the malware executes on a computer and potentially spreads to other network hosts.

The following categories describe some types of malware according to vector:

- **Virus—These are concealed within the code of an executable process image stored as a file on disk. In Windows, executable code has extensions such as .EXE, .MSI, .DLL, .COM, SCR, and .JAR. When the program file is executed, the virus code is also able to execute with the same privileges as the infected process. The first viruses were explicitly created to infect other files as rapidly as possible. Modern viruses are more likely to use covert methods to take control of the host.**
- **Boot Sector Virus—These infect the boot sector code or partition table on a disk drive. When the disk is attached to a computer, the virus attempts to hijack the bootloader process to load itself into memory.**
- **Trojan—This is malware concealed within an installer package for software that appears to be legitimate. The malware will be installed alongside the program and executed with the same privileges. It might be able to add itself to startup locations so that it always runs when the computer starts or the user signs in. This is referred to as persistence.**
- **Worm—These replicate between processes in system memory rather than infecting an executable file stored on disk. Worms can also exploit vulnerable client/server software to spread between hosts in a network.**
- **Fileless malware—This refers to malicious code that uses the host's scripting environment, such as Windows PowerShell or PDF JavaScript, to create new malicious processes in memory. As it may be disguised as script instructions or a document file rather than an executable image file, this type of malware can be harder to detect. The term fileless means that there is not a host file involved to house the malware.**

19.4.2 Malware Payloads

Classifying malware by payload is a way of identifying what type of actions the code performs other than simply replicating or persisting on a host.

Backdoors

Modern malware is usually designed to implement some type of backdoor, also referred to as a remote access trojan. Once the malware is installed, it allows the threat actor to access the PC, upload/exfiltrate data files, and install additional malware tools. This could allow the attacker to use the computer to widen access to the rest of the network or to add it to a botnet and launch distributed denial of service (DDoS) attacks or mass-mail spam.

Whether a backdoor is used as a standalone intrusion mechanism or to manage bots, the threat actor must establish a connection from the compromised host to a command and control (C2 or C&C) host or network. There are many means of implementing a covert C&C channel to evade detection and filtering. Historically, the Internet relay chat (IRC) protocol was popular. Modern methods are more likely to use command sequences embedded in HTTPS or DNS traffic.

Adware

Adware is a specialized malware used to display unwanted and unsolicited advertisements on your workstation or device. This can be accomplished by storing cookies in your browser or redirecting connection requests to an advertisement server. These Potentially Unwanted Program (PUP's) can reduce system resources and generally cause a nuisance when trying to access legitimate content. Additionally some websites now allow for notifications to be sent from the website directly to the operating system's notification system. By allowing these notifications, a user may be overwhelmed with the amount of advertisement notifications they receive. A user should manage what notifications are allowed and remove any sources they do not explicitly trust.

Spyware and Keyloggers

Spyware is malware that can perform browser reconfigurations, such as allowing tracking cookies, changing default search providers, opening arbitrary pages at startup, adding bookmarks, and so on. Spyware might also be able to monitor local application activity, take screenshots, and activate recording devices, such as a microphone or webcam. Another spyware technique is to perform DNS redirection to spoofed sites.

A keylogger is spyware that actively attempts to steal confidential information by recording keystrokes. The attacker will usually hope to discover passwords or credit card data.

Keyloggers are not only implemented as software. A malicious script can transmit key presses to a third-party website. There are also hardware devices to capture key presses to a modified USB adapter inserted between the keyboard and the port.

Some spyware and even some legitimate monitoring software applications are classified as stalkerware because they can be used to track the habits and whereabouts of a user, similar to stalking them. Abuse of employee monitoring software applications should be monitored and minimized where possible.

Figure 1. Using the Metasploit Meterpreter remote access tool to dump keystrokes from the victim machine, revealing the password used to access a web app.

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
https<Right Shift>://tickets.structureality.com/scp<CR>
jaime<Tab><Right Shift>Pa<Right Shift>$$w0rd

meterpreter >
```

Rootkits

In Windows, malware can only be manually installed with local administrator privileges. This means the user must be confident enough in the installer package to enter the credentials or accept the User Account Control (UAC) prompt. Additionally, Windows tries to protect the OS files from abuse of administrator privileges. Critical processes run with a higher level of privilege (SYSTEM).

Consequently, Trojans installed in the same way as regular software cannot conceal their presence entirely and will show up as a running process or service. Often the process image name is configured to be similar to a genuine executable or library to avoid detection. For example, a Trojan may use the filename "run32d11" to masquerade as "run32dll". To ensure persistence, the Trojan may have to use a registry entry or create itself as a service. All these techniques are relatively easy to detect and remediate.

If the malware can be delivered as the payload for an exploit of a severe vulnerability, it may be able to execute without requiring any authorization using SYSTEM privileges. Alternatively, the malware may be able to use an exploit to escalate privileges after installation. Malware running with this level of privilege is referred to as a rootkit. The term derives from UNIX/Linux where any process running as root has unrestricted access to everything from the root of the file system down.

In theory, there is nothing about the system that a rootkit could not change. In practice, Windows uses other mechanisms to prevent misuse of kernel processes, such as code signing (microsoft.com/security/blog/2017/10/23/hardening-the-system-and-maintaining-integrity-with-windows-defend

er-system-guard). Consequently, what a rootkit can do depends largely on adversary capability and level of effort. When dealing with a rootkit, you should be aware that there is the possibility that it can compromise system files and programming interfaces so that local shell processes, such as Explorer or Task Manager on Windows, `ps` or `top` on Linux, and port-listening tools (`netstat`, for example), no longer reveal their presence (when run from the infected machine, that is). A rootkit may also contain tools for cleaning system logs, further concealing its presence.

19.4.3 Ransomware and Cryptominers

Ransomware is a type of malware that tries to extort money from the victim. One class of ransomware will display threatening messages, such as requiring Windows to be reactivated or suggesting that the computer has been locked by the police because it was used to view child pornography or for terrorism. This may block access to the file system by installing a different shell program, but this sort of attack is usually relatively simple to fix.

Figure 1. WannaCry ransomware



Screenshot courtesy of Wikimedia.

Crypto-ransomware attempts to encrypt files on any fixed, removable, and network drives. If the attack is successful, the user will be unable to access the files without obtaining the private encryption key, which is held by the attacker. If successful, this sort of attack is extremely difficult to mitigate unless the user has up-to-date backups. One example of crypto-ransomware is Cryptolocker, a Trojan that searches for files to

encrypt and then prompts the victim to pay a sum of money before a certain countdown time, after which the malware destroys the key that allows the decryption.

Ransomware uses payment methods such as wire transfer, cryptocurrency, or premium-rate phone lines to allow the attacker to extort money without revealing his or her identity or being traced by local law enforcement.

A cryptominer hijacks the resources of the host to perform cryptocurrency mining. This is also referred to as cryptojacking. Commonly, such as Bitcoin, the total number of coins within a cryptocurrency is limited by the difficulty of performing the blockchain calculations necessary to generate a new digital coin. Consequently, new coins can be very valuable, but it takes enormous computing resources to achieve them. Cryptomining is often performed across botnets.

19.4.4 Troubleshoot PC Security Symptoms

The multiple classifications for malware vectors and payloads mean that there can be very many different symptoms of security issues. In very general terms, any sort of activity or configuration change that was not initiated by the user is a good reason to suspect malware infection.

Performance Symptoms

When the computer is slow or "behaving oddly," one of the things you should suspect is malware infection. Some specific symptoms associated with malware include:

- **The computer fails to boot or experiences lockups.**
- **Performance at startup or in general is very slow.**
- **The host cannot access the network and/or Internet access or network performance is slow.**

The problem here is that performance issues could have a wide variety of other causes. If you identify these symptoms, run an anti-virus or anti-malware scanner. If this is negative but you cannot diagnose another cause, consider quarantining the system or at least putting it under close monitoring.

Application Crashes and Service Problems

One of the key indicators of malware infection is that security-related applications, such as antivirus, firewalls, and Windows Update, stop working. You might notice that OS updates and virus definition updates fail. You might also notice that applications or Windows tools (Task Manager, for instance) stop working or crash frequently.

Software other than Windows is often equally attractive for malware writers as not all companies are diligent in terms of secure coding. Software that uses browser plug-ins is often targeted; examples include Adobe's Reader software for PDFs and Flash Player. If software from a reputable vendor starts crashing (faulting) repeatedly, suspect malware infection and apply quarantining/monitoring procedures.

File System Errors and Anomalies

Another marker for malware infection is changes to system files and/or file permissions. Symptoms of security issues in the file system include the following:

- **Missing or renamed files.**
- **Additional executable files with names similar to those of authentic system files and utilities, such as scvhost.exe or ta5kmgr.exe.**
- **Altered system files or personal files with date stamps and file sizes that are different from known-good versions.**

- **Files with changed permissions attributes, resulting in "Access Denied" errors.**

These sorts of issues are less likely to have other causes so you should quarantine the system and investigate it closely.

19.4.5 Desktop Alerts and Notifications

While there are some critical exploits that allow malicious code to execute without authorization, to infect a fully patched host, malware usually requires the user to explicitly install the product and confirm the UAC consent prompt. However, the malware may be able to generate something that looks like a Windows notification without being fully installed. One technique is to misuse the push notification system that allows a website to send messages to a device or app. The notification will be designed to trick or frighten the user into installing the malware by displaying a fake virus alert, for example. A notification may also link to a site that has a high chance of performing a drive-by download on an unpatched host.

False alert anti-virus is a particularly popular way to disguise a Trojan. In the early versions of this attack, a website would display a pop-up disguised as a normal Windows dialog box with a fake security alert, warning the user that viruses have been detected. As browsers and security software have moved to block this vector, cold-calling vulnerable users, then claiming to represent Microsoft support or the user's ISP and asking them to enable a remote desktop tool has become a popular attack.

19.4.6 Endpoint Monitoring Solutions

Proper monitoring of endpoint systems can be critical in the rapid detection of malicious issues on workstations. Software monitoring solutions may aid in quickly identifying issues and sending alerts to the security response team.

Endpoint detection and response (EDR) is a monitoring solution that integrates with existing security tools and can provide automated response solutions for each endpoint. Manage detection and response (MDR) solutions further the monitoring solution with customized dashboards and detection using intelligence. MDR is usually outsourced to a third-party managed security service provider (MSSP.)

Extended detection and response (XDR) solutions extend beyond the organization's endpoints to cloud systems, applications, etc. XDR solutions can also integrate intelligence-based systems to provide updated response and mitigation strategies from trusted sources.

19.4.7 Troubleshoot Browser Symptoms

Malware often targets the web browser. Common symptoms of infection by spyware or adware are random or frequent pop-ups, installation of additional toolbars, a sudden change of home page or search provider, searches returning results that are different from other computers, slow performance, and excessive crashing. Viruses and Trojans may spawn pop-ups without the user opening the browser.

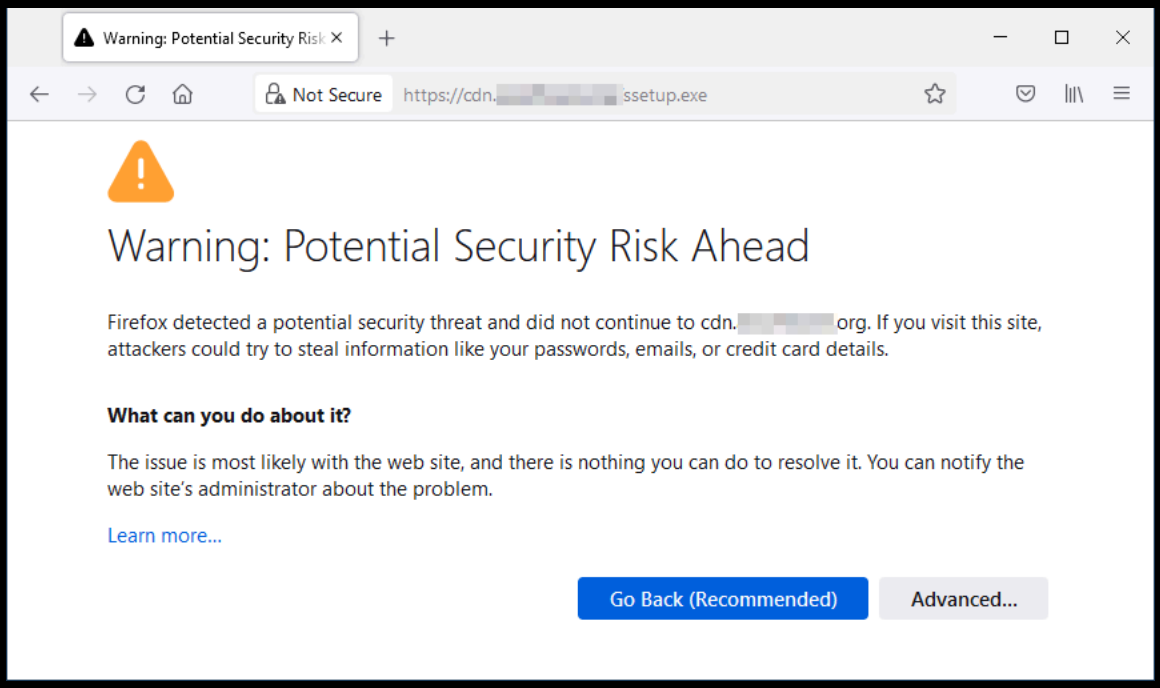
Redirection

Redirection is where the user tries to open one page but gets sent to another. Often this may imitate the target page. In adware, this is just a blunt means of driving traffic through a site, but spyware may exploit it to capture authentication details.

Certificate Warnings

When you browse a site using a certificate, the browser displays the information about the certificate in the address bar. If the certificate is untrusted or otherwise invalid, the padlock icon is replaced by an alert icon, the URL is displayed with strikethrough formatting, and the site content is likely to be blocked by a warning message.

Figure 1. Untrusted certificate warning in Mozilla Firefox



Screenshot courtesy of Mozilla.

There are many causes of certificate warnings. Some of the most common are:

- **The certificate is self-signed or issued by a CA that is not trusted.**
- **The FQDN requested by the browser is different from the subject name listed in the certificate.**
- **The certificate has expired or is listed as revoked.**

Each of these warnings could either indicate that the site is misconfigured or that some malware on the computer is attempting to redirect the browser to a spoofed page. Analyze the certificate information and the URL to determine the likely cause.

Improper use of certificates is also an indicator for a type of on-path attack by a malicious proxy:

1. **A user requests a connection to a secure site and inspects the site's certificate.**
2. **Malware on the host or some type of evil-twin access point intercepts this request and presents its own spoofed certificate to the user/browser. Depending on the sophistication of the attack, this spoof certificate may or may not produce a browser warning. If the malware is able to compromise the trusted root certificate store, there will be no warning.**
3. **If the browser accepts this certificate or the user overrides a warning, the malware implements a proxy and forwards the request to the site, establishing a session.**
4. **The user may think he or she has a secure connection to the site, but the malware is in the middle of the session and can intercept and modify all the traffic that would normally be encrypted.**

When issues within the browser are found or the performance of the browser is below expectations, you may attempt to repair or reinstall the browser application. Additionally you may want to clear the browser cache, cookies, and disable any add-ons or plug-ins to determine the root cause of the issue. Another solution may be to download another browser and see if the performance also suffers. This may indicate larger problems with the website or resource you are attempting to access.

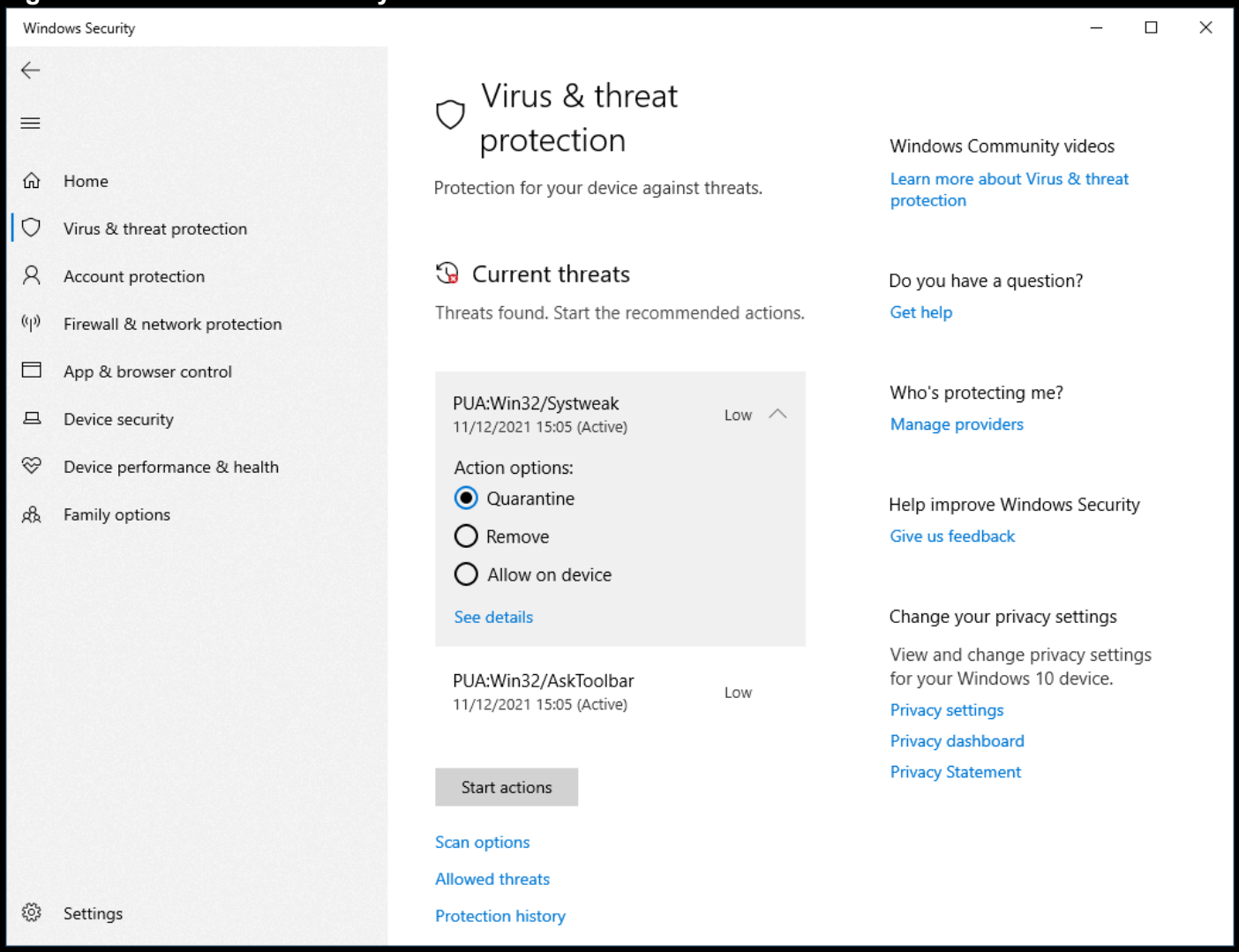
19.4.8 Best Practices for Malware Removal

CompTIA has identified a ten-step best practice procedure for malware removal:

1. **Investigate and verify malware symptoms.**
2. **Quarantine infected systems.**
3. **Disable System Restore in Windows.**
4. **Remediate infected systems.**
5. **Update anti-malware software.**
6. **Scan and removal techniques (e.g., safe mode, preinstallation environment).**
7. **Reimage/Reinstall**
8. **Schedule scans and run updates.**
9. **Enable System Restore and create a restore point in Windows. Newer Windows OS prefer that a user use the File History or Reset Windows options instead of using system restore.**
10. **Educate the end user.**

Most malware is discovered via on-access scanning by an antivirus product. If the malware is sophisticated enough to evade automated detection, the symptoms listed above may lead you to suspect infection.

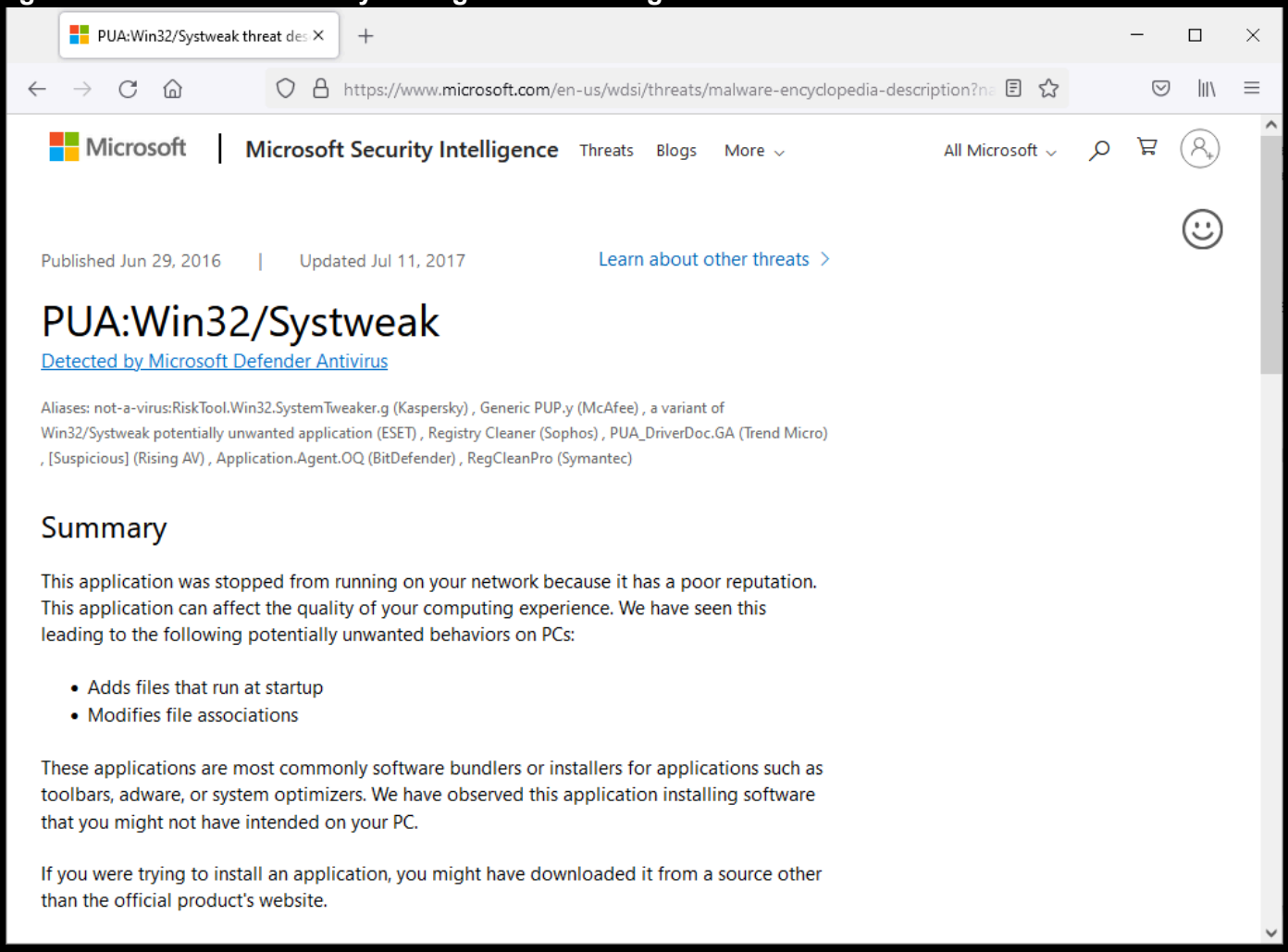
Figure 1. Threats discovered by Windows Defender Antivirus



Screenshot courtesy of Microsoft.

Antivirus vendors maintain malware encyclopedias ("bestiaries") with complete information about the type, symptoms, purpose, and removal of viruses, worms, Trojans, and rootkits. These sources can be used to verify the symptoms that you discover on a local system against known malware indicators and behaviors.

Figure 2. Microsoft's Security Intelligence knowledge base



Screenshot courtesy of Microsoft.

19.4.10 Infected Systems Quarantine

Following the seven-step procedure, if symptoms of a malware infection are detected and verified, the next steps should be to apply a quarantine and disable System Restore.

Quarantine Infected Systems

If a system is "under suspicion," do not allow users with administrative privileges to sign in—either locally or remotely—until it is quarantined. This reduces the risk that malware could compromise a privileged account.

Putting a host in quarantine means that it is not able to communicate on the main network. Malware such as worms propagates over networks. A threat actor might use backdoor malware to attempt to access other systems. This means that one of the first actions should be to disconnect the network link.

Note:

In practical terms, you might quarantine a host before fully verifying malware infection. A strong suspicion of infection by advanced malware might be a sufficient risk to warrant quarantining the host as a precaution.

Move the infected system to a physically or logically secure segment or sandbox. To remediate the system, you might need network access to tools and resources, but you cannot risk infecting the production network.

Also, consider identifying and scanning any removable media that has been attached to the computer. If the virus was introduced via USB stick, you need to find it and remove it from use. Viruses could also have infected files on any removable media attached to the system while it was infected.

Disable System Restore

Once the infected system is isolated, the next step is to disable System Restore and other automated backup systems, such as File History. If you are relying on a backup to recover files infected by malware, you must consider the possibility that the backups are infected too. The safest option is to delete old system restore points and backup copies, but if you need to retain them, try to use antivirus software to determine whether they are infected.

19.4.11 Malware Removal Tools and Methods

The main tool to use to try to remediate an infected system will be antivirus software, though if the software has not detected the virus in the first place, you are likely to have to use a different suite. Make sure the antivirus software is fully updated before proceeding. This may be difficult if the system is infected, however. It may be necessary to remove the disk and scan it from a different system.

Figure 1. Microsoft's Windows Defender Antivirus uses continual threat/definition updates



While there were differences in the past, the terms antivirus and anti-malware are synonymous. Almost every antivirus product protects against a broad range of viruses, worms, fileless malware, Trojans, rootkits, ransomware, spyware, and cryptominer threats.

If a file is infected with a virus, you can (hopefully) use antivirus software to try to remove the infection (cleaning), quarantine the file (the antivirus software blocks any attempt to open it), or erase the file. You might

also choose to ignore a reported threat if it is a false positive, for instance. You can configure the default action that software should attempt when it discovers malware as part of a scan.

Recovery Options

Infection by advanced malware might require manual removal steps to disable persistence mechanisms and reconfiguration of the system to its secure baseline. For assistance, check the website and support services for your antivirus software, but in general terms, manual removal and reconfiguration will require the following tools:

- Use Task Manager to terminate suspicious processes.

- Execute commands at a command prompt terminal, and/or manually remove registry items using `regedit`.
- Use `msconfig` to perform a safe boot or boot into Safe Mode, hopefully preventing any infected code from running at startup.
- Boot the computer using the product disc or recovery media, and use the Windows Recovery Environment (WinRE) to run commands from a clean command environment.
- Remove the disk from the infected system, and scan it from another system, taking care not to allow cross-infection.

OS Reinstallation

Antivirus software will not necessarily be able to recover data from infected files. Also, if malware gains a persistent foothold on the computer, you might not be able to run antivirus software anyway and would have to perform a complete system restore. This involves reformatting the disk, reinstalling the OS and software (possibly from a system image snapshot backup), and restoring data files from a (clean) backup.

19.4.12 Malware Infection Prevention

Once a system has been cleaned, you need to take the appropriate steps to prevent reinfection.

Configure On-access Scanning

Almost all security software is now configured to scan on-access. On-access means that the A-V software intercepts an OS call to open a file and scans the file before allowing or preventing it from being opened. This reduces performance somewhat but is essential to maintaining effective protection against malware.

Configure Scheduled Scans

All security software supports scheduled scans. These scans can impact performance, however, so it is best to run them when the computer is otherwise unused.

You also need to configure the security software to perform malware-pattern and antivirus-engine updates regularly.

Re-enable System Restore and Services

If you disabled System Restore and automatic backups, you should re-enable them as part of the recommissioning process:

- **Create a fresh restore point or system image and a clean data backup.**
- **Validate any other security-critical services and settings that might have been compromised by the malware.**
- **Verify DNS configuration—DNS spoofing allows attackers to direct victims away from the legitimate sites they were intending to visit and toward fake sites. As part of preventing reinfection, you should inspect and re-secure the DNS configuration.**
- **Configure an email security gateway to auto-scan emails sent or received by the domain. This can prevent issues from malicious emails before they reach a user's inbox.**
- **Re-enable software firewalls—If malware was able to run with administrative privileges, it may have made changes to the software (host) firewall configuration to facilitate connection with a C&C network. An unauthorized port could potentially facilitate the reinfection of the machine. You should inspect the firewall policy to see if there are any unauthorized changes. Consider resetting the policy to the default.**

As a final step, complete another antivirus scan; if the system is clean, then remove the quarantine and return it to service.

Educate the End User

Another essential malware prevention follow-up action is effective user training. Untrained users represent a serious vulnerability because they are susceptible to social engineering and phishing attacks. Appropriate security-awareness training needs to be delivered to employees at all levels, including end users, technical staff, and executives. Some of the general topics that need to be covered include the following:

- **Password and account-management best practices plus security features of PCs and mobile devices.**
- **Education about common social engineering and malware threats, including phishing, website exploits, and spam plus alerting methods for new threats.**
- **Secure use of software such as browsers and email clients plus appropriate use of Internet access, including social networking sites.**
- **Specific anti-phishing training to identify indicators of spoofed communications, such as unexpected communications, inconsistent sender and reply to addresses, disguised links and attachments, copied text and images, and social engineering techniques, such as exaggerated urgency or risk claims.**

Continuing education programs ensure that the participants do not treat a single training course or certificate as a sort of final accomplishment. Skills and knowledge must be continually updated to cope with changing threat types.

20.0 Supporting Mobile Software

You work for a logistics and transportation company, which relies heavily on mobile devices for tracking shipments, managing logistics, and communicating with drivers on the road. Recently, the company has experienced several issues with mobile device security and performance, impacting operational efficiency. Your task is to ensure that all mobile devices used by the company are secure, perform optimally, and comply with company policies to maintain smooth logistics operations.

Prepare for A+ Core 2 by:

- **Configuring mobile OS security.**
- **Troubleshooting mobile OS and app software.**
- **Troubleshooting mobile OS and app security.**

20.1 Mobile OS Security

Core 2 Exam Objectives Covered

- **2.1 Summarize various security measures and their purposes.**
- **2.8 Given a scenario, apply common methods for securing mobile devices.**

The company has noticed that some of its mobile devices have been compromised due to weak security measures. Your task is to implement robust security protocols to protect sensitive shipment data and ensure that all devices are compliant with company security policies.

Learning Outcomes

As you study this lesson, answer the following questions:

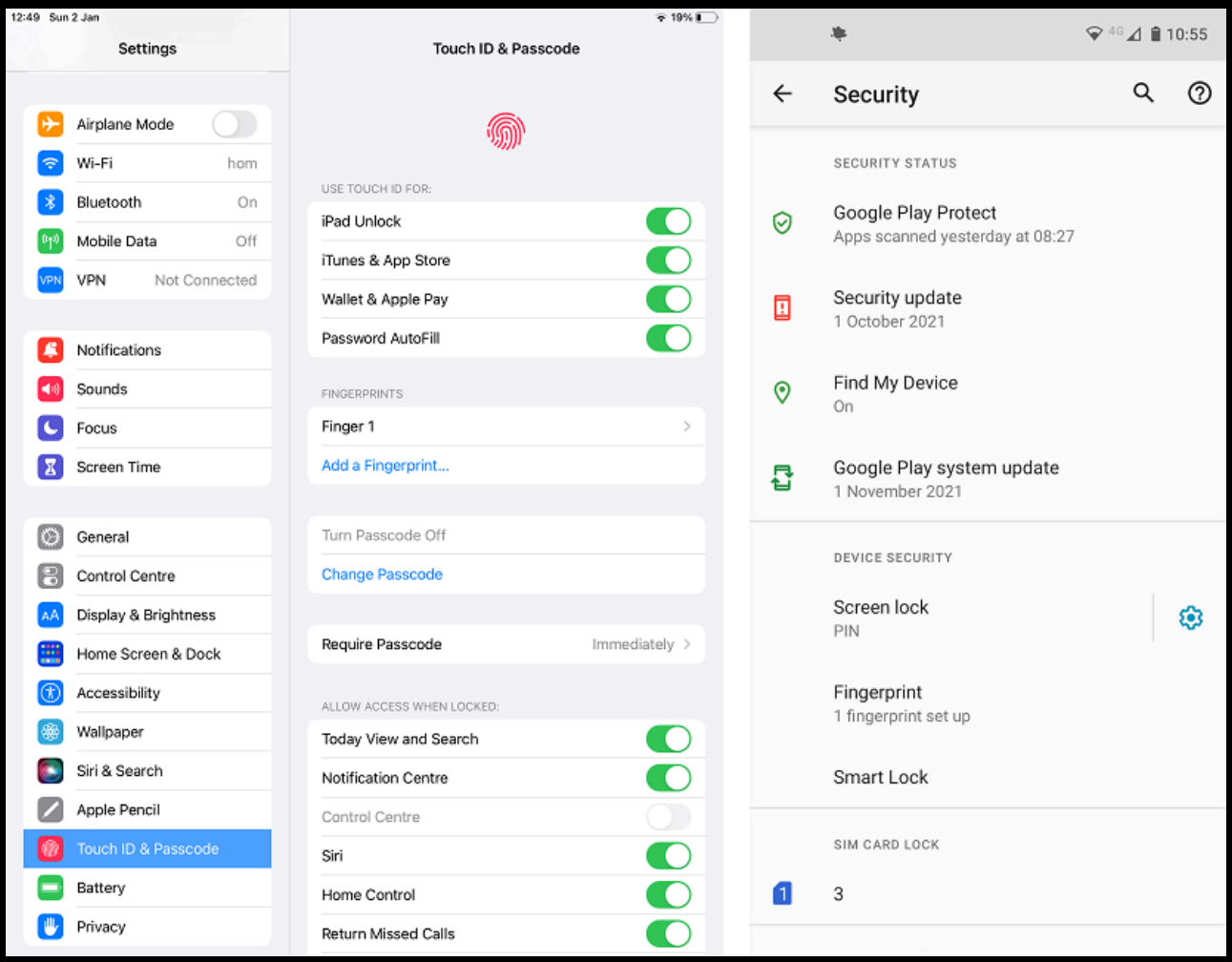
- **What are the different types of screen locks available on mobile devices, and how do they contribute to device security?**
- **How does mobile security software protect against malware and phishing attacks?**
- **What is the importance of keeping the mobile OS and apps updated with the latest patches?**
- **How can antivirus and anti-malware apps enhance the security of mobile devices?**
- **How can Mobile Device Management (MDM) software enforce security policies on mobile devices?**

20.1.1 Screen Locks

If threat actors gain access to smartphones or tablets, they can retrieve vast amounts of information to facilitate further attacks. This includes confidential data, cached passwords for email, VPNs, and websites, as well as contacts and message histories (SMS, email, and IM), which can aid in social engineering attacks. Therefore, hardening techniques are crucial to protect mobile devices against loss, theft, and unauthorized access with a screen lock.

A screen lock activates when the device is idle, or the power button is pressed. To unlock, the user must perform a gesture. A simple swipe provides unauthenticated access, suitable for shared or public devices, but personal devices require stronger authentication:

- **Personal Identification Number(PIN) or Password: Most devices require a PIN or password to enable screen lock and encryption. A 4- or 6-digit PIN offers adequate security if not easily guessable. For high-risk scenarios, a strong password is recommended. Figure 1. Configuring screen lock options in iOS (left) and Android (right)**



Screenshots reprinted with permission from Apple Inc. and Android platform, a trademark of Google LLC.

Fingerprint: Many devices utilize fingerprint sensors for biometric unlocking. The user initially scans their fingerprint to create a template stored securely on the device for future authentication.
Facial Recognition: This method uses a 3-D image of the user's face for authentication, leveraging the device's camera and infrared technology to enhance accuracy and security.

Note: If a biometric method is used, a PIN or password serves as a backup or for high-privilege tasks like factory resets.

Pattern Lock: Involves the user swiping a "join-the-dots" pattern. However, it has several weaknesses: it is easy to observe and can be traced from screen smudges. Research also shows that users often choose predictable patterns, like C, M, N, O, and S shapes.

Screen locks can be configured for failed login attempts restriction, escalating lockout times to deter unauthorized access attempts. For example, the first incorrect attempt might lock the device for 30 seconds, while subsequent attempts increase the lockout duration.

20.1.2 Mobile Security Software

Mobile devices can use similar security software as PCs and laptops to protect against malware, phishing, and software exploits.

Patching/OS Updates

Keeping a mobile OS and its apps updated with patches and new OS versions is crucial, similar to desktop computers.

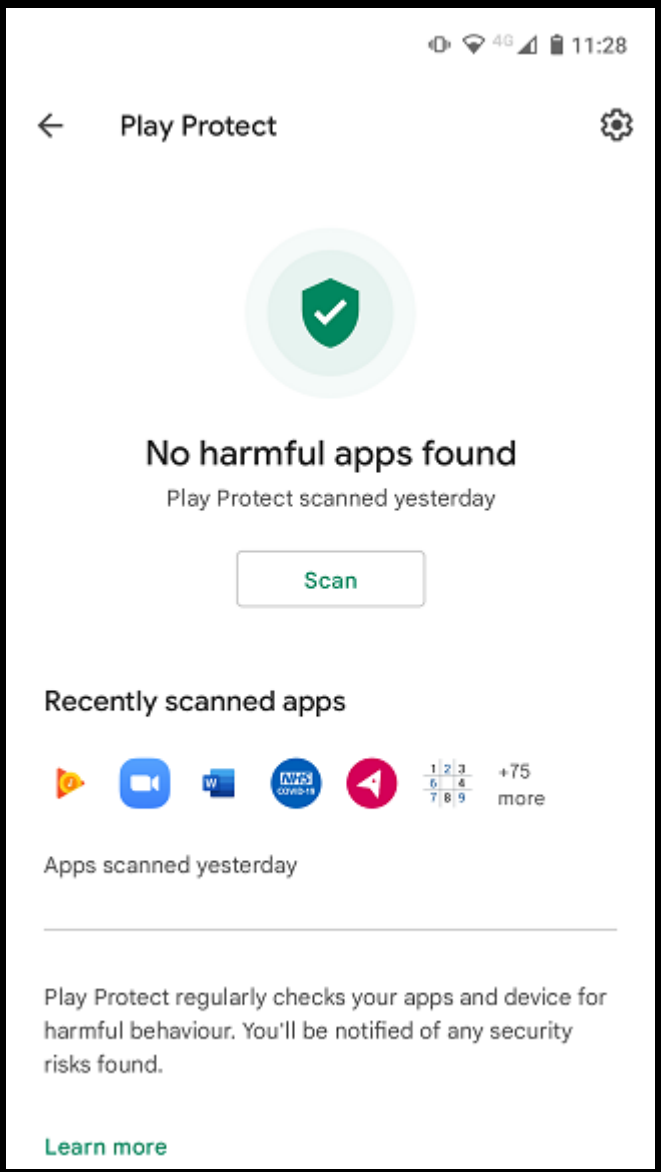
- **iOS: The consistent hardware and software platform allows for efficient updates, delivered via Settings > General > Software Update. App updates are notified via app icons and delivered through the App Store's Updates page.**
- **Android: Updates depend on the device vendor, as they must adapt patches for their specific Android version. Support for new OS versions varies. Updates are delivered via the notification bar and can be accessed through Settings > System > Advanced > System updates. App updates are typically managed through the Google Play Store, where users can check for and install updates.**

Antivirus/Anti-malware Apps

Modern smartphones are vulnerable to software exploits and malware, especially if apps are installed from untrusted sources. The evolving nature of mobile OS threats makes it challenging to maintain pattern databases or use heuristics effectively.

Endpoint security software, or mobile antivirus/anti-malware apps, often act as content filters, blocking access to known phishing sites and adware/spyware activity. They also detect configuration errors and monitor app permissions and usage. Many offer third-party data backup and device location services.

Figure 1. The Google Play store has a Play Protect feature that is enabled by default



Screenshot courtesy of Google Play Store, a trademark of Google LLC.

Firewall Apps

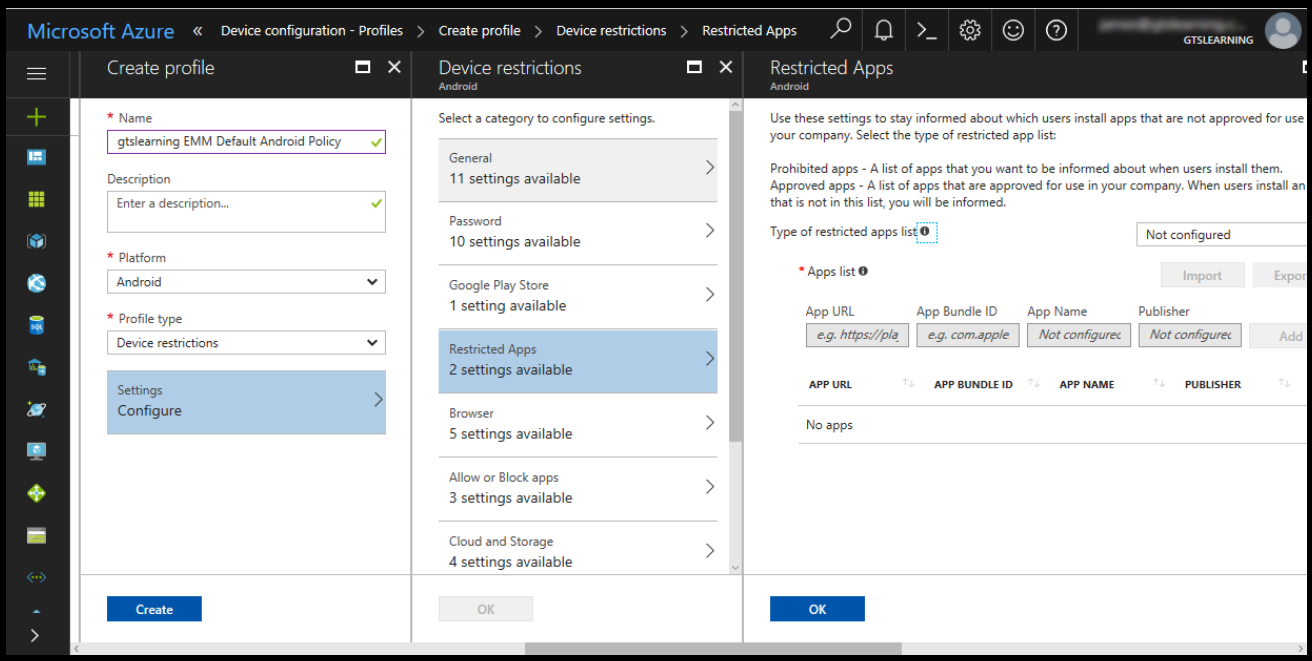
Firewall apps for mobile devices monitor app activity and prevent connections to specific ports or IP addresses. Firewalls need higher permission levels (root) to control other apps, making installation challenging. "No-root" firewalls create a local virtual private network (VPN) interface to manage app access.

20.1.3 Enterprise Mobility Management

Mobile devices have become essential for email, daily management tasks, and accessing business processes and cloud applications. A mobile device deployment model includes the policies and procedures that define how employees receive mobile devices and applications:

- **Bring Your Own Device (BYOD): Employees use their own devices, which must meet company specifications for OS version and functionality. Employees must agree to install corporate apps and allow some oversight and auditing. This model is popular with employees but presents security challenges.**
- **Corporate Owned, Business Only (COBO): The company owns the device, and it is used solely for business purposes.**
- **Corporate Owned, Personally Enabled (COPE): The company provides and owns the device, but employees can use it for personal activities like email and social media, following acceptable use policies.**
- **Choose Your Own Device (CYOD): Similar to COPE, but employees choose from a list of approved devices.**

Figure 1. Endpoint management software



Screenshot courtesy of Microsoft.

By utilizing configuration profiles, companies can tailor security profile requirements for different employees and locations, applying selective policies as needed, such as disabling smartphone cameras in high-risk areas. While some policies require technical solutions, others may involve "soft" measures like training and disciplinary actions.

20.1.4 Mobile Device Management

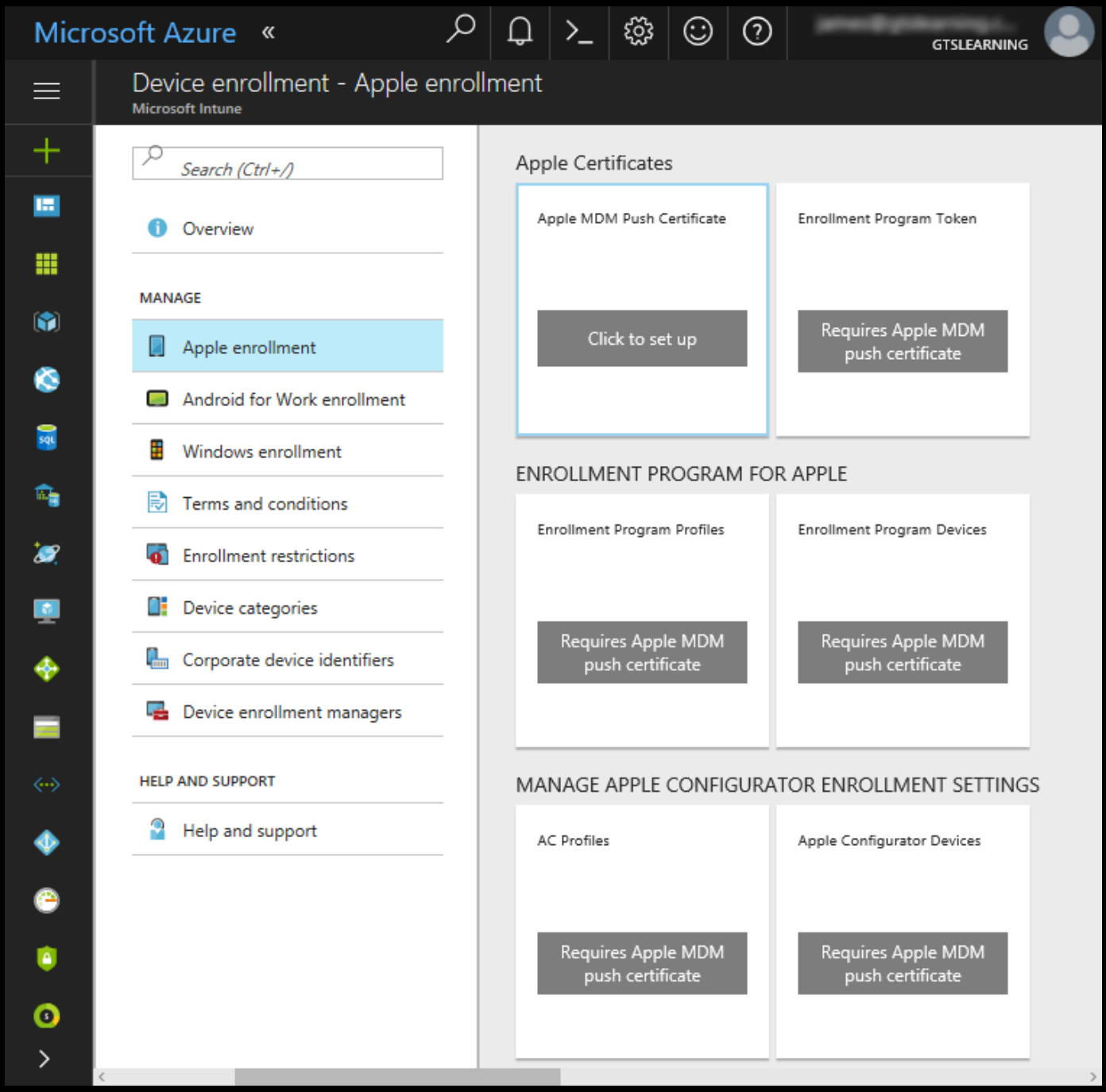
Mobile device management (MDM) is a class of software designed to apply security policies to the use of mobile devices in the enterprise. This software can be used to manage enterprise-owned devices as well as bring your own device (BYOD) user-owned smartphones.

The MDM software logs the use of a device on the network and determines whether to allow it to connect or not, based on administrator-set parameters. When the device is enrolled with the management software, it can be configured with policies to allow or restrict the use of apps, corporate data, and built-in functions, such as a video camera or microphone.

The MDM software is essential for enforcing security policies on smartphones and tablets within business networks, managing both corporate-owned devices and BYOD. A key component of MDM is the use of configuration profiles, which are crucial for defining and enforcing security profile requirements to ensure compliance with organizational security standards. These profiles:

- **Manage Device Settings: Configure Wi-Fi and VPN settings.**
- **Enforce Security Policies: Implement password and encryption requirements.**
- **Control App Installations and Permissions: Regulate which apps can be installed and what permissions they have.**
- **Regulate Network Access: Control how devices connect to networks.**
- **Monitor Compliance: Ensure devices adhere to security policies.**
- **Facilitate Remote Management: Allow IT administrators to update or remove profiles without physical access.**

Figure 1. Configuring iOS device enrollment in Microsoft's Intune Enterprise Mobility Management (EMM) suite



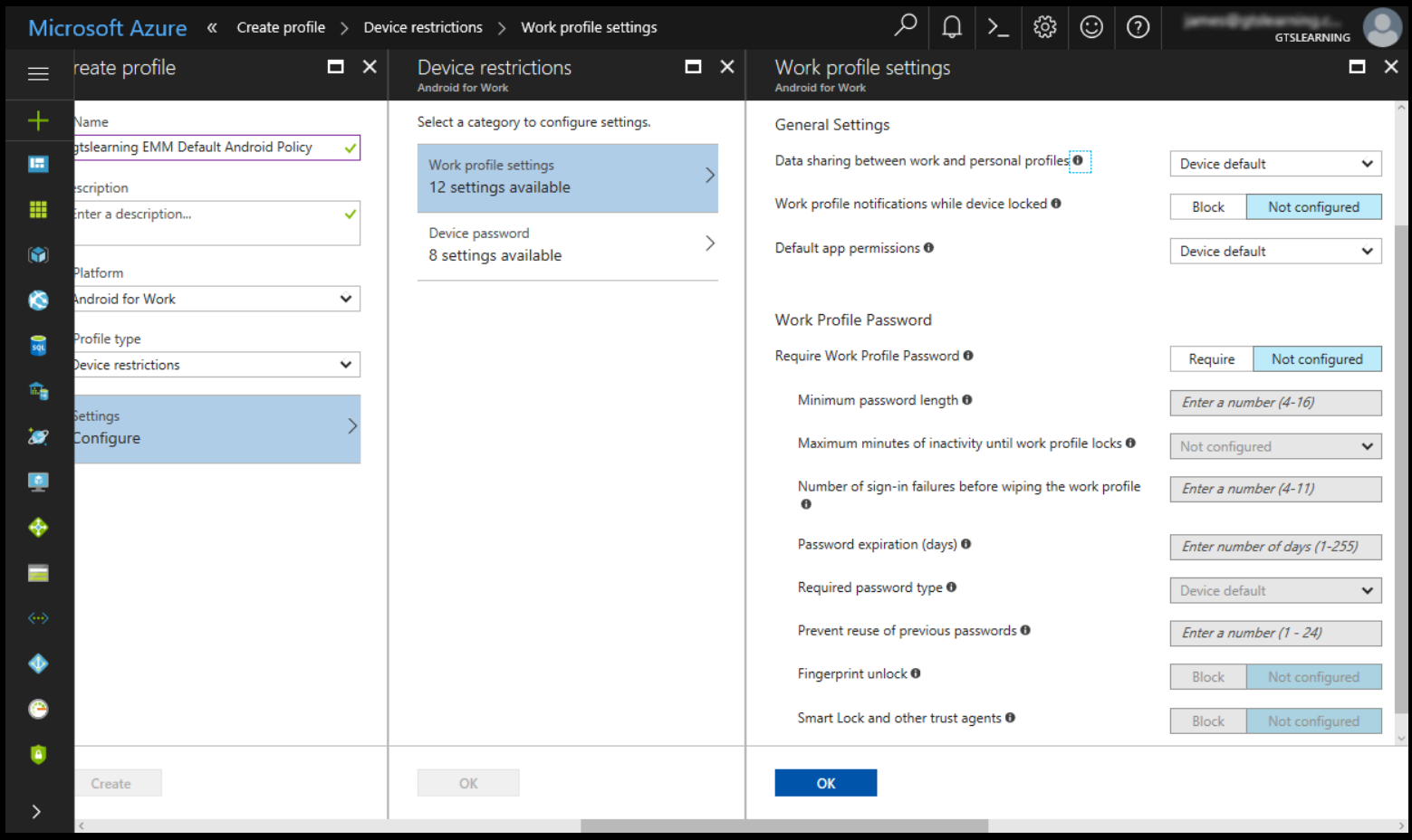
Screenshot courtesy of Microsoft.

20.1.5 Two-factor Authentication

Most smartphones and tablets are single-user devices. Access control can be implemented by configuring a screen lock that can only be bypassed using the correct password, personal identification number (PIN), or swipe pattern. Many devices now support biometric authentication, such as a fingerprint or facial recognition.

When enrolled with an enterprise management app, the user might have to re-authenticate to access the corporate workspace. The corporate policy might require stronger authentication methods, such as the use of two-factor authentication. 2FA means that the user must submit two different kinds of credentials to authenticate, such as both a fingerprint and a PIN. Alternatively, the account might be configured with an authenticator device or app, a trusted email account, or a registered phone number. When the user uses a new device to access the account, or when the workspace policy requires 2FA, the user must first authenticate normally, using a fingerprint, for instance. If this is accepted, an email, text, or phone call is generated as a notification on the trusted authenticator app or device. The message may include a one-time password code for the user to input to confirm that the sign-in attempt is legitimate.

Figure 1. Configuring authentication and profile policies using Intune EMM



Screenshot courtesy of Microsoft.

20.1.6 Mobile Data Security

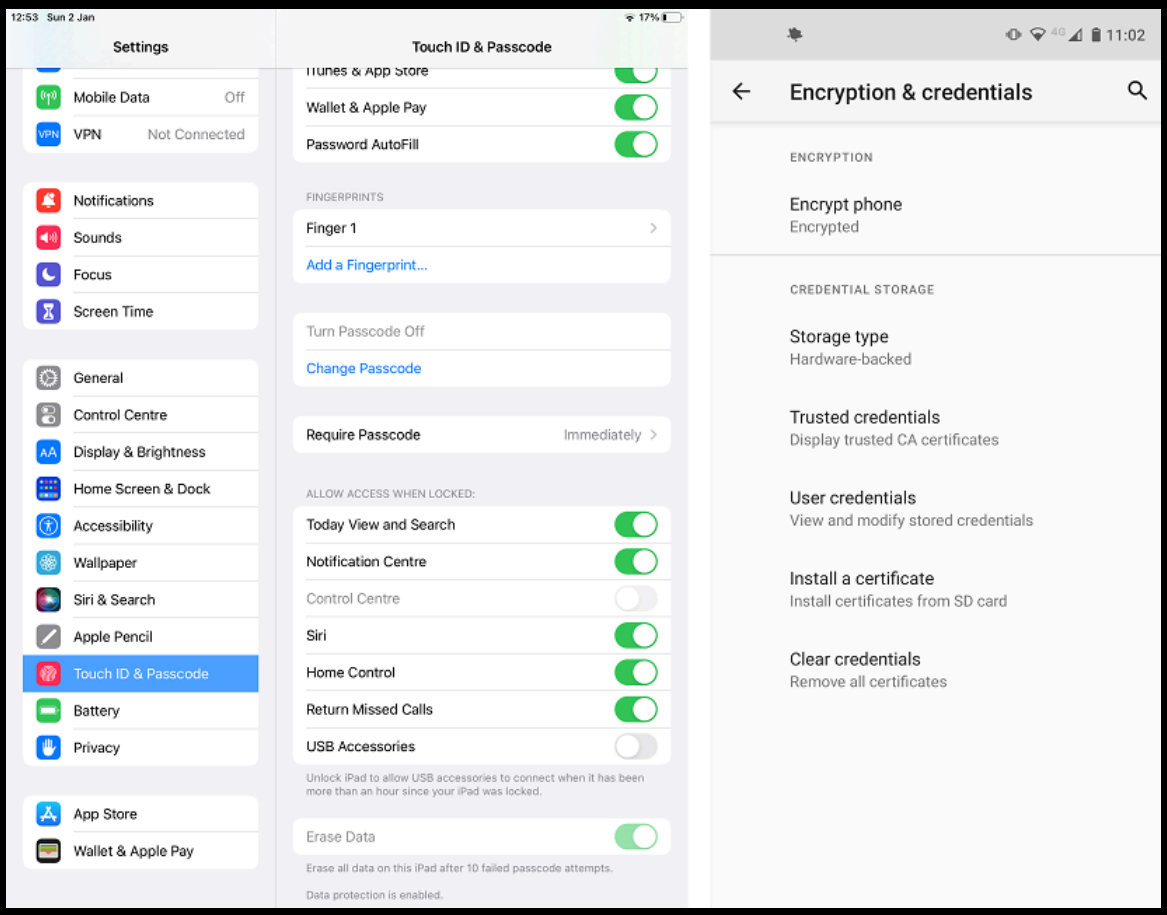
If a mobile device is lost or stolen, mechanisms exist to recover it and prevent misuse or data loss.

Device Encryption

All but the earliest versions of mobile device OSs for smartphones and tablets provide some type of default encryption.

- **In iOS:**
  - **All user data is encrypted by default, with the key stored on the device. This allows for quick data wiping by deleting the key.**
  - **Email data and apps using "Data Protection" undergo additional encryption with a key derived from the user's credentials, enhancing security if the device is stolen. Not all data, like contacts and SMS messages, is encrypted with "Data Protection."**
  - **Data Protection encryption is automatically enabled when a passcode lock is set.**
- **In Android:**
  - **Encryption options vary by version (source.android.com/security/encryption). As of Android 10, full disk encryption is not used due to performance concerns. Instead, user data is encrypted at the file level by default when a secure screen lock is configured.**

Figure 1. In iOS, the data protection encryption option is enabled when a passcode is configured (left, at bottom). Android uses file encryption for user data and settings when a lock is configured (right).



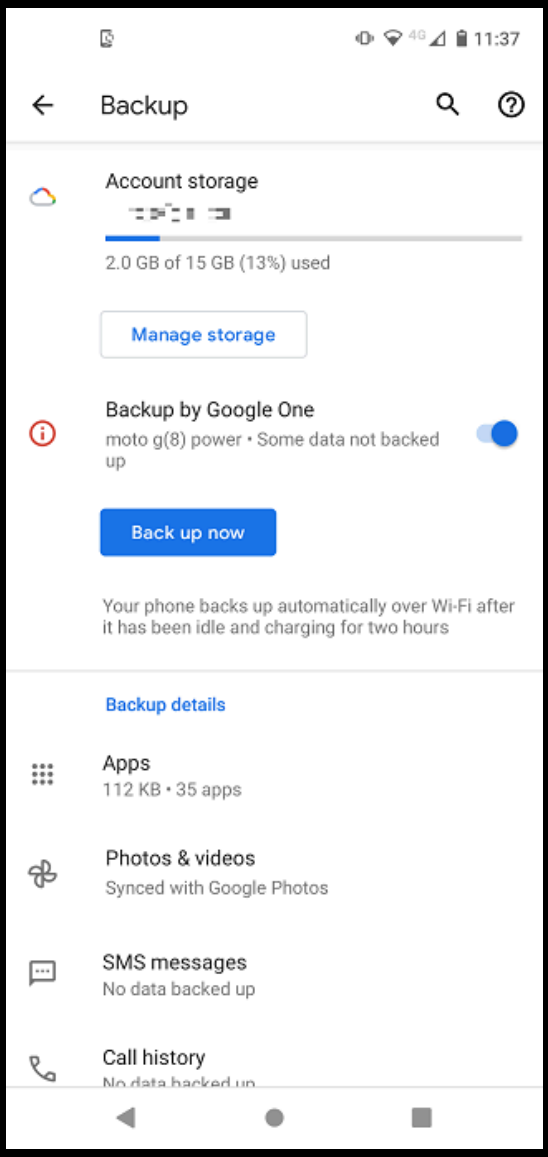
Description

The image shows two screenshots of mobile device settings. On the left is an iOS device's "Touch ID & Passcode" settings screen. It includes options for managing fingerprints, turning the passcode on or off, changing the passcode, and requiring the passcode immediately. Below, there are toggles to allow access to features like Today View, Notification Centre, Control Centre, Siri, Home Control, and Return Missed Calls when the device is locked. There is also an option to erase all data after 10 failed passcode attempts. On the right is an Android device's "Encryption & Credentials" settings screen. It shows the encryption status as "Encrypted" and provides options for credential storage, including storage type (hardware-backed), viewing trusted credentials, managing user credentials, installing a certificate, and clearing credentials.

Remote Backup Applications

Most mobile devices are linked to vendor cloud services (iCloud for iOS, Google Sync for Android, OneDrive for Microsoft) for automatic remote backup of data, apps, and settings. Users can choose alternative backup providers, such as OneDrive on Android or third-party services like Dropbox.

Figure 2. Using Google's default remote backup service



Screenshot courtesy of Google One™ subscription service, a trademark of Google LLC.

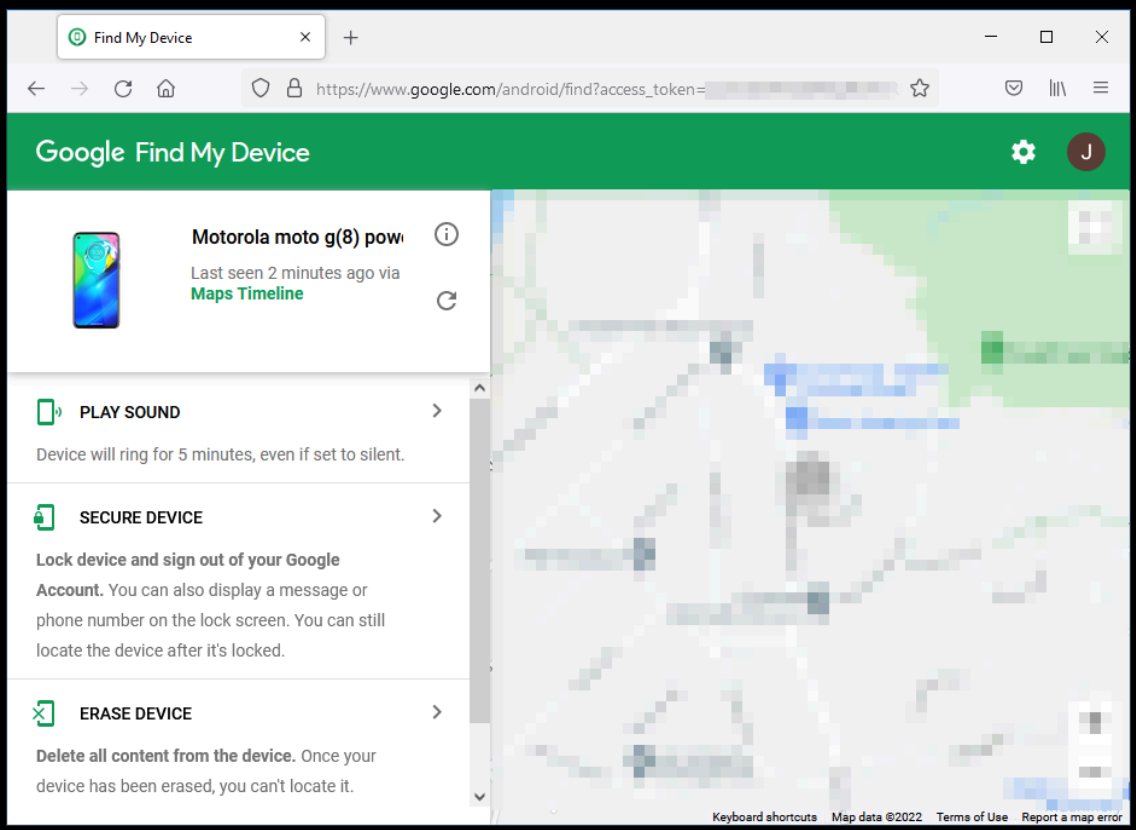
Devices can also be backed up to a PC. iOS supports backups to macOS or Windows via Finder or iTunes. MDM software can be configured to automatically back up user devices or specific container workspaces.

20.1.7 Locator Apps and Remote Wipe

Most smartphones and many tablets are equipped with GPS receivers, which determine a device's position using satellite information. GPS requires line-of-sight and does not work indoors. High-accuracy location services use GPS along with Wi-Fi access points and Bluetooth beacons to calculate a device's location.

Both Android and iOS have built-in "find-my-phone" features that use location services to track lost or stolen devices. Third-party antivirus and MDM software also support this functionality. Once set up, the device's location can be tracked from any web browser when it is powered on.

Figure 1. Find My Device app to locate an Android device



Locator apps can remotely lock the device, display a "Please return" message, call the device at full volume, disable features like the wallet, and prevent changes to the passcode or disabling of location/network services.

If a device is irretrievably lost, a remote wipe can protect data and account credentials by performing a factory reset, or device wipe, clearing all data, apps, and settings.

For devices enrolled in MDM, an enterprise wipe can be performed to remove corporate accounts and files while leaving personal apps, accounts, settings, and files intact, protecting corporate data without affecting personal information.

20.2 Troubleshoot Mobile OS and App Software

Core 2 Exam Objectives Covered

- **3.2 Given a scenario, troubleshoot common mobile OS and application issues.**

Several drivers have reported that their mobile devices are experiencing slow performance and frequent app crashes, which are affecting their ability to update shipment statuses in real-time. Your task is to troubleshoot these performance issues and ensure that all devices are running efficiently.

Learning Outcomes

As you study this lesson, answer the following questions:

- **What are the common troubleshooting steps for resolving performance issues on mobile devices?**
- **How can rebooting a mobile device help resolve temporary performance or stability issues?**
- **What is the process for performing a factory reset on iOS and Android devices, and when should it be used?**
- **How can you identify and address battery life issues on mobile devices?**
- **What steps should you take if an OS update fails to install on a mobile device?**
- **How can you troubleshoot app issues, such as apps failing to launch or crashing frequently?**

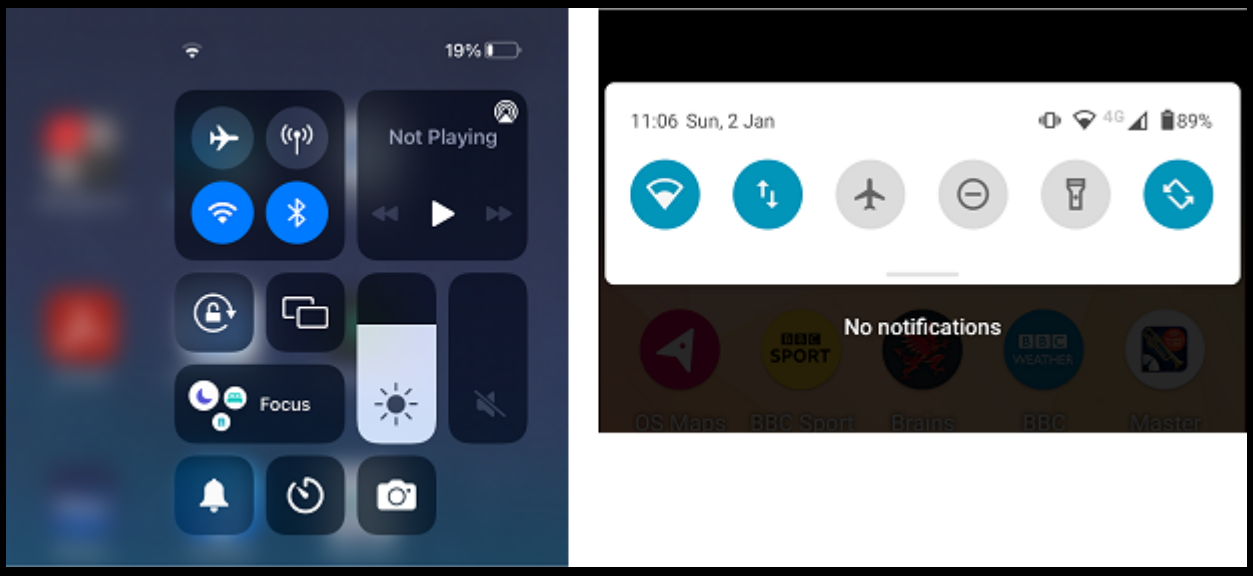
20.2.1 Mobile Device Troubleshooting Tools

When troubleshooting mobile devices, the Settings app is frequently used. Its layout differs between iOS and Android and can vary with different versions.

- **Android: Access the notification bar by swiping down from the top of the screen and view all apps by swiping up from the bottom.**
- **iOS: Access the Control Center by swiping down from the top-right corner on newer models or up from the bottom on older models.**

Always refer to the latest device-specific instructions, as interfaces may change with updates.

Figure 1. Access the iOS Control Center (left) by swiping from the top-right and Android notification drawer by swiping from the top



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

Reboot

Rebooting a mobile device can often resolve temporary performance or stability issues. Unlike leaving the device in sleep mode, powering it off closes all applications and clears RAM without affecting stored data and settings. This soft reset is effective for restoring unresponsive or frozen systems and should be one of the first steps when dealing with malfunctioning apps or slow performance. If the touchscreen is unresponsive, perform a soft reset or force restart by pressing a combination of the side/top and volume buttons—refer to the device's support documentation for specifics.

For Android devices, booting into Safe Mode disables third-party apps while keeping core services running, aiding in troubleshooting.

Factory Reset

A factory reset erases all user data, apps, and settings from a device. Afterward, the device must be manually set up with a new user account and apps or restored from a backup. Ensure the device is fully charged or connected to a power source before performing a reset.

- **iOS: Use the factory reset option found in the General section of Settings.**
- **Android: Follow device-specific instructions. On stock Android, initiate a reset from the System > Advanced section in Settings.**

Note:

You may need to sign in immediately after a factory reset to prevent unauthorized access. Ensure you have the necessary account credentials and avoid resetting within 72 hours of changing your account password.

Battery Life Issues

Battery life issues on mobile devices could come from a variety of factors. Background app activity can significantly drain the battery, so check which apps consume the most power and disable unnecessary background processes. Adjust screen brightness and timeout settings to conserve energy, and limit location services to essential apps only. Frequent push notifications and constant data syncing can also impact battery life, so review and adjust these settings.

Check battery health on iOS via Settings > Battery > Battery Health, or use third-party apps on Android. Turn off power-hungry features like Bluetooth, Wi-Fi, and mobile data when not in use. Utilize battery-saver modes available on both iOS and Android to extend battery life when needed. Also, avoid exposing the device to extreme temperatures, as they can affect battery performance.

20.2.3 Troubleshoot Device and OS Issues

If rebooting doesn't resolve the issue, follow these troubleshooting steps. If problems persist, consider a factory reset.

OS Fails to Update

An OS update failure can expose the device to security vulnerabilities. Follow these steps:

1. **Verify update compatibility with your device model on the vendor's website.**
2. **Verify the device lifecycle and confirm if it is still supported by the vendor.**
3. **Ensure the device is connected to a power source and Wi-Fi, as updates may be blocked by low battery or metered networks.**
4. **Restart the device and attempt the update again.**
5. **Check for sufficient free space:**
    - **On iOS: Go to Settings > General > Storage.**
    - **On Android: Go to Settings > Storage.**

Device Randomly Reboots

Random reboots can occur due to overheating, low battery, or faulty hardware. To address this, first check the battery health using the Settings menu or third-party diagnostic apps to identify any hardware faults. If hardware issues are not the cause, ensure the device has sufficient storage space and verify that the OS and apps are up-to-date. Additionally, try to isolate the problem to a specific faulty app and uninstall it to see if the issue resolves.

Device Is Slow to Respond

If hardware issues like throttling from high temperatures or low battery are ruled out, a device may be slow to respond due to resource constraints, such as too many open apps or poorly optimized apps consuming excessive memory. A reboot can provide a temporary fix. For persistent issues, identify if a specific app is causing the slowdown or free up space by removing unnecessary data or apps.

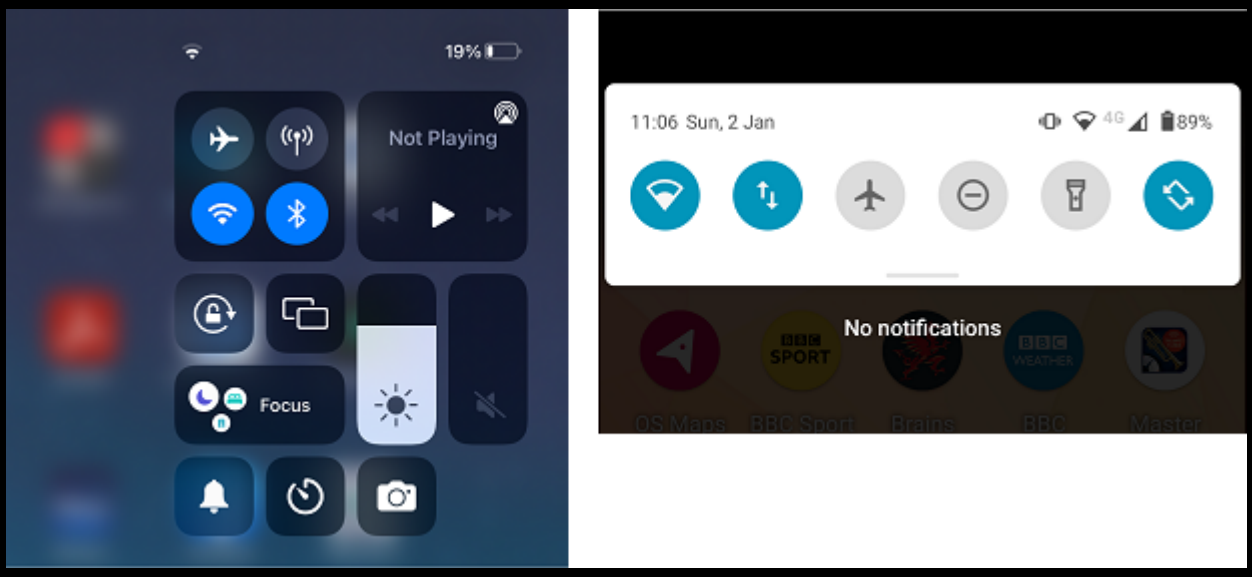
Consider recently installed apps, especially those running background tasks or displaying real-time content in widgets, as they can impact performance. Use Battery settings to check which apps are using the most resources, or install a third-party system monitor app for detailed utilization information.

Note: While vendors aim to support devices for as long as possible, major or minor OS updates can significantly affect performance on older models. Unfortunately, rollback options for updates are typically unavailable, so reporting the issue and awaiting a vendor fix is often the only recourse.

Screen Does Not Autorotate

If the screen fails to autorotate, it may be due to a hardware issue. To eliminate simple causes, follow these steps:

1. Check the notification drawer or Control Center to ensure rotation lock is not enabled.
   Figure 1. In iOS (left), enabling the rotation lock from Control Center prevents the device from autorotating. In Android (right), enabling the autorotate button allows the screen to reorient automatically, while disabling it locks the orientation



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

2. Ensure the screen is not being touched, as this can prevent rotation.
3. Some apps are designed for a single orientation and may interfere with others. Close apps using the task list:

- **On iOS, double-tap the Home button or swipe up from the bottom to the middle of the screen.**
- **On Android, tap the square button in the navigation bar.**

Note:

On Android, when autorotate is disabled, an icon appears in the navigation bar for manual orientation changes. On iOS, manual control can be added via AssistiveTouch in Accessibility settings.

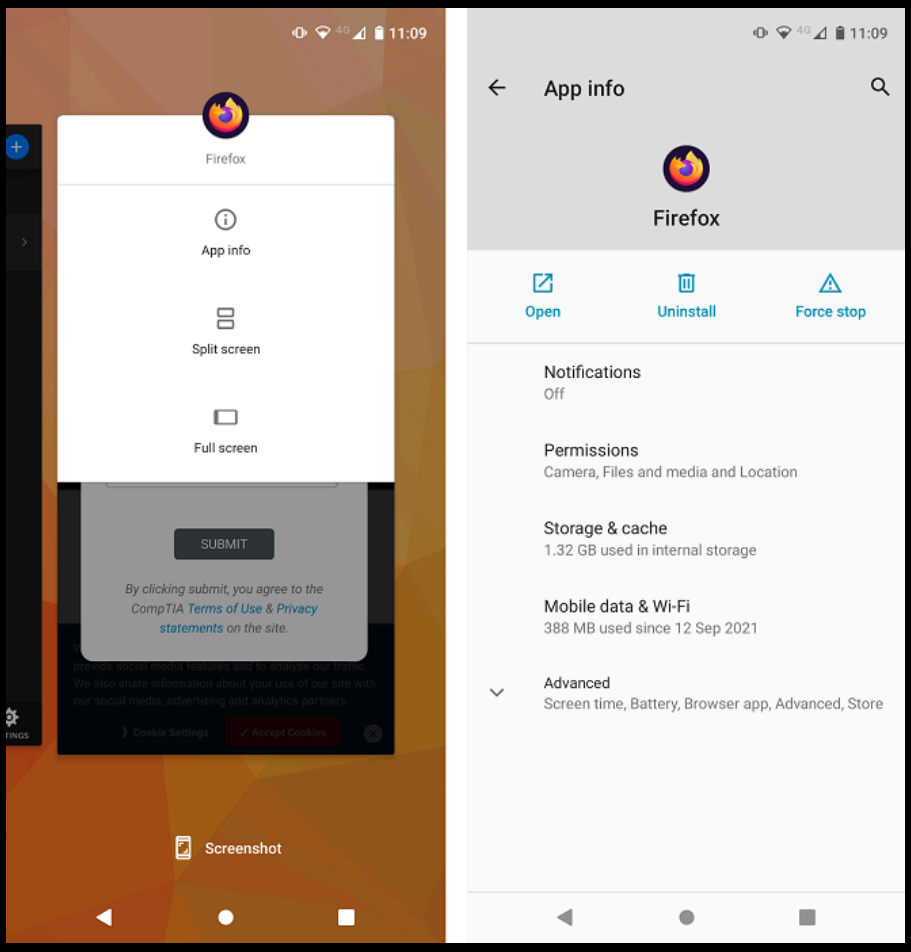
20.2.4 Troubleshoot App Issues

Mobile operating systems use advanced memory management to run multiple apps efficiently, allocating resources while conserving power. Apps transition between foreground (active use), background (network/resource access), and suspended (no resource use) states.

If an app fails to launch, close, or crashes, try force-stopping it:

- **Android: Go to Settings > Apps, select the app, and tap Force Stop or Disable to make it unavailable.**
- **iOS: Swipe up from the bottom of the screen to access the App Switcher, then swipe the app card up to close it.**

Figure 1. In Android, tap the square multitasking button (bottom-right) to view open apps, then swipe up to remove them



Screenshot courtesy of Android platform, a trademark of Google LLC.

If issues persist, clear the app cache (in Android, use the Clear Cache option under App info), reboot the device, and check for app updates in the store. If an app fails to update ensure it is compatible with the current OS version, and verify sufficient storage and internet connection.

If problems continue, uninstall and reinstall the app:

- iOS: Tap and hold the app until it wiggles, press the X icon, and confirm deletion. Note that Default apps cannot be uninstalled.
- Android: Go to Settings > Apps to uninstall or disable apps. Alternatively, long-press the app icon on the home screen and drag it to Uninstall (dragging it to Remove just hides the app icon).

Previously used and purchased apps are listed in the user's account and can be reinstalled via the store.

When an application fails to install on iOS or Android devices, several troubleshooting steps can help resolve the issue.

For iOS:

1. Ensure the device has a stable internet connection and sufficient storage space by checking Settings > General > iPhone Storage.
2. Restart the device and verify that it is running the latest iOS version via Settings > General > Software Update.
3. Sign out and back into your Apple ID to refresh the session, and ensure your payment method is valid.
4. You can also clear the App Store cache by tapping any bottom icon 10 times and then retry the installation.

For Android:

1. Confirm a reliable internet connection and adequate storage space through Settings > Storage.
2. Restart the device and update the Android OS if needed via Settings > System > System Update.
3. Clear the Google Play Store cache by navigating to Settings > Apps > Google Play Store > Storage, and ensure your Google account is synced correctly.
4. Check that your payment method is up-to-date, then attempt the installation again.

Note:

Mobile Device Management (MDM) software may restrict app functionality based on security policies, such as disabling the camera in certain locations.

Note:

For iOS devices that don't update wirelessly, connect to a macOS device (using Finder in macOS Catalina or later) or a Windows PC (using iTunes) with a Lightning cable or Lightening-to-USB cable.

20.2.5 Troubleshoot Connectivity Issues

Connectivity problems with Wi-Fi, Bluetooth, and other wireless technologies are common on mobile devices. To address these issues effectively, it's important to determine whether the problem stems from hardware interference, configuration errors, or network compatibility. Leveraging apps, programs, and management interfaces to map out your network can also aid in troubleshooting and ensuring proper configuration.

Signal Strength and Interference

Radio signals can be weakened by distance, interference, and physical barriers like walls. Mobile radios are less powerful than those in computers, and low battery can further reduce signal strength. Move closer to the access point or Bluetooth device and consider removing the device case or adjusting its position to improve reception.

Configuration Issues

Ensure the device is not in airplane mode and that Wi-Fi and Bluetooth are enabled. Check network settings and Bluetooth pairing information in Settings. If needed, forget and reconnect to the network or device.

For Wi-Fi connectivity, ensure the access point supports the same 802.11 standard as the device. For instance, a smartphone with an 802.11n adapter cannot connect to an access point set to 802.11ac only; the access point should be in compatibility mode. Additionally, some mobile devices only support 2.4 GHz radios and cannot connect to 5 GHz networks.

Troubleshooting NFC

Near-field communication (NFC) issues often arise during contactless payments. Ensure the device is unlocked to authorize payments and that NFC is enabled for the wallet app. Confirm that airplane mode is off. If problems persist, hold the device closer to the card reader and maintain contact for a longer duration.

Troubleshooting AirDrop

AirDrop is an iOS feature that allows file transfer between iOS and macOS devices over Bluetooth, Wi-Fi, or cellular connections. Ensure AirDrop is enabled and properly configured under Settings > General > AirDrop. The sender should be in the recipient's contacts or AirDrop should be set to receive files from everyone. Make sure the devices are within Bluetooth range.

Note:

Android offers a similar feature called Nearby Share accessible via Settings > Google > Devices > Nearby Share.

20.3 Troubleshoot Mobile OS and App Security

Core 2 Exam Objectives Covered

- **3.3 Given a scenario, troubleshoot common mobile OS and application security issues.**

The company has detected unauthorized apps on some devices which pose a security risk. Your task is to identify and remove these apps, ensure that all devices are secure, and prevent future unauthorized installations.

Learning Objectives

As you study this lesson, answer the following questions:

- **What are the security concerns associated with root access and jailbreaking on mobile devices?**
- **How can Mobile Device Management (MDM) solutions detect and prevent access to rooted or jailbroken devices?**
- **What are the risks of installing apps from untrusted sources, and how can they be mitigated?**
- **What steps should you take to address unexpected application behavior that may indicate a security threat?**
- **How can you protect against data leakage and unauthorized location tracking on mobile devices?**

20.3.1 Root Access Security Concerns

In both iOS and Android, the default user account can install apps and configure settings but is restricted from making system-level changes. Users seeking to bypass these restrictions often resort to privilege escalation methods:

- **Root Access (Android): This involves gaining administrative control over the device. Some vendors offer authorized methods to access root, while others require exploiting vulnerabilities or installing custom firmware (custom ROMs). Rooting can disable security features, compromising the device's integrity and any management software.**
- **Jailbreaking (iOS): iOS is more restrictive, so the term jailbreaking is used to describe gaining root privileges, allowing sideloading apps, changing carriers, and customizing the interface. This is typically done by booting with a patched kernel, often requiring a tethered connection to a computer. Jailbreaking can leave security measures disabled, compromising the device's security.**

Both rooting and jailbreaking subvert OS security controls, leaving devices vulnerable. Mobile Device Management (MDM) solutions can detect rooted or jailbroken devices and prevent access to enterprise apps, networks, or workspaces. They can also block devices with custom firmware lacking valid signatures.

Devices can be placed into developer mode, granting access to advanced configuration settings and diagnostic data. While developer mode doesn't inherently weaken security, it should be used exclusively for app development and not enabled routinely, as it can be exploited to install unauthorized apps. Mobile Device Management (MDM) systems can often be configured to block devices with developer mode enabled.

20.3.2 Mobile App Source Security Concerns

Trusted app sources are managed by service providers that authenticate developers and issue certificates for app signing, ensuring apps are secure. Service providers may also analyze submitted code to prevent security or privacy risks and enforce policies, such as prohibiting adult content or duplicate core OS functions.

App Spoofing

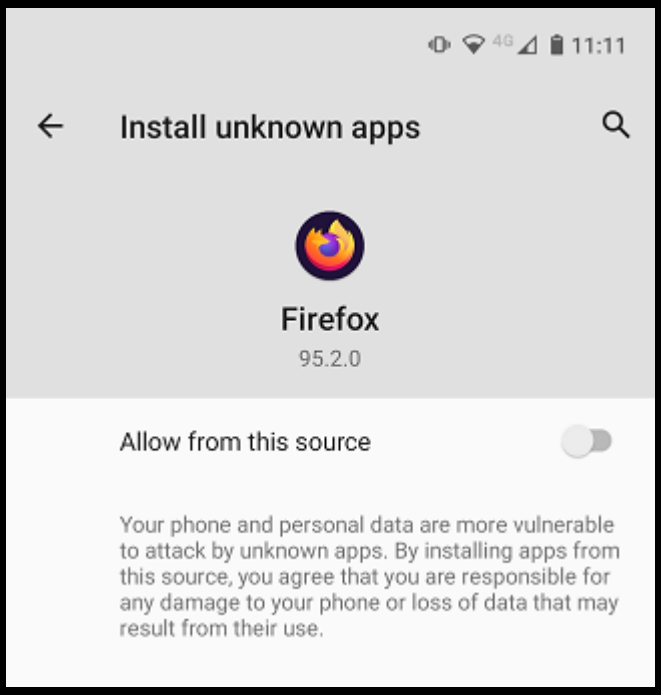
Despite robust app store security, rogue developers may publish malicious apps disguised as legitimate ones. These apps often mimic popular apps with similar names and use fake reviews to appear credible. Common targets include VPNs, fake antivirus/ad blockers, and dating apps. Even when using an approved store, users should exercise caution, especially if an app requests unrelated permissions.

Enterprise Apps and APK Sideloading

Mobile operating systems typically restrict app installations to official stores (App Store for iOS and Play Store for Android). While this model suits most consumers, it may not be ideal for enterprises needing to distribute custom corporate apps privately. Apple addresses this with enterprise developer and distribution programs via Apple Business Manager, while Google offers Managed Google Play for private app distribution. These solutions enable Mobile Device Management (MDM) suites to push apps from private channels directly to devices.

Unlike iOS, Android allows users to select different stores and install apps from third-party sources if enabled. This process, known as sideloading, involves downloading and installing apps using the .APK file format. While convenient, enabling unknown sources weakens device security. It's crucial to ensure only legitimate enterprise apps are sideloaded and to monitor devices for unauthorized apps. MDM can be configured to prevent the use of third-party stores or sideloading, effectively blocking unapproved app sources.

Figure 1. In Android, each app has an Install unknown apps toggle



Screenshot courtesy of Android platform, a trademark of Google LLC and Mozilla.

Bootleg App Stores

Bootleg apps mimic legitimate ones and may tempt users to enable unknown sources for sideloading, infringing copyrights, and exposing devices to malware. On iOS, developer tools can install apps outside the App Store without jailbreaking, posing similar risks.

Overall, maintaining app source security involves using trusted stores, exercising caution with app permissions, and leveraging MDM to enforce policies and monitor app installations.

20.3.3 Mobile Security Symptoms

While antivirus software for mobile OSs exists, its reliability can vary. It's important to be aware of general malware symptoms, which often resemble those on PCs:

- **Excessive Ads: Free apps are typically supported by advertising revenue, so a high volume of ads isn't always indicative of a malicious app. However, if ads appear unexpectedly, display in the browser, open persistent pop-ups, or show a high level of unauthorized personalization, this could suggest tracking or spyware activity.**
- **Fake Security Warnings: Scareware uses these alerts to trick users into installing apps or granting additional permissions to Trojan apps.**
- **Degraded Response Time: Malware may run background processes like data collection or cryptomining, leading to excessive power drain and high resource utilization, causing other apps to slow down.**
- **Limited/No Internet Connectivity: Malware may corrupt DNS settings or search providers to execute redirection attacks, leading users to spoofed sites. This can disrupt access to legitimate sites, trigger certificate warnings, and slow down network performance.**

Unexpected Application Behavior

Bootleg or spoofed apps often act like Trojans. While they may deliver expected functionality, such as games or VPNs, they can secretly operate as spyware, harvesting data from the device. This behavior may appear as unexpected permission requests or unauthorized use of the camera and microphone. If the app is transferring files from the device, it may result in high network traffic. Excessive bandwidth usage can also indicate the device is compromised, possibly being used for DDoS attacks, mass mailing, or cryptomining. The app might even attempt to use premium-rate call services. Most devices offer data usage monitoring and limit triggers to alert users when limits are reached. This feature not only helps avoid large data bills but also encourages users to review the data usage of each app to assess its legitimacy.

Leaked Personal Files/Data

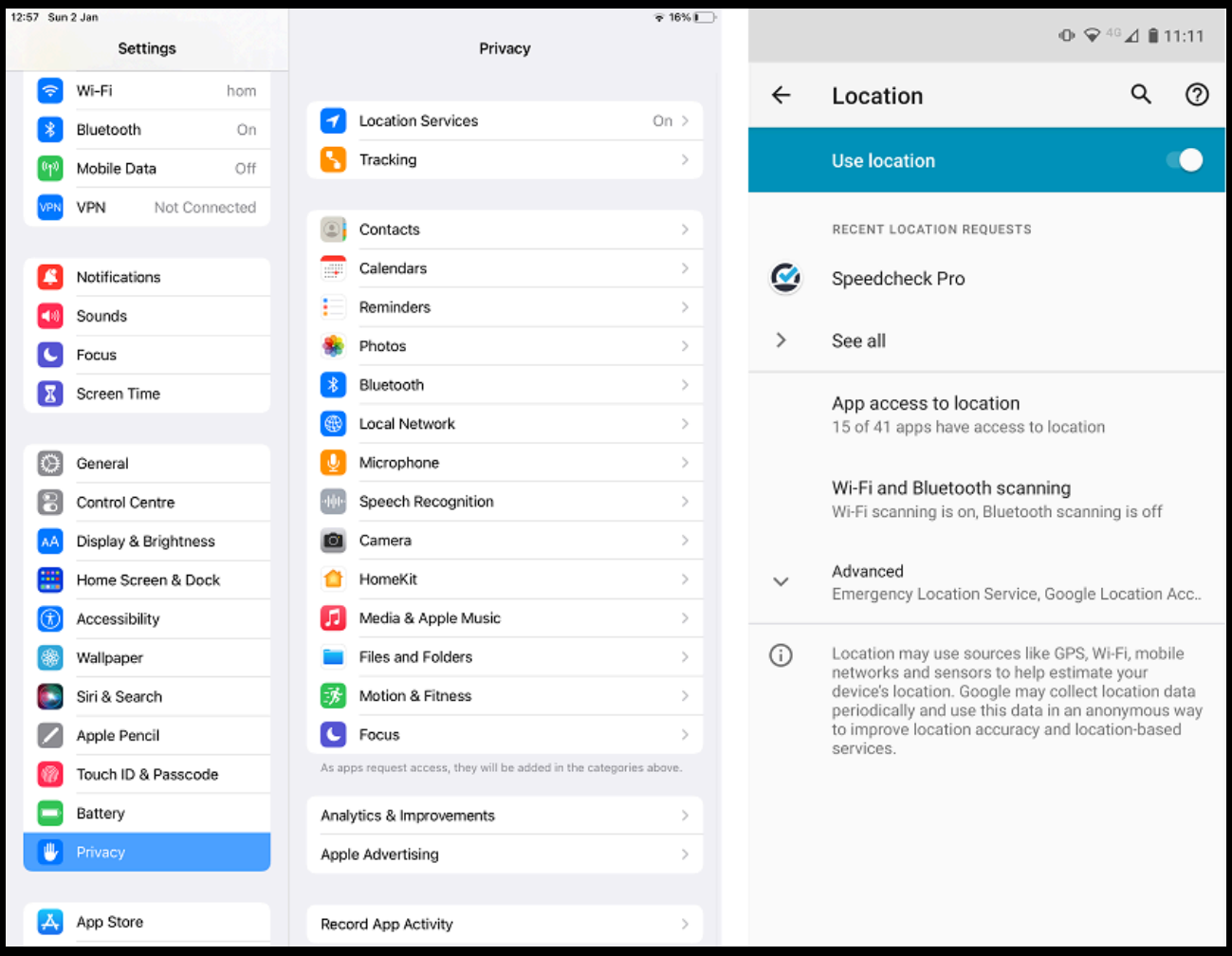
When a device is compromised, personal or corporate data may be sold and appear on forums or file-sharing sites. If data leakage occurs, all potential source devices must be quarantined and investigated to identify the breach's origin.

Users should watch for 2-step verification alerts indicating new device access attempts or unexpected password changes. Data breaches often provide hackers with authentication credentials and personal information, enabling them to access email accounts. Once an email account is compromised, hackers can infiltrate other accounts lacking secondary authentication.

Websites or services experiencing data breaches should promptly notify users. Breach notification services can alert users to the misuse of email addresses and account details. To protect personal information, users should employ strong security practices, such as using unique passwords for different accounts.

Unauthorized location tracking can expose sensitive information to third parties. While many apps collect location data for targeted advertising, rogue apps might misuse it for crimes like burglary.

Figure 1. Managing location services in iOS (left) and Android



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC

Note:

Criminals can also obtain location information from geotagged online photos. They can determine where someone lives and identify vacation times from social media posts. Users should be trained to remove geotagging information from images before posting them online to mitigate these risks.

21.0 Using Data Security

As a CompTIA A+ technician, you will usually perform support tasks within the context of a company's operational procedures. These procedures include performing data backups and recovery, handling different types of sensitive data, and even integrating artificial intelligence into the organization's applications and workflows.

This module will help you to identify the technologies and best practices that underpin these important procedures.

Prepare for A+ Core 2 by:

- **Implementing backup and recovery.**
- **Explaining data handling best practices.**
- **Explaining the basics of Artificial Intelligence.**

21.1 Data Backup and Recovery

Core 2 Exam Objectives Covered

- **4.3 Given a scenario, implement workstation backup and recovery methods.**

Your organization has tasked you with developing an appropriate data backup and recovery plan. The organization wants you to make sure that all critical data is backed up and can be quickly recovered in case of a catastrophic loss.

In this lesson, you will learn the different methods that can be used to back up data, how to properly store data backups, and data recovery best practices.

Learning Outcomes

As you study this lesson, answer the following questions:

- **What is the purpose of backing up data?**
- **What are the types of backup chains?**
- **What is the GFS backup scheme?**
- **When would an in-place recovery be used instead of recovering to an alternate location?**

21.1.1 Backup Operations

Data backup is a system maintenance task that enables you to store copies of critical data for safekeeping. Backup protects against loss of data due to disasters such as file corruption or hardware failure. Data recovery is a task that enables you to restore user access to lost or corrupt data via the backup.

Most large organizations will implement a structured backup scheme that includes a backup schedule and specifications for which files are backed up, where the backup is stored, and how it can be recovered.

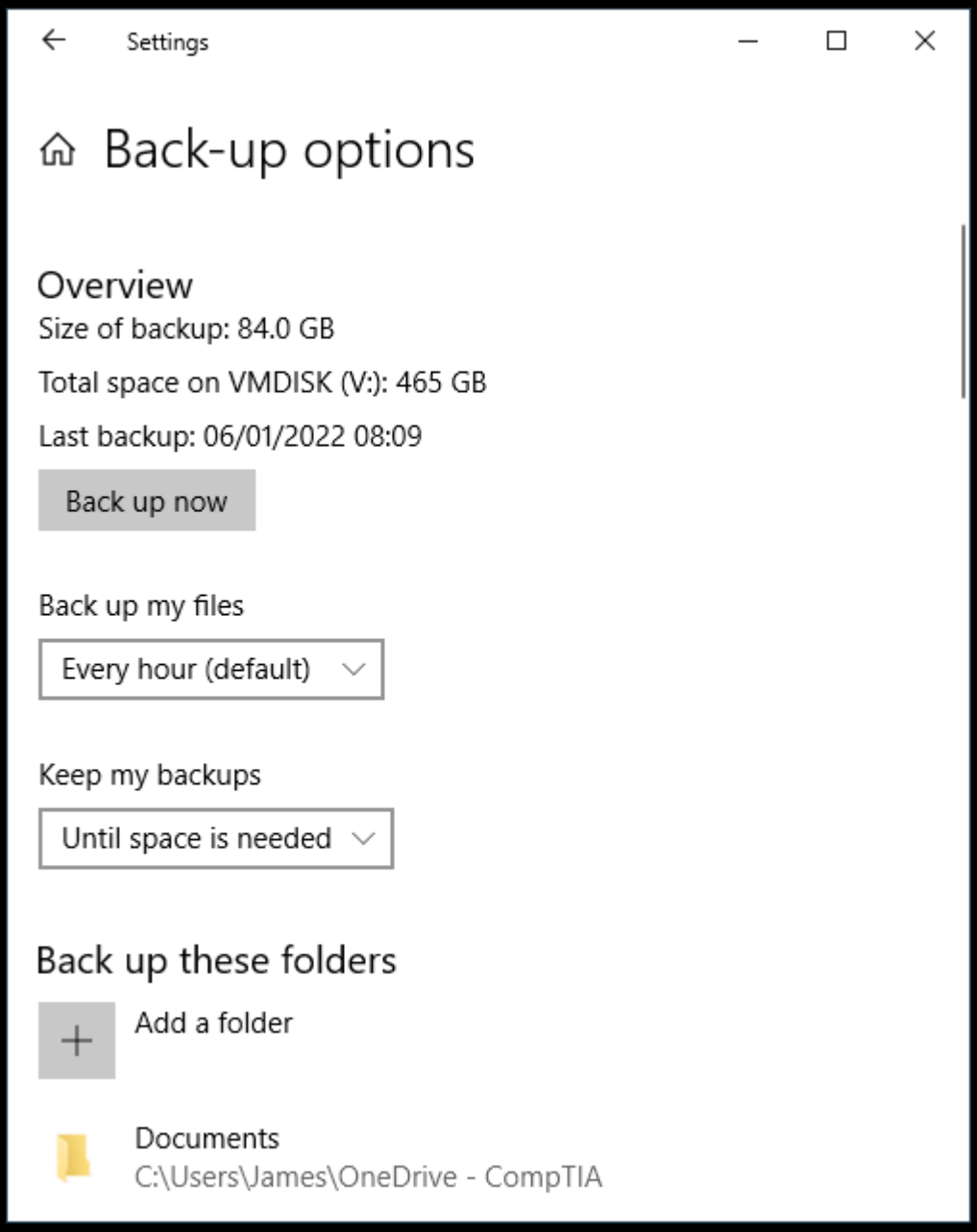
Note:

When a computer is connected to a network, it is bad practice for a user to store data locally (on the client PC's fixed disks). Network home folders and the use of scripts to copy data can help users transfer data to a file server, where it can be backed up safely.

Personal backups are necessary for home users or on workgroups, where no central file server is available. In this scenario, the backup software supplied with Windows is serviceable. Most home users will back up to external hard drives or use some sort of cloud-based storage.

In Windows, user data backup options are implemented via the File History feature, which is accessed through Settings Update & Security Backup . You can configure a local drive or network folder as the target for storing backup files. You can choose which folders and files to include or exclude from the backup job plus a schedule for running the job.

Figure 1. Configuring File History backup options via Windows Settings



If you need to restore a file or folder, you can either use the Previous Versions tab in the object's Properties dialog box or use the File History applet to restore multiple files.

The Backup and Restore Center control panel tool provides an alternative backup manager. It can also be used to make image backups of the entire operating system, rather than just data file backups. Using OneDrive, through syncing, is another alternative for backing up data.

21.1.2 Backup Methods

When considering a file server or database server, the execution and frequency of backups must be carefully planned and guided by policies. Each backup job records data as it was at a certain point in time. As each backup job might take up a lot of space and there is never limitless storage capacity, there must be some system to minimize the amount of data occupying backup storage media while still giving adequate coverage of the required recovery window.

Two main factors govern backup operations:

- Frequency is the period between backup jobs. The frequency configuration reflects how much lost work can be tolerated. For example, if employees can recall and input the previous day's work on document files, a daily backup will meet the requirement. If the edits are much more difficult to reconstruct, the backup frequency might need to be measured in hours, minutes, or seconds.
- Data retention is the period that any given backup job is kept for. Short-term retention is important for version control and for recovering from malware infection. Consider the scenario where a backup is made on Monday, a file is infected with a virus on Tuesday, and when that file is backed up later on Tuesday, the copy made on Monday is overwritten. This means that there is no good means of restoring the uninfected file. In the long term, data may need to be stored to meet legal requirements or to comply with company policies or industry standards. Conversely, regulations might require that data *not* be kept for longer than necessary.

Backup Chains

The requirements for backup frequency and retention must be managed against the capacity of the backup media and the time it takes to complete a backup job. These requirements are managed by using different types of jobs in a backup chain. The main types of backups are full only, full with incremental, and full with differential:

- "Full only" means that the backup job produces a file that contains all the data from the source. This means that the backup file is nominally the same size as the source, though it can be reduced via compression. A full backup has the highest storage and time requirements but has the least recovery complexity as only a single file is required.
- "Full with incremental" means that the chain starts with a full backup and then runs incremental jobs that select only new files and files modified since the previous job. An incremental job has the lowest time and storage requirement. However, this type of chain has the most recovery complexity as it can involve two or more jobs, each of which might be stored on different media.
- "Full with differential backup"means that the chain starts with a full backup and then runs differential jobs that select new files and files modified since the original full job. A differential chain has moderate time and storage requirements and slightly less recovery complexity than incremental as it requires a maximum of two jobs (the full backup plus the differential job).

Type	Data Selection	Backup Job Time and Storage Requirement	Recovery Complexity	Archive Attribute
Full	All selected data regardless of when it was previously backed up	High	Low (single job)	Cleared
Incremental	New files and files modified since last backup job	Low	High (multiple jobs)	Cleared
Differential	New files and files modified since last full backup job	Moderate	Moderate (two jobs)	Not cleared

Note: Windows uses an archive attribute to determine the backup status. Linux doesn't support a file archive attribute. Instead, a date stamp is used to determine whether the file has changed. Most software can also do copy backups. These are made outside the chain system (ad hoc) and do not affect the archive attribute.

Synthetic Full Backup

A synthetic full backup is similar to a Full backup, but instead of scanning the system again to create the full backup, the system will use the original full backup and then add in the data from the incremental backups to create a new full up-to-date backup.

This backup type is typically quicker to create and requires less storage, but if any of the incremental backups are corrupted, the synthetic full backup will be affected.

Restoring data from a synthetic full backup is quicker than restoring from incremental backups, but might take longer than restoring from a full backup. This is because the backup software needs to assemble the synthetic full backup from its components before the data can be restored.

21.1.4 Backup Media Requirements

A backup rotation scheme allows some media to be reused once the retention period of the job stored on it has expired. Rotation is most closely associated with the use of tape media but can be applied to disk devices too. There are many backup rotation schemes, but the most widely used is grandfather-father-son (GFS.)

Grandfather - Father - Son (GFS) Scheme

The GFS scheme labels the backup tapes in generations. Son tapes store the most recent data and have the shortest retention period (one week, for example). Grandfather tapes are the oldest and have the longest retention period (one year, for example). Assuming a single tape has sufficient capacity for each job and no weekend backups, a GFS scheme could be implemented as follows:

1. A full backup is performed each week on Friday night to one of the tapes marked "Father." As some months will have five Fridays, this requires five tapes labeled and dedicated to the father role.

2. Incremental Backups are made each day to a tape marked "Son," using whatever frequency is required (every 15 minutes or every hour, for instance). The five son tapes are reused each week in the same order.

3. A full backup is performed at the end of the last working day of the month on a tape marked "Grandfather." Twelve grandfather tapes are required.

4. The father tapes are then reused for the next month in the same order, and the cycle continues. At the end of the year, the first grandfather tape is overwritten.

Note: A longer version-control window could be achieved by doubling the number of son tapes and reusing them on a bi-weekly schedule. Note that the father tapes could use synthetic backups.

On Site versus Off Site Storage

On site backup storage means that the production system and backup media are in the same location. This means that if a disaster strikes the facility, there is the risk of losing both the production and backup copies of the data.

A media rotation scheme such as GFS means that at least some of the backup media can be taken for storage off site once the backup job has run. For example, in the GFS scheme outlined above, four of the father tapes could be kept off site at any one time. Grandfather tapes can all routinely be kept off site with only one needing to be brought on site at the time of the backup job.

Transporting media off site is an onerous task, however. High-bandwidth Internet and high-capacity cloud storage providers have made off-site backup solutions more affordable and easier to implement.

Note: While cloud backup is convenient, there are still substantial risks from the failure of the cloud provider. It is prudent to perform local backups in addition to cloud backups.

3-2-1 Backup Rule

The 3-2-1 backup rule is a best-practice maxim that you can apply to your backup procedures to verify that you are implementing a solution that can mitigate the widest possible range of disaster scenarios. It states that you should have three copies of your data (including the production copy), across two media types, with one copy held offline and off site.

21.1.5 Backup Testing and Recovery Best Practices

When you design a backup scheme, test it to make sure it's reliable. To test the backup:

- **Try restoring some of the backed-up data into a test directory, making sure you don't overwrite any data when doing so. Alternatively, use a virtual machine to test recovery procedures without affecting the production host.**
- **Configure the backup software to verify after it is written. Most backup software can use hashing to verify that each job is a valid copy of the source data. It is also important to verify media integrity regularly, such as by running `chkdsk` on hard drives used for backup.**
- **Verify that the backup contains all the required files.**

You should re-test recovery procedures whenever there is a change to the backup schedule or requirements. It is also best practice to perform routine tests periodically - every week or every month, depending on criticality. Frequent testing mitigates risks from media failure and configuration oversights.

Recovery Options

When performing a recovery, you can choose to either perform an in-place (overwrite) recovery or recover to an alternate location.

An in-place recovery restores the data to the original system and location which overwrites the current system. This method is commonly used when recovering from minor issues such as a corrupted file. This method will most likely require downtime while the restoration process takes place.

Restoring to an alternate location restores the data to a different computer or even to an off-site cloud environment. If the data loss was due to a catastrophic hardware failure or major cyberattack leaving the original hardware inaccessible, this method is preferred. This method does require more planning but can lead to reduced disruption of business operations if the backup system is ready to go and the data can be quickly restored.

21.2 Data Handling Best Practices

Core 2 Exam Objectives Covered

- **2.1 Summarize various security measures and their purposes.**
- **2.9 Compare and contrast data destruction and disposal methods.**
- **4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.**

After designing and implementing an appropriate data backup and recovery plan, you have been tasked with developing appropriate policies for handling sensitive data across the organization.

In this lesson, you will learn the different classifications of data, prohibited content and licensing concerns, how to preserve data during an incident, and how to properly destroy data and dispose of hardware.

Learning Objectives

As you study this lesson, answer the following questions:

- **What regulations does healthcare data fall under?**
- **What type of data is considered prohibited?**
- **What are the different software license types?**
- **What is the chain of custody?**
- **How can a mechanical hard drive be destroyed?**

21.2.1 Regulated Data Classification

Regulated data is information that must be collected, processed, and stored in compliance with federal and/or state legislation. If a company processes regulated data collected from customers who reside in different countries, it must comply with the relevant legislation for each country.

A breach is where confidential or regulated data is read, copied, modified, or deleted without authorization. Data breaches can be accidental or intentional and malicious. Any type of breach of regulated data must normally be reported to the regulator and to individual persons impacted by the breach.

Personally Identifiable Information

Personally identifiable information (PII) is data that can be used to identify, contact, or locate an individual or, in the case of identity theft, to impersonate them. A cell phone number is a good example of PII. Others include name, date of birth, email address, street address, biometric data, and so on. PII may also be defined as responses to challenge questions, such as "What is your favorite color/pet/movie?" PII is often used for password reset mechanisms and to confirm identity over the telephone. Consequently, disclosing PII inadvertently can lead to identity theft.

Some types of information may be PII depending on the context. For example, when someone browses the web using a static IP address, the IP address is PII. An address that is dynamically assigned by the ISP may not be considered PII. These are the sorts of complexities that must be considered when determining compliance with privacy legislation.

Personal Government-issued Information

Personal government-issued information that is issued to individuals by federal or state governments is also PII. Examples include a social security number (SSN), passport, driving license, and birth/marriage certificates. Data collected and held by the US federal government is subject to specific privacy legislation, such as the US Privacy Act.

Healthcare Data

Protected-health-information refers to medical and insurance records plus associated hospital and laboratory test results. Healthcare data may be associated with a specific person or used as an anonymized or de-identified data set for analysis and research, such as in clinical trials to develop new medicines.

- An anonymized data set is one where the identifying data is removed completely.
- A de-identified data set contains codes that allow the subject information to be reconstructed by the data provider.

Healthcare data is highly sensitive. Consequently, the reputation damage caused by a healthcare data breach is huge.

Credit Card Transactions

There are also industry-enforced regulations mandating data security. A good example is the Payment Card Industry Data Security Standard (PCI DSS) which governs the processing of credit card transactions and other bank card payments. It sets out protections that must be provided if cardholder data - names, addresses, account numbers, and card numbers and expiry dates - is stored. It also sets out sensitive authentication data, such as the CV2 confirmation number or the PIN used for the card.

Regulations such as PCI DSS have specific cybersecurity control requirements; others simply mandate "best practice," as represented by a particular industry or international framework. Frameworks for security controls are established by organizations such as the National Institute of Standards and Technology (NIST).

Data Handling Best Practices

Employees should be trained to identify PII and to handle personal or sensitive data appropriately. This means not making unauthorized copies or allowing the data to be seen or captured by any unauthorized persons. Examples of treating sensitive data carelessly include leaving order forms with customers' credit card details on view on a desk, putting a credit card number in an unencrypted notes field in a customer database, or forwarding an email with personal details somewhere in the thread or a Cc (copy all) field.

To help ensure that employees remember and understand the importance of proper data handling, splash screens can be implemented. Splash screens are those screens that you see when starting a program or logging into the system. These screens can display legal disclaimers, policies, and other important notices. Users should be reminded to look at these splash screens to remind themselves of the policies that they must adhere to.

The policies and tools used to handle data and prevent it from leaving the organization's control are known as Data Loss Prevention (DLP). Software tools can be used to help identify where sensitive data is stored and then classify it based on sensitivity. Once this is done, DLP software will monitor the data and can take action to block the data from being removed or accessed.

Data Retention Requirements

Another issue for regulated data is its retention on both file and database servers and in backup files:

- Regulation might set a maximum period for the retention of data. For example, if a company collects a customer’s address and credit card information to fulfill an order and the customer then makes no further orders, the company might be expected to securely destroy the information it has collected.

- **Regulation might also demand that information be retained for a minimum period. In the credit card example, the company should log when and how the protected information was destroyed and preserve that log for inspection for a given period.**

21.2.2 Prohibited Content and Licensing Issues

As well as ensuring secure handling of confidential and sensitive data, you need to consider methods for identifying and removing prohibited content and unlicensed software from company workstations.

Prohibited Content

Employee workstations should only be used for work-related activities and data storage. In this context, prohibited content is any information that is not applicable to work. It can also specifically mean content that is obscene or illegally copied/pirated. The acceptable use policies built into most employee contracts will prohibit the abuse of Internet services to download games, obscene material, or pirated movies or audio tracks. Employees should also avoid using work accounts for personal communications.

End-User License Agreements

Prohibited content also extends to the unauthorized installation and use of software. When you install software, you must accept the license governing its use, often called the end-user license agreement. The terms of the license will vary according to the type of software, but the basic restriction is usually that the software may only be installed on one computer or for use by one single person at any one time.

An EULA might distinguish between personal and corporate/business/for-profit use. For example, a program might be made available as freeware for personal use only. If an employee were to install that product on a company-owned device, the company would be infringing the license.

License Compliance Monitoring

Software is often activated using a product key, which will be a long string of characters and numbers. The product key generates a different product ID, which is often used to obtain technical support. The product ID can typically be accessed using the About option on the Help menu.

A personal license allows the product to be used by a single person at a time, though it might permit installation on multiple personal devices. A company may have hundreds of employees who need the same software on their computers. Software manufacturers do not expect such companies to buy individual copies of the software for each employee. Instead, they will issue a corporate-use license for multiple users, which means that the company can install the software on an agreed-upon number of computers for its employees to use simultaneously.

It is illegal to use or distribute unlicensed or pirated copies of software. Pirated software often contains errors and viruses as well. Enterprises need monitoring systems to ensure that their computers are not hosting unlicensed or pirated software. There are two particular situations to monitor for:

- **Valid licenses - A personal license must not be misused for corporate licensing. Also, matching the number of corporate-use licenses purchased with the number of devices or users able to access the software at a given time can be complex. Various inventory and desktop management suites can assist with ensuring that each host or user account has a valid license for the software it is using and that device/user limits are not being exceeded.**
- **Expired licenses - The software product must be uninstalled if the license is allowed to expire or the number of devices/user accounts is reduced. It is also important to track renewal dates and ensure that licenses do not expire due to a lack of oversight. Some software comes with a perpetual license which means it never expires and requires no recurring subscription or renewal fees.**

Open-source Licenses

Software released under an open-source license generally makes it free to use, modify, and share and makes the program code used to design it available. The idea is that other programmers can investigate the program and make it more stable and useful. An open-source license does not forbid commercial use of applications derived from the original, but it is likely to impose the same conditions on further redistributions. When using open-source software, it is important to verify the specific terms of the license as they can vary quite widely.

Commercial open-source software may be governed by additional subscription or enterprise agreements to supplement the open-source software license.

Digital Rights Management

Digital music and video are often subject to copy protection and digital rights management. When you purchase music or video online, the vendor may license the file for use on a restricted number of devices. You generally need to use your account with the vendor to authorize and deauthorize devices when they change. Most DRM systems have been defeated by determined attackers, and consequently, there is plenty of content circulating with DRM security removed. From an enterprise's point of view, this is prohibited content, and it needs monitoring systems to ensure that its computers are not hosting pirated content files. Additional shortcomings from use of DRM include a lack of portability, lack of backup support, weak encryption, and increased risk of obsolescence. To address these shortcomings, numerous vendors have adopted DRM alternatives, such as encouraging customers not to share illegally shared digital files and making digital files so affordable that it is not worth the time and effort to create illegal copies.

Non-Disclosure Agreements

Non-disclosure agreements (NDA) are agreements designed to protect sensitive information. An NDA is a legally binding contract that obligates all parties to protect sensitive information that is shared between them. An NDA agreement can be either unilateral or mutual:

- **In a unilateral NDA, one party shares sensitive data with the other party, and only the receiving party is obligated to keep the information secret. An example would be a company having employees sign an NDA before being allowed to work on a project that contains sensitive information.**

- **With a mutual NDA, both parties agree to protect each other's secrets. This type of agreement is common when two organizations partner together for a project.**

21.2.3 Incident Response

While performing technical support, you may have to report or respond to security incidents. A security incident could be one of a wide range of different scenarios, such as:

- **A computer or network infected with viruses, worms, or Trojans.**
- **A data breach or data exfiltration where information is seen or copied to another system or network without authorization.**
- **An attempt to break into a computer system or network through phishing or an evil twin Wi-Fi access point.**
- **An attempt to damage a network through a denial of service (DoS) attack.**
- **Users with unlicensed software installed on their PC.**
- **Finding prohibited material on a PC, such as illegal copies of copyrighted material, obscene content, or confidential documents that the user should not have access to.**

An incident response plan sets out procedures and guidelines for dealing with security incidents. Larger organizations will provide a dedicated computer incident response team (CIRT) as a single point-of-contact so that a security incident can be reported through the proper channels. The members of this team should be able to provide the range of decision-making and technical skills required to deal with different types of incidents. The team needs managers and technicians who can deal with minor incidents on their own initiative. It also needs senior decision-makers (up to director level) who can authorize actions following the most serious incidents.

The actions of staff immediately following the detection of an incident can have a critical impact on the subsequent investigation. When an incident is detected, it is critical that the appropriate person on the CIRT be notified so that they can act as the first responder, take charge of the situation, and formulate the appropriate response.

If there is no formal CIRT, it might be appropriate to inform law enforcement directly. Involving law enforcement will place many aspects of investigating the incident out of the organization's control. This sort of decision will usually be taken by the business owner.

Note:

One exception may be when you act as a whistleblower because you have proof that senior staff in the organization pose an insider threat or are disregarding regulations or legislation.

21.2.4 Data Integrity and Preservation

Forensics is the science of collecting evidence from computer systems to a standard that will be accepted in a court of law. Like DNA or fingerprints, digital evidence is mostly latent. Latent means that the evidence cannot be seen with the naked eye; rather, it must be interpreted using a machine or process.

It is unlikely that a computer forensic professional will be retained by an organization, so such investigations are normally handled by law enforcement agencies. However, if a forensic investigation is launched (or if one is a possibility), it is important that technicians and managers are aware of the processes that the investigation will use. It is vital that they are able to assist the investigator and that they do not do anything to compromise the investigation. In a trial, the defense will try to exploit any uncertainty or mistake regarding the integrity of evidence or the process of collecting it.

Documentation of Incident and Recovery of Evidence

The general procedure for ensuring data integrity and preservation from the scene of a security incident is as follows:

1. Identify the scope of the incident and the host systems and/or removable drives that are likely to contain evidence. If appropriate, these systems should be isolated from the network.

2. Document the scene of the incident using photographs and ideally video and audio. Investigators must record every action they take in identifying, collecting, and handling evidence.

3. If possible, gather any available evidence from a system that is still powered on, using live forensic tools to capture the contents of cache, system memory, and the file system. If live forensic tools are not available, it might be appropriate to video record evidence from the screen.

4. If appropriate, disable encryption or a screen lock and then power off each device.

5. Use a forensic tool to make image copies of fixed disk(s) and any removable disks. A forensic imaging tool uses a write blocker to ensure that no changes occur to the source disk during the imaging process.

6. Make a cryptographic hash of each source disk and its forensic image. This can be used to prove that the digital evidence collected has not been modified subsequent to its collection.

7. Collect physical devices using tamper-evident bags and a chain-of-custody form, and transport them to secure storage.

Order of Volatility

When recovering evidence, it is important to follow the order of volatility. This is the order that data should be collected based on how long it is likely to remain available. The most volatile data should be collected first and then go down the list to the data that is least likely to disappear.

A general order of volatility from most to least volatile is:

1. **CPU cache and registers - This data is extremely volatile and changes rapidly.**
2. **Memory (RAM) - RAM is volatile memory, and its contents are lost when the power is turned off.**
3. **Temporary file system/swap space - This space is used for temporary storage and can contain valuable evidence.**
4. **Disk storage - This can include hard drives, SSDs, and other persistent storage devices. While persistent, this data can be overwritten or deleted.**
5. **Archival media - This includes any backup media such as USB drives, tape drives, etc. This data is the least volatile.**

Chain of Custody

It is vital that the evidence collected at the crime scene conforms to a valid timeline. Digital information is susceptible to tampering, so access to the evidence must be tightly controlled. Once evidence has been bagged, it must not subsequently be handled or inspected, except in controlled circumstances.

A chain of custody form tracks where, when, and who collected the evidence, who has handled it subsequently, and where it was stored. The chain of custody must show access to, plus storage and transportation of, the evidence at every point from the crime scene to the courtroom. Everyone who handles the evidence must sign the chain of custody and indicate what they were doing with it.

21.2.5 Data Destruction Methods

Data destruction and disposal refer to either destroying or decommissioning data storage media, including hard disks, flash drives, tape media, and CDs/DVDs. The problem has become particularly prominent as organizations repurpose and recycle their old computers, either by donating them to charities or by sending them to a recycling company, where parts may later be recovered and sold.

If the media device is going to be repurposed or recycled, a best practice procedure to sanitize data remnants on the media must be applied before the disk can be released. It is important to understand that media must also be sanitized if the device is repurposed within the organization. For example, a server used to host a database of regulated data that no longer meets the performance requirement might be repurposed as a file server. It is imperative that the database information be sanitized prior to this change in role.

When selecting an appropriate sanitization method, you need to understand the degree to which data on different media types may be recoverable and the likelihood that a threat actor might attempt such recovery. Data from a file "deleted" from a disk is not erased. Rather, the HDD sector or SSD block is marked as available for writing. The information contained at that storage location will only be removed when new file data is written. Similarly, using the OS standard formatting tool to delete partitions and write a new file system will only remove references to files and mark all sectors as usable. In the right circumstances and with the proper tools, any deleted information from a hard drive could be recovered. Recovery from SSDs requires specialist tools but is still a risk.

Erasing / Wiping

Disk erasing/wiping software ensures that old data is destroyed by writing to each location on a hard disk drive, either using zeroes or in a random pattern. This leaves the disk in a "clean" state ready to be passed to the new owner. This overwriting method is suitable for all but the most confidential data, but it is time-consuming and requires special software. Also, it does not work reliably with SSDs.

Low Level Format

Most disk vendors supply low-level formatting tools to reset a disk to its factory condition. Most of these tools will now incorporate some type of sanitize function. You must verify the specific capability of each disk model, but the following functions are typical:

- Secure erase performs zero-filling on HDDs and marks all blocks as empty on SSDs. The SSD firmware's automatic garbage collectors then perform the actual erase of each block over time. If this process is not completed (and there is no progress indicator), there is a risk of remnant recovery, though this requires removing the chips from the device to analyze them in specialist hardware.
- Instant secure erase Crypto Erase uses the capabilities of self-encrypting drives (SEDs) as a reliable sanitization method for both HDDs and SSDs. An SED encrypts all its contents by using a media encryption key (MEK). Crypto Erase destroys this key, rendering the encrypted data unrecoverable.

Note: If the device firmware does not support encryption, using a software disk-encryption product and then destroying the key and using SE should be sufficient for most confidentiality requirements.

21.2.6 Disposal and Recycling Outsourcing Concepts

If a media device is not being repurposed or recycled, physical destruction might be an appropriate disposal method. A disk can be mechanically destroyed in specialist machinery:

- Drilling - A disk can be destroyed using a drill on specific sections of the platters including the landing zone (where read/write heads rest when not in use) and along the data tracks. Safety goggles should always be worn when using this method. While safe for most cases, this method is not appropriate for the most highly confidential data as there is at least some risk of leaving fragments that could be analyzed using specialist tools.
- Shredding - The disk is ground into little pieces. A mechanical shredder works in much the same way as a paper shredder.
- Incinerating - The disk is exposed to high heat to melt its components. This should be performed in a furnace designed for media sanitization. Municipal incinerators may leave remnants.
- Degaussing - A hard disk is exposed to a powerful electromagnet that disrupts the magnetic pattern that stores the data on the disk surface. Note that degaussing does not work with SSDs or optical media.

There are many third-party vendors specializing in outsourced secure disposal. They should provide a certificate of destruction/recycling showing the make, model, and serial number of each drive they have handled plus date of destruction and how it was destroyed. A third-party company might also use overwriting or crypto-erase and issue a certificate of recycling rather than destruction.

These certificates are important to retain, especially when dealing with data that falls under certain regulatory requirements, such as HIPAA. These regulations will have strict requirements on how data should be destroyed. You should also make sure that all environmental regulations are followed as hard drives can contain hazardous materials and should be disposed of properly. Hard drives also contribute to the growing problem of e-waste and should be disposed of properly.

21.3 Artificial Intelligence

Core 2 Exam Objectives Covered

- **4.10 Explain basic concepts related to artificial intelligence (AI).**

Artificial intelligence (AI) involves using computers to do things that traditionally require human intelligence. As your company grows and implements newer technologies, you have been tasked with researching if artificial intelligence should be integrated into the organization's workflow and how to best implement AI.

In this lesson you will learn how AI can be integrated into applications, what policies and limitations should be implemented, and the difference in public and private AI systems.

Learning Objectives

As you study this lesson, answer the following questions:

- **What benefits can integrating AI into an application provide?**
- **What should an AUP for AI include?**
- **Why would an AI's output be biased?**
- **Why is data security and privacy a primary concern when it comes to AI?**

21.3.1 Application Integration

Artificial Intelligence can be integrated into software applications to enhance their functionality and leverage the capabilities of AI across multiple areas of the organization.

AI can be integrated into existing software applications increasing the capabilities of these systems. For example, AI can enhance a Supply Chain Management (SCM) system by forecasting demand, optimizing logistics, and identifying potential disruptions. AI integration will also help facilitate the exchange of data between multiple systems to ensure that AI models have access to the necessary data to generate accurate insights and predictions.

How AI is integrated will vary based on the application developer. Some app developers will include AI as an installation option. Users might add AI functionality through a 3rd party vendor, such as adding AI through a web browser extension. Another option is for the AI developer themselves to develop their own APIs or plugins that integrate with multiple apps. Every app and AI is going to be different and you will need to research how best to integrate AI if it is possible.

Applications can also gain new features by integrating AI, such as being able to understand and respond to human language (Natural Language Processing), make predictions or decisions based on data (Machine Learning), and even recognize images (Computer Vision).

21.3.2 Policy

When implementing AI into an organization's workflow, appropriate policies that dictate how AI can be used in the workplace need to be put in place.

A common policy that is used for software and network resources is an Acceptable Use Policy (AUP). An AUP for AI will outline guidelines and restrictions on how AI tools and systems can be used within the organization. Having the AUP in place will set clear expectations for users on what they can and cannot do. The AUP will also protect the company by ensuring they are in compliance with laws and regulations.

Policies need to also be put into place defining what is considered plagiarism when it comes to AI. This policy needs to define how AI can be used to assist in writing. The policy should also address attribution when AI is used and needs to clearly state that submitting AI-generated work is not acceptable.

21.3.3 Limitations

While AI is often a great tool and will continue to grow in its capabilities, there are limitations that you should be aware of:

- **Bias - AI is trained to perform its tasks using data sets. If this data is flawed and biased, then the AI will be flawed and contain these same biases. The way the algorithm is designed may also contain some biases that will prioritize certain features or patterns over others. Even with perfect data and algorithms, developers may inadvertently introduce their own biases into the AI during the design and training phases.**

- **Hallucinations - AI hallucinations occur when the AI generates wrong information that is not based on facts or the data it was trained on. This can include completely made up information, distorted information, or flawed deductions. This can obviously lead to some negative consequences if this flawed output is used. This is why it is important to fact check any AI output.**

- **Accuracy - AI can only be as accurate as the data used to train it. If the data is messy, flawed, biased, or there is just not enough data to properly train the AI, the AI will make mistakes in its output.**

AI can be a powerful tool, but it is important to verify the information and not solely rely on AI to perform important tasks.

21.3.4 Private vs. Public

AI programs can typically be categorized as either public or private. This refers to how the AI is deployed and who has access to it:

- **Private AI models are developed for a specific organization and use cases. These AI models will generally only be accessible to users within the organization who need to use them. These AI models can be trained using both public data and the organization's private data. Because sensitive data may be used to train these AI models, it is important to make sure that access is kept secure to prevent sensitive data from being leaked.**

- **A Public AI model is typically built by larger organizations and is accessible to anyone through APIs or web interfaces. These AI models are trained on publicly available data (such as the Internet) and also user interactions. Examples of public AI models include ChatGPT and Google Gemini.**

AI models will typically run through a cloud platform and clients connect using HTTPS so the network communication should be secure.

Regardless of which model is being used, protecting the privacy of users should be a primary concern. When users interact with AI, they will often input personal or confidential information and this data can be stored and used to train the AI model. This could lead to an accidental leak of private information.

Malicious users may also carry out a prompt injection attack which involves crafting a prompt to trick the AI into revealing sensitive data. When using a private AI model, employees or third-party vendors may have access to sensitive information and appropriate security protocols should be put into place to reduce the chance of these individuals gaining access to sensitive data.

22.0 Implementing Operational Procedures

Documented procedures for employees and clients to follow ensure that a high level of service is maintained and that processes are completed with consistent outcomes. Having the documentation to support your operations, along with understanding the processes to follow should an incident or disaster occur, can ensure your organization can maintain progress as business needs change. Documentation of your organization's infrastructure ensures that you and your team of IT professionals have an awareness of the assets you are all responsible for. When changes are made to those assets, be it an update for the operating systems or a complete reconfiguration of an equipment rack, all changes should be documented so all team members are aware of the change.

Prepare for A+ Core 2 by:

- **Implementing best practice documentation to track assets.**
- **Using common safety and environmental procedures.**
- **Explaining basic scripting constructs and use cases.**

22.1 Change and Inventory Management

Core 2 Exam Objectives Covered

- **4.1 Given a scenario, implement best practices associated with documentation and support systems information management.**
- **4.2 Given a scenario, apply change management procedures.**

The organization has just announced they are expanding their operations from Chicago to Los Angeles. This new location will have several new employees and they will need to be supported with new IT equipment that suits their needs. Procuring new equipment and adding it to a network may seem easy, but it requires many different steps to incorporate these changes into the existing environment. Ensuring that your inventory of assets is updated with the new equipment but also ensuring the network documentation also incorporates this expansion will be key to ensuring an accurate accounting of the full environment and accountability for the changes being made.

Learning Outcomes

As you study this lesson, answer the following questions:

- **What is a change request?**
- **What purpose does a change advisory board serve?**
- **What is an asset?**
- **What information should be included in an inventory of assets?**
- **Why must a technician understand the warranty process for a particular system?**

22.1.1 Change Requests

Change management (CM) refers to policies and procedures that reduce the risk of configuration changes causing service downtime. Change management is closely related to configuration management.

A change request is generated when a fault needs to be fixed, new business needs or processes are identified, or there is room for improvement in an existing SOP or system. The need to change is often described either as reactive, where the change is forced on the organization, or as proactive, where the need for change is anticipated and initiated internally.

In a formal change-management process, the need or reasons for change and the procedure for implementing the change are captured in a request-for-change (RFC) form and submitted for approval. Change-request documentation should include:

- **Purpose of the change— This is the business case for making the change and the benefits that will accrue. It might include an analysis of risks associated with performing the change and risks that might be incurred through not performing the requested change.**
- **Scope of the change— This is the number of devices, users, or customers that will be affected by the change. Scope can also include costs and timescales. For a complex project, it might include sub-tasks and stakeholders. Scope should also include the factors by which the success or failure of the change can be judged.**
- **Type of change— Does the change need to be implemented quickly or is this a routine or standard change request? Or is this an emergency change that needs to be implemented now to correct a major outage? Documenting the priority and type of change can help expedite the approval process when necessary. Some organizations may wish to categorize the change as follows:**
    - **Standard- Low impact and repeatable; may require the change management process to be set up but can be repeated as necessary without triggering the full CM process.**
    - **Normal- One-time change that triggers the full CM process and requires change board approval.**
    - **Emergency- high impact, but urgent change request requiring an expedited CM process and approval.**
- **Implementation schedule— When will this change be incorporated? Is there a specific date and time? Will it be conducted during a normal maintenance window? Is there currently a change freeze, where the company or organization has placed a temporary stop on making changes?**
- **Effects of the change— What systems are directly or indirectly affected? Are there any risks involved in the implementation of the change?**

Other considerations when making a change suggestion may require adequate testing of the change in a sandbox or non-production testing environment. You should also document the responsible employee who will implement the change and others who may be responsible for the affected system or service.

22.1.2 Risk Analysis

Each change being requested should undergo a risk analysis. Risk analysis is a systematic approach to identify possible risks associated with implementing the change. Could the change cause a temporary outage of a critical system or service? Is there a risk of injury or death to the employee? While some changes will have minimal risks, others may include high-level, severe risks.

For each risk identified, what controls or checks can be used to mitigate the risk to an acceptable level? Are there safety procedures that can be followed, such as securing power to the equipment or having a safety observer present during the implementation process, that may help reduce the risk or even eliminate it altogether? Understanding the cause and effect of changes can be just as important as the change itself.

22.1.3 Change Board Approvals

When a change request has been drafted and submitted, it must go through an approval process.

If the change is normal or minor, approval might be granted by a supervisor or department manager. Major changes are more likely to be managed as a dedicated project and require approval through a Change Advisory Board (CAB). The role of the CAB is to assess both the business case and the technical merits and risks of the change plan. The CAB should include stakeholders for departments, users, or customers who will be impacted by the change as well as those proposing it, technicians who will be responsible for implementing it, and managers/directors who can authorize the budget.

22.1.4 Implementation and Acceptance

Implementation is when we have the approval to make a change and we have the authority to make the change. This process may require multiple steps to be followed to accomplish the change task.

Once the change is completed, it may be necessary to have a colleague conduct a peer review that the change was implemented correctly in accordance with the approval. Sometimes technicians may skip a step or misspell something while making a change. The peer review process allows mistakes to be caught before bringing the system or service back online.

If the change process runs into any issue, it may require a rollback plan to reverse the change and restore the system to the original configuration. Part of the rollback plan should include a backup plan. The backup plan is a system and data backup that can be used to restore the system should an error in the change process occur. Switching to a complete replacement system may also be required. This can also include shifting services to alternative sites.

It may also be necessary to receive end-user acceptance that the change has been implemented and the system is fully functional. End-user acceptance ensures that the customer or client is satisfied with the change that was made and that there are no further issues caused by the change. Some organizations may require a signature from the customer or client after they have accepted the change and its successful implementation.

22.1.5 Asset Management

While troubleshooting or implementing changes to a system or service, it will be important to ensure you are working on the correct system or service. Accurate tracking of what physical assets your company or organization has is just as important as fixing the issues with those systems. An asset is any physical system or peripheral equipment that has value and needs to be tracked by the organization.

Accurate inventory lists should consist of at least the following details:

- **System Name, Make/Model - Assists in the identification of the asset among other assets.**
- **Asset ID - Unique value assigned to the system by the organization or manufacturer; sometimes referred to as a service tag number and is usually printed on a sticker or that is attached to the system as an asset tag.**
- **Manufacturer - Company that manufactured or provided the system**
- **Systems specifications - Processor, RAM, and other hardware details; this is helpful to know should parts or replacement of the asset be necessary in the future.**
- **Dates - Date of purchase and warranty information is helpful when seeking support from the manufacturer.**
- **Cost - The cost of the asset; this information is helpful for business insurance and to document the value of the asset should it need to be replaced.**



Figure 1. Dell Service Tag

The list of assets can be a manually developed spreadsheet, but many organizations now track assets using a configuration management database (CMDB). This database may include software and license information in addition to tracking of hardware devices the organization owns or leases. The database may also include information relating to the lifecycle of the hardware assets. The lifecycle refers to the full "life" of the asset: from purchase completion and delivery of the asset, sometimes referred to as the procurement process, to the

eventual disposal of the asset when it is no longer needed. Asset tracking may also be seen as a feature within a support ticketing system. This would allow tracking of issues for each asset the organization has.

The purchase information, including the date, can be used to verify warranty coverage on the asset. This will be key should an issue arise that requires escalation of support to the manufacturer. It may also be beneficial to list the assigned user or administrator for the system. This would facilitate faster communication to the responsible party should an issue occur with that system. For example, for an Active Directory Domain Controller, you may want to include the domain system administrator's contact name, email, and telephone number.

Software licensing information should be documented also. This ensures the organization is aware of any software applications that are in use and/or installed on their systems. Tracking the licensing ensures the organization is maintaining compliance with the license's requirements and limitations and not potentially violating that license.

22.1.6 Warranty and Licensing

Each asset record should include appropriate procurement documentation, such as the invoice and warranty/support contract (along with appropriate contact information). For software, it should record the licensing details with device/user allocations and limits.

22.2 Common Safety and Environmental Procedures

Core 2 Exam Objectives Covered

- **4.4 Given a scenario, use common safety procedures.**
- **4.5 Summarize environmental impacts and local environmental controls.**

Safety is paramount when dealing with IT systems due to their use of electricity and the fact they may contain materials that can harm the environment if not disposed of correctly and possibly can lead to death or illness underlines the importance of safe work and handling practices. Ensuring compliance with local and international laws or regulations should also be considered to ensure the organization is handling materials properly.

Learning Outcomes

As you study this lesson, answer the following questions:

- **Why is electrical safety important?**
- **What purpose do fuses and grounding straps serve?**
- **What precautions should be taken with hazardous materials?**
- **What causes ESD and how can it be minimized?**

22.2.1 Compliance with Regulations

When performing PC maintenance work, you may need to take into account compliance with government regulations. Regulations that typically affect PC maintenance or the installation of new equipment are:

- **Health and safety laws— Keeping the workplace free from hazards.**
- **Building codes— Ensuring that fire prevention and electrical systems are intact and safe.**
- **Environmental regulations— Disposing of waste correctly.**

For example, in the United States, the most common safety regulations are those issued by the federal government, such as the Occupational Safety and Health Administration (OSHA), and state standards regarding employee safety.

While specific regulations may vary from country to country and state to state, in general, employers are responsible for providing a safe and healthy working environment for their employees. Employees have a responsibility to use equipment in the workplace in accordance with the guidelines given to them and to report any hazards. Employees should also not interfere with any safety systems, including signs or warnings or devices such as firefighting equipment. Employees should not introduce or install devices, equipment, or materials to the workplace without authorization or without assessing the installation.

22.2.2 Electrical Safety

Electricity flows in a circuit. A circuit is made when conductors form a continuous path between the positive and negative terminals of a power source. An electrical circuit has the following properties:

- **Current is the amount of charge flowing through a conductor, measured in amps (A or I).**
- **Voltage is the potential difference between two points (often likened to pressure in a water pipe) measured in volts (V).**
- **Resistance is the degree of opposition to the current caused by characteristics of the conductor, measured in ohms (Ω or R).**

Electrical equipment can give a shock if it is broken, faulty, or installed incorrectly. An electric shock can cause muscle spasms, severe burns, or even death.

Safety Equipment and Tools

While working with electronic equipment, it would be wise to utilize insulated tools and gloves to protect yourself from harm. You may also want to test the component with a voltage tester before attempting to work on it. Ensuring there is no voltage present can protect you from unexpected electrical shocks.

Figure 1. Electrical voltage tester reading zero volts



Image © macmackyky 123RF.com

Fuses

An electrical device must be fitted with a fuse appropriate to its maximum current, such as 3A, 5A, or 13A. A fuse blows if there is a problem with the electrical supply, breaking the circuit to the power source. If the fuse fitted is rated too low, it will blow too easily; if the rating is too high, it may not blow when it should and will allow too much current to pass through the device.

Note:

Take care with power strip sockets. The total amperage of devices connected to the power strip must not exceed the strip's maximum load (typically 13 amps).

Equipment Grounding

Electrical equipment must be grounded. If there is a fault that causes metal parts in the equipment to become live in the circuit, the ground provides a path of least resistance for the electrical current to flow away harmlessly. Devices such as PCs and printers are connected to the building ground via the power plug. However, the large metal equipment racks often used to house servers and network equipment must also be grounded. Do not disconnect the ground wire. If it must be removed, make sure it is replaced by a professional electrician.

Figure 2. Grounding terminals and wires

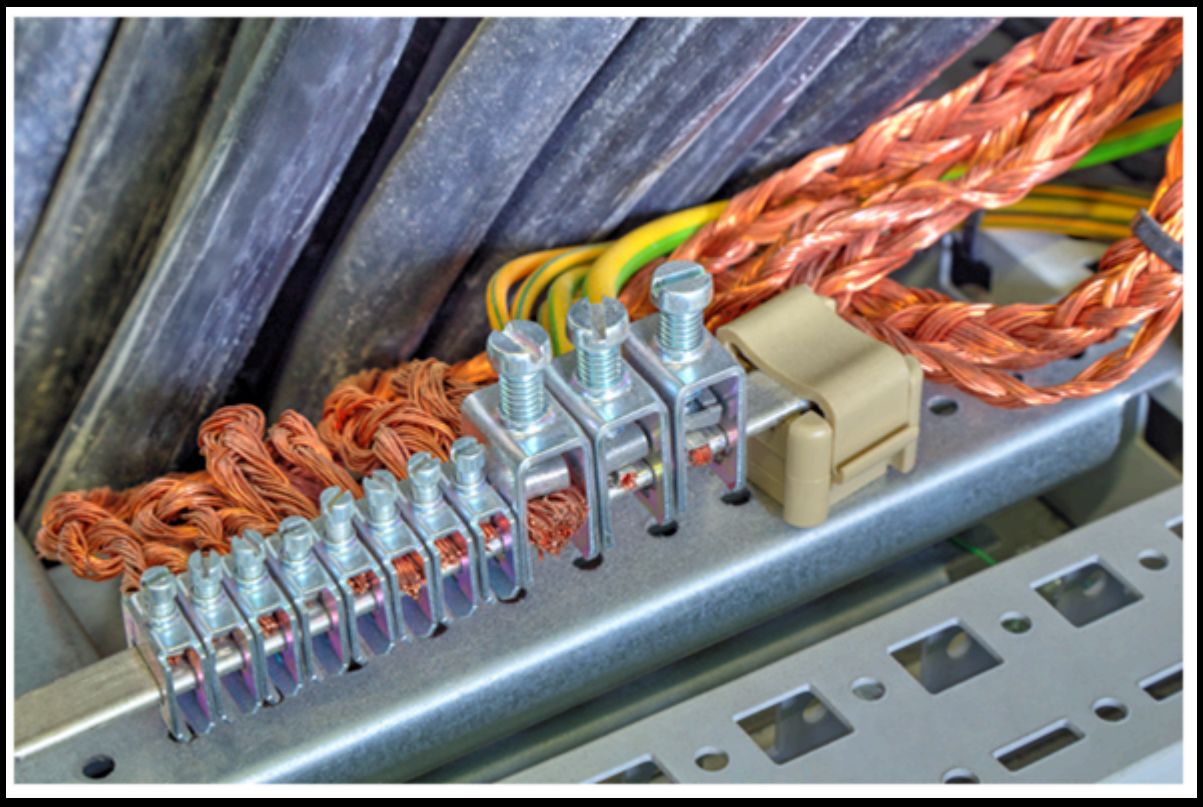


Image by phadventure © 123RF.com

Note:

Electrical currents can pass through metal and most liquids, so neither should be allowed to come into contact with any electrical device installations. Damaged components or cables are also a risk and should be replaced or isolated immediately. It is important to test electrical devices regularly. The frequency will depend on the environment in which the device is used. In some countries, portable appliance testing (PAT) carried out by a qualified electrician or technician ensures that a device is safe to use.

Proper Power Handling and Personal Safety

Whenever you add or replace components within a PC or laptop, the power must be disconnected first. Remove the AC plug and also remove the battery if present. Hold down the power button on the device to ensure the circuits are drained of any residual power from the circuit and capacitors.

PC power supply units can carry dangerously high levels of voltage. Charges held in capacitors can persist for hours after the power supply is turned off. You should not open these units unless you have been specifically trained to do so. Adhere to all printed warnings, and never remove or break open any safety devices that carry such a warning.

Note:

Never insert anything into the power supply fan to get it to rotate. This approach does not work, and it is dangerous.

Electrical Fire Safety

Faulty electrical equipment can pose a fire risk. If the equipment allows more current to flow through a cable than the cable is rated for, the cable will heat up. This could ignite flammable material close to the cable. If an electrical wire does start a fire, it is important to use the correct type of extinguisher to put it out. Many extinguishers use water or foam, which can be dangerous if used near live electrical equipment. The best type to use is a carbon dioxide (CO_2) gas extinguisher. CO_2 extinguishers typically have a black label but sometimes have a red or white label. Dry powder extinguishers can also be used, though these can damage electronic equipment.

You should also ensure that the electricity supply is turned off. This should happen automatically (the fuses for the circuit should trip but may have failed), but make sure you know the location of the power master switches for a building.

Equipment Placement

Equipment placement or location is just as important as the equipment itself. Ensuring equipment is located in a secure location near a power source and out of public access ensures that only authorized personnel can access it. Servers and other networking equipment should be mounted in a secure networking closet or server room.

Understanding the basic principle that heat rises, the equipment location should have ample ventilation to collect the warm air and remove it from the environment, while also supplying the space with cool air to reduce equipment operating temperatures.

Other considerations when selecting an equipment location include ensuring systems that need to be connected are near each other or there is a proper cable connection available to connect the devices.

22.2.3 Other Safety Hazard Mitigations

In addition to electrical hazards, there are other safety hazards that computer technicians must account for.

Trip Hazards

A trip hazard is caused by putting any object in pathways where people walk.

- **When installing equipment, ensure that cabling is secured, using cable ties or cable management products, if necessary. Trays and Velcro straps can be used to bundle cables together to present a neat and tidy look. Check that cables running under a desk cannot be kicked out by a user's feet. Do not run cabling across walkways, but if there is no option but to do so, use a cord protector to cover the cabling.**

- **When servicing equipment, do not leave devices (PC cases, for instance) in walkways or near the edge of a desk (where they could be knocked off). Be careful about putting down heavy or bulky equipment (ensure that it cannot topple).**

Lifting Techniques

Lifting a heavy object in the wrong way can damage your back or cause muscle strains and ligament damage. You may also drop the object and injure yourself or damage the object. When you need to lift or carry items, be aware of the maximum safe lifting weight as well as any restrictions and guidance set out in your job description or site safety handbook. To lift a heavy object safely:

1. **Plant your feet around the object with one foot slightly toward the direction in which you are going to move.**

2. **Bend your knees to reach the object while keeping your back as straight and comfortable as possible and your chin up.**

3. **Find a firm grip on the object, and then lift smoothly by straightening your legs—do not jerk the object up.**

4. **Carry the object while keeping your back straight.**

5. **To lower an object, reverse the lifting process; keep your chin up and bend at the knees. Take care not to trap your fingers or to lower the object onto your feet. If you cannot lift an object because it is too awkward or heavy, then get help from a coworker or use a cart to relocate the equipment. If you use a cart, make sure the equipment is tightly secured during transport. Do not stack loose items on a cart. If you need to carry an object for some distance, make sure that the route is unobstructed and that the**

pathway (including stairs or doorways) is wide and tall enough.

Safety Goggles and Masks

If necessary, you should obtain protective clothing for handling equipment and materials that can be hazardous:

- **Use gloves and safety goggles to minimize any risk of burns from corrosive materials such as broken batteries, cell phones, and tablets or irritation from particles such as toner or dust.**

- **When you are using a compressed air canister, working around toner spills, or working in a dusty environment, use an air-filter mask that fits over your mouth and nose. People who suffer from asthma or bronchitis should avoid changing toner cartridges where possible.**

22.2.4 Environmental Impacts

The location in which computer equipment is placed can affect its proper operation and lifespan. All electronic equipment should be kept away from extremes of temperature and damp or dusty conditions.

Dust Cleanup

Dust is drawn into the computer via ventilation holes. Over time, the dust can form a thick layer over components, heat sinks, fan blades, peripheral connection ports, and ventilation slots, preventing effective heat dissipation. It can clog up peripherals such as keyboards and mice. Dust and smears can make the display hard to read. To perform dust cleanup:

- **Use a compressed air blaster to dislodge dust from difficult-to-reach areas. Take care with use, however, as you risk contaminating the environment with dust. Ideally, perform this sort of maintenance within a controlled work area, and wear an appropriate air-filter mask and goggles. Air filter masks help a user to not ingest dust, dirt, or otherwise harmful particles into their lungs. Some filters will also prevent the inhalation of harmful vapors from cleaning agents or chemicals.**

Figure 1. Air filter mask



Note: Do not use compressed air blasters to clean up a toner spill or a laser printer within an office-type area. You will blow fine toner dust into the atmosphere and create a health hazard.

- **Use a PC vacuum cleaner or natural bristle brush to remove dust from inside the system unit, especially from the motherboard, adapter cards, and fan assemblies. Domestic vacuum appliances should not be used as they can produce high levels of static electricity. PC-safe vacuums can often be used to blow air as well as for suction, so they can replace the need for compressed air canisters.**

Note: A PC vacuum can be used to deal with toner spills only if the filter and bag are fine enough to contain toner particles. Such vacuums should be labeled as toner-safe. Ideally, move the printer to a maintenance

room with filters to contain airborne particles. Alternatively, a toner cloth is a special cloth for wiping up loose toner. Be careful if you are using it inside the printer so that the cloth does not get caught on any components and leave fibers behind.

Temperature, Humidity, and Ventilation Control

A computer that is too hot is likely to be unreliable. A computer must be ventilated so that its fans can draw relatively cool air across the motherboard and expel the warmed air from the rear vents. You must ensure that the room (ambient) temperature is not too high and that there is space for air to flow around the case, especially around the ventilation slots. Do not place the computer in direct sunlight or near a radiator.

High humidity— the amount of water vapor in the air— can cause condensation to form. On the other hand, low humidity allows static charges to build up more easily and increases the risk of electrostatic discharge (ESD). The ideal level is around 50%.

Condensation can form because of sudden warming. When installing new equipment that has just been delivered, it is important to leave it in its packaging for a few hours— depending on the outside temperature— to allow it to adjust to room temperature gradually.

22.2.5 Electrostatic Discharge Mitigation

Static electricity is a high voltage, low current charge stored in an insulated body. Electrostatic discharge occurs when a path allows electrons to rush from a statically charged body to a component that has no charge. This can occur through touch or even over a small gap if the charge is high enough. Static electricity discharged into the delicate structure of electronic devices will flash-over between the conductive tracks, damaging or even vaporizing them. A static discharge may make a chip completely unusable. If not, it is likely to fail at some later time. Damage occurring in this way can be hidden for many months and might only manifest itself in occasional failures.

The human body is mostly water and so does not generate or store static electricity very well. Unfortunately, our clothes are often made of synthetic materials, such as nylon and polyester, which act as good generators of static electricity and provide insulating layers that allow charges to accumulate, especially when walking over carpet. Humidity and climate also affect the likelihood of ESD. The risk increases during dry, cool conditions when humidity is low. In humid conditions, the residual charge can bleed into the environment before it can increase sufficiently to be harmful to electrical components.

Proper Component Handling

Proper component handling tools and techniques protect electronic components against ESD when you service a PC or mobile device:

- **If possible, work in an uncarpeted area. Ideally, use an ESD-safe floor or chair mat.**
- **Touch an unpainted part of a metal computer chassis or power supply case to drain residual charge from your body. This is only a temporary solution, and a static charge could build up again.**

Note:

For your safety, unplug the computer from building power before opening the chassis

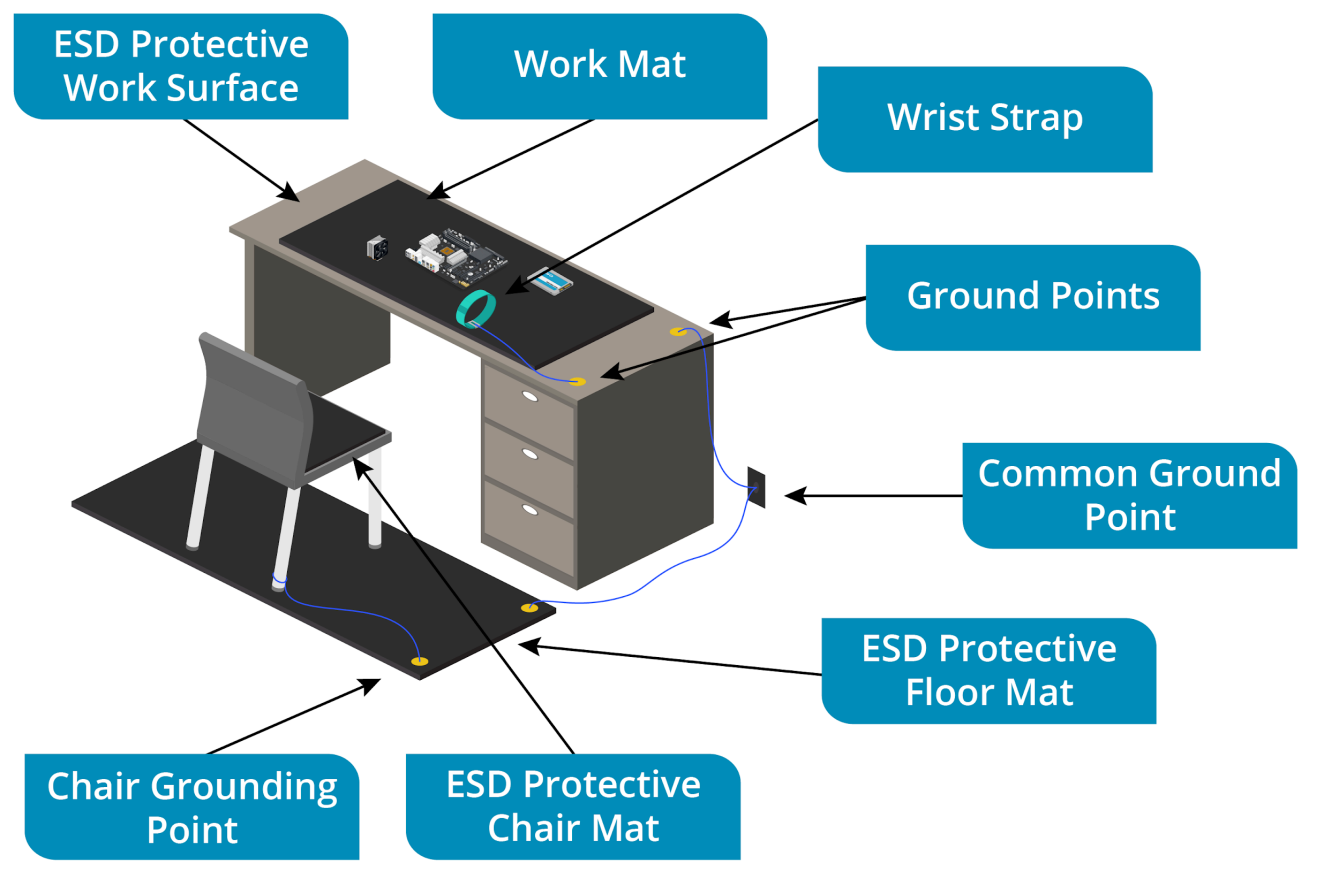
- **Wear an anti-ESD wrist strap or leg strap to dissipate static charges more effectively. The band should fit snugly around your wrist or ankle so that the metal stud makes contact with your skin. Do not wear it over clothing. The strap ground is made either using a grounding plug that plugs into a wall socket or a crocodile clip that attaches to a grounded point or an unpainted part of the computer's metal chassis. Figure 1. Electrostatic Discharge (ESD) wrist strap on ESD mat**



Note: Ensure that the strap has a working current-limiting resistor for safety (straps should be tested daily). Do not use a grounding plug if there is any suspicion of a fault in the socket or the building's electrical wiring or if the wiring is not regularly inspected and tested.

- **Use an anti-ESD service mat as a place to organize sensitive components. The mats contain a snap that you connect to the wrist or leg strap.**

- **Handle vulnerable components by holding the edges of the plastic mounting card. Avoid touching the surfaces of the chips themselves. Figure 2. An example of an electrostatic discharge (ESD) workstation**



Description
A desk with a work mat, wrist strap, and ground points is shown. The floor has an ESD protective floor mat and a chair grounding point, while the chair sits on an ESD protective chair mat. Labels identify key elements, including the common ground point, ensuring a controlled static-safe environment.

Proper Component Storage

Electronic components, assemblies, and spare parts are shipped and stored in antistatic packaging to protect them from ESD damage:

- **Antistatic bags— This packaging reduces the risk of ESD because it is coated with a conductive material. This material prevents static electricity from discharging through the inside of the bag. These bags are usually a shiny, gray metallic color. To protect the contents of the bag fully, you should seal it or at least fold the top over and seal that down.**
- **Dissipative packaging— This light pink or blue packaging reduces the buildup of static in the general vicinity of the contents by being slightly more conductive than normal. A plastic bag or foam packaging may be sprayed with an antistatic coating or have antistatic materials added to the plastic compound.**

This is used to package non-static-sensitive components packed in proximity to static-sensitive components.

22.2.6 Building Power Issues and Mitigations

Faults in building power supply cause power problems such as surges, under-voltage events, and power failures:

- Surges— A surge is a brief increase in voltage, while a spike is an intense surge. A surge or spike can be caused by machinery and other high-power devices being turned on or off and by lightning strikes. This type of event can take the supply voltage well over its normal value and cause sufficient interference to a computer to crash it, reboot it, or even damage it.
- Under-voltage event— Devices with large motors, such as lifts, washing machines, power tools, and transformers, require high-starting, or inrush, current. This might cause the building supply voltage to dip briefly, resulting in an under-voltage event. Overloaded or faulty building power distribution circuits sometimes cause an under-voltage event. An under-voltage event could cause computer equipment to power off. This is sometimes referred to as a brownout.
- Power failure— A power failure is a complete loss of power. This will cause a computer to power off suddenly. A power failure may be caused by a disruption to the power distribution grid— an equipment failure or the accidental cutting of a cable during construction work, for example— or may simply happen because a fuse has blown or a circuit breaker has tripped. This is formerly referred to as a blackout.

A range of power protection devices are available to mitigate the faults these power events can cause in computer equipment.

Surge Suppressors

Passive protection devices can be used to filter out the effects of surges and spikes. The simplest surge suppressor devices come in the form of adapters, trailing sockets, or filter plugs, with the protection circuitry built into the unit. These devices offer low-cost protection to one or two pieces of equipment. Surge protectors are rated according to various national and international standards, including Underwriters Laboratory (UL) 1449. There are three important characteristics:

- Clamping voltage— Defines the level at which the protection circuitry will activate, with lower voltages (400 V or 300 V) offering better protection.
- Joules rating— The amount of energy the surge protector can absorb, with 600 joules or more offering better protection. Each surge event will degrade the capability of the suppressor.
- Amperage— The maximum current that can be carried or the number of devices you can attach. As a rule of thumb, you should only use 80% of the rated capacity. For example, the devices connected to a 15 A protector should be drawing no more than 12 A. Of course, for domestic wiring, you should take care not to overload the building's power circuits in any case.

Battery Backups

Sudden power loss is likely to cause file corruption. If there is loss of power due to an under-voltage event or power failure, system operation can be sustained for a few minutes by using battery backup. Battery backup can be provisioned at the component level for disk drives, RAID arrays, and memory modules. The battery protects any read or write operations cached at the time of power loss.

At the system level, an uninterruptible power supply (UPS) will provide a temporary power source in the event of complete power loss. The time allowed by a UPS is sufficient to activate an alternative power source, such as a standby generator. If there is no alternative power source, a UPS will at least allow you to save files and shut down the server or appliance properly.

Figure 1. Example of a UPS



Image by magraphics© 123RF.com.

The key characteristics of a UPS are volt-amperes (VA) rating and runtime:

- **VA rating is the maximum load the UPS can sustain. To work out the minimum VA, sum the wattage of all the devices that will be attached to the UPS and multiply by 1.67 to account for a conversion factor. For example, if you have a 10 W home router and two 250 W computers, the VA is (10 + 250 + 250) * 1.67 = 852 VA. A 1K VA UPS model should therefore be sufficient.**

- **Runtime is the number of minutes that the batteries will supply power. The strength of the UPS batteries is measured in amp hours (Ah).**

Vendors provide calculators to help select an appropriate UPS size for the required load and runtime.

22.2.7 Materials Handling and Responsible Disposal

Some of the components and consumables used with computer and printer systems can be hazardous to health and to the environment. You must comply with all relevant regulations when handling and disposing of these substances.

Material Safety Data Sheets

Employers are obliged to assess the risk to their workforce from hazardous substances at work and to take steps to eliminate or control that risk. No work with hazardous substances should take place unless an assessment has been made. Employees are within their rights to refuse to work with hazardous substances that have not been assessed.

Suppliers of chemicals are required to identify the hazards associated with the substances they supply. Some hazard information will be provided on labels, but the supplier must also provide more detailed information on a material safety data sheet (MSDS). An MSDS will contain information about ingredients, health hazards, precautions, and first aid information and what to do if the material is spilled or leaks. The MSDS should also include information about how to recycle any waste product or dispose of it safely.

You may need to refer to an MSDS in the course of handling monitors, power supplies, batteries, laser-printer toner, and cleaning products. If handling devices that are broken or leaking, use appropriate protective gear, such as gloves, safety goggles, and an air-filter mask.

Proper Disposal

Even with procedures in place to properly maintain IT equipment, eventually, it will need to be decommissioned and either disposed of or recycled. IT equipment contains numerous components and materials that can cause environmental damage if they are disposed of as ordinary refuse. Waste disposal regulations to ensure protection of the environment are enforced by the federal and local governments in the United States and many other nations. Computer equipment is typically classed as waste electrical and electronic equipment (WEEE).

Special care must be taken with respect to the following device types:

- **Battery disposal— Swollen or leaking batteries from laptop computers or cell phones and tablets must be handled very carefully and stored within appropriate containers. Use gloves and safety goggles to minimize any risk of burns from corrosive material. Batteries must be disposed of through an approved waste management and recycling facility.**
- **Toner disposal— Photocopier and laser-printer toner is an extremely fine powder. The products in toner powder are not classified as hazardous to health, but any dust in substantial concentration is a nuisance as it may cause respiratory tract irritation. Most vendors have recycling schemes for used toner cartridges. Loose toner must be collected carefully by using an approved toner vacuum and sealed within a strong plastic waste container. Get the manufacturer's advice about disposing of loose toner safely. It must not be sent directly to a landfill.**
- **Other device and asset disposal— Many components in PCs, cell phones, tablets, and display screens contain toxins and heavy metals, such as lead, mercury, and arsenic. These toxins may be present in batteries, circuit boards, and plastics. These toxins are harmful to human health if ingested and are damaging to the environment. This means that you must not dispose of electronic devices as general waste in landfills or incinerators. If an electronic device cannot be donated for reuse, it must be disposed of through an approved waste management and recycling facility.**

22.3 Scripting Basics

Core 2 Exam Objectives Covered

- **4.8 Identify the basics of scripting**

Setting up, configuring, and making changes to a system can be a time-consuming and tedious process. Some processes and tasks will be repeated several times per day. For example, creation of new user accounts and termination of old accounts no longer needed is part of the routine operations of a network environment. You may find that using a script to perform this task can ensure no steps are missed and the process is carried out the same way every time. Consistency of work ensures mistakes are minimized and tasks are completed promptly. These are just a few benefits of using a script.

Learning Outcomes

As you study this lesson, answer the following questions:

- **What is a script?**
- **What are the common scripting languages and file types?**
- **What are some examples of tasks that can be completed using a script?**

A+ Core 1 and Core 2 CertMaster Perform 15.0

22.3.1 Shell Scripts

Coding means writing a series of instructions in the syntax of a particular language so that a computer will execute a series of tasks. There are many types of coding language and many ways of categorizing them, but three helpful distinctions are as follows:

- **A shell scripting language uses commands that are specific to an operating system.**
- **A general-purpose scripting language uses statements and modules that are independent of the operating system. This type of script is executed by an interpreter. The interpreter implements the language for a particular OS.**
- **A programming language is used to compile an executable file that can be installed on an OS and run as an app.**
  Note:

  The various types of scripting are often described as glue languages. Rather than implement an independent bit of software (as a programming language would), a glue language is used to automate and orchestrate functions of multiple different OS and app software.

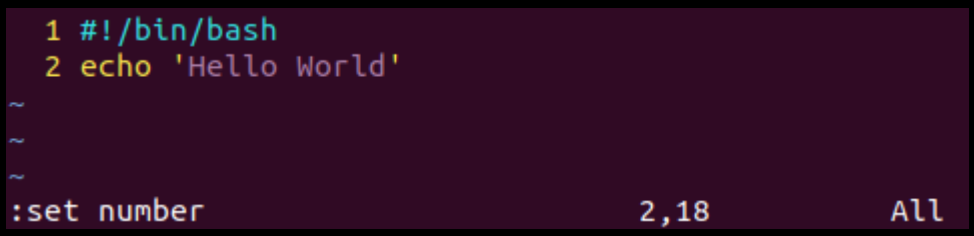
You can develop a script in any basic text editor, but using an editor with script support is more productive. Script support means the editor can parse the syntax of the script and highlight elements of it appropriately. For complex scripts and programming languages, you might use an integrated development environment (IDE). This will provide autocomplete features to help you write and edit code and debugging tools to help identify whether the script or program is executing correctly.

Linux shell script uses the sh extension by convention. Every shell script starts with a shebang line that designates which interpreter to use, such as Bash or Ksh. Each statement comprising the actions that the script will perform is then typically added on separate lines. For example, the following script instructs the OS to execute in the Bash interpreter and uses the echo command to write “Hello World” to the terminal:

```
#!/bin/bash

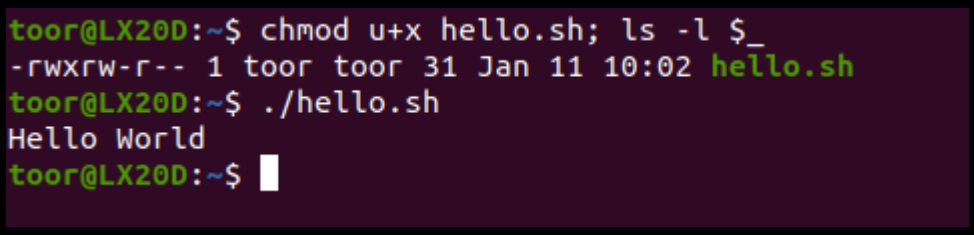
echo 'Hello World'
```

Figure 1. An example of a Linux shell script open in the Vim text editor



Remember that in Linux, the script file must have the execute permission set to run. Execute can be set as a permission for the user, group, or world (everyone). If a PATH variable to the script has not been configured, execute it from the working directory by preceding the filename with `./` (for example, `./hello.sh`), or use the full path.

Figure 2. Setting execute permission for the user and running the script



A+ Core 1 and Core 2 CertMaster Perform 15.0

22.3.3 Basic Script Constructs

To develop a script in a particular language, you must understand the syntax of the language. Most scripting languages share similar constructs, but it is important to use the specific syntax correctly. A syntax error will prevent the script from running, while a logical error could cause it to operate in a way that is different from what was intended.

Comments

It is best practice to add comments in code to assist with maintaining it. A comment line is ignored by the compiler or interpreter. A comment line is indicated by a special delimiter. In Bash and several other languages, the comment delimiter is the hash or pound sign (#).

```
#!/bin/bash

# Greet the world

echo 'Hello World'
```

Variables

A `variable` is a label for some value that can change as the script executes. For example, you might assign the variable `FirstName` to a stored value that contains a user's first name. Variables are usually declared, defined as a particular data type (such as text string or number), and given an initial value at the start of the routine in which they are used.

An argument or parameter is a variable that is passed to the script when it is executed. In Bash, the values `$1`, `$2`, and so on are used to refer to arguments by position (the order in which they are entered when executing the script). Other languages support passing named arguments.

A constant is a label for a value that remains constant throughout the execution of the script. Common constants in scripts may include tax percentages that are not changing during the script.

Branches and Loops

A script contains one or more statements. In the normal scheme of execution, each statement is processed in turn from top to bottom. Many tasks require more complex structures, however. You can change the order in

which statements are executed based on logical conditions evaluated within the script. There are two main types of conditional execution: branches and loops.

Branches

A branch is an instruction to execute a different sequence of instructions based on the outcome of some logical test. For example, the following code will display "Hello Bobby" if run as `./hello.sh Bobby`, executing the statement under "else". If run with no argument, it prints "Hello World":

```
#!/bin/bash

# Demonstrate If syntax in Bash

if [ -z "$1" ]

then

echo 'Hello World'

else

echo "Hello $1"

fi
```

`-z` tests whether the first positional parameter (`$1`) is unset or empty.

Note:

In the condition, the variable is enclosed in double quotes as this is a safer way to treat the input from the user (supplied as the argument). In the second echo statement, double quotes are used because this allows the variable to expand to whatever it represents. Using single quotes would print "Hello $1" to the terminal.

Loops

A loop allows a statement block to be repeated based on some type of condition. A "For" loop can be used when the number of iterations is predictable. The following command executes the `ping` command for each host address in 192.168.1.0/24:

```
#!/bin/bash

# Demonstrate For syntax in Bash
```

```
for i in {1..254}

do

ping -c1 "192.168.1.$i"

done
```

As well as "For" structures, loops can also be implemented by "While" statements. A "While" or "Until" loop repeats an indeterminate number of times until a logical condition is met. The following script pings the address supplied as an argument until a reply is received:

```
#!/bin/bash

# Demonstrate Until syntax in Bash

until ping -c1 "$1" &/dev/null

do

echo "192.168.1.$1 not up"

done

echo "192.168.1.$1 up"
```

The condition executes the ping command and tests the result. When a reply is received, ping returns true. The `&/dev/null` part stops the usual ping output from being written to the terminal by redirecting it to a null device.

Note:

Make sure your code does not contain unintended or infinite loops. The loop above will continue until a reply is received, which could never happen.

Operators

Looping and branching structures depend on logical tests to determine which branch to follow or whether to continue the loop. A logical test resolves to a TRUE or FALSE value. You need to be familiar with basic comparison and logical operators:

Symbol Notation	Switch Notation	Usage
==	-eq	Is equal to (returns TRUE if both conditions are the same)
!=	-ne	Is not equal to (returns FALSE if both conditions are the same)
<	-lt	Is less than
>	-gt	Is greater than
<=	-le	Is less than or equal to
>=	-ge	Is greater than or equal to
&&	AND	If both conditions are TRUE, then the whole statement is TRUE
||	OR	If either condition is TRUE, then the whole statement is TRUE

22.3.5 Windows Scripts

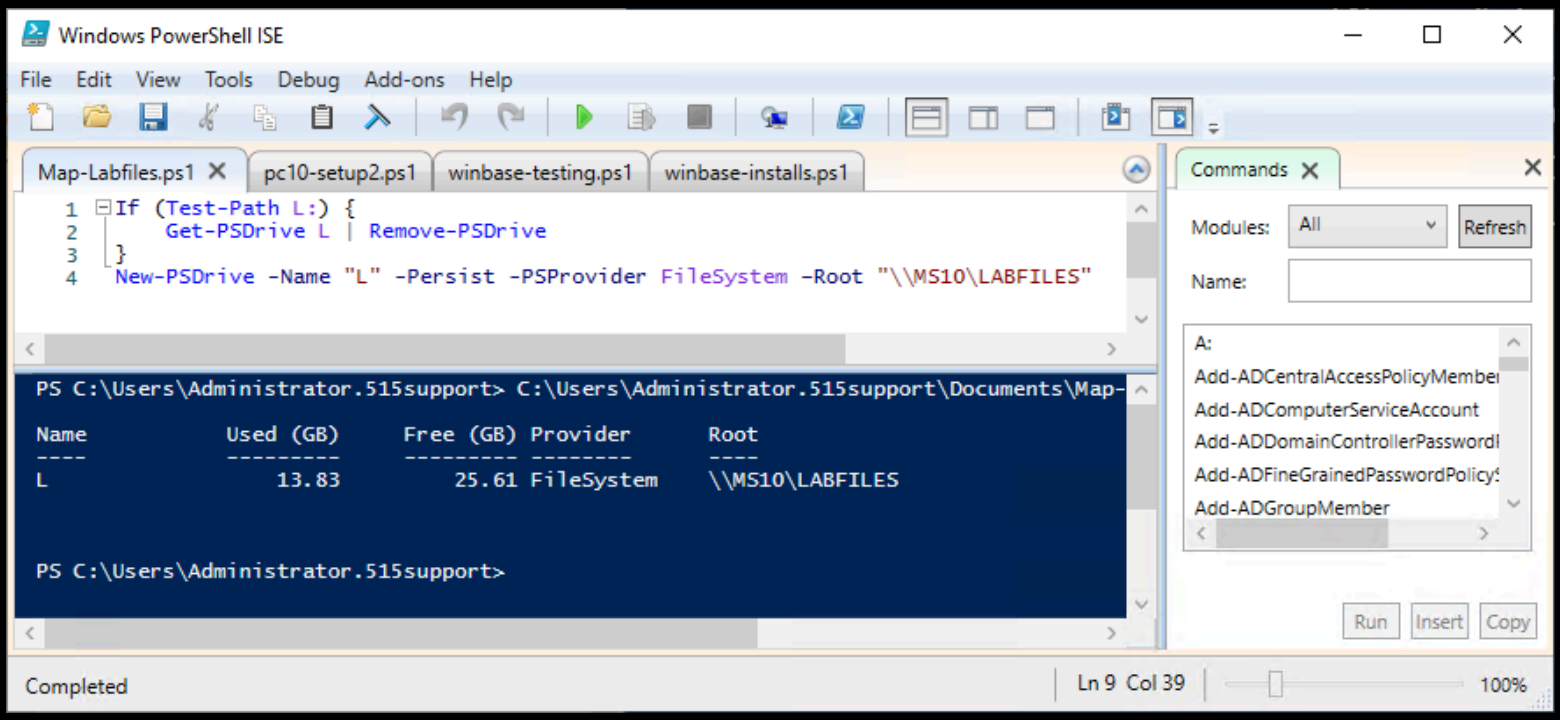
Windows supports several distinct shell coding environments. The three commonly used are PowerShell, Visual Basic Script, and the CMD interpreter.

Windows PowerShell

Windows PowerShell combines a script language with hundreds of prebuilt modules called cmdlets that can access and change most components and features of Windows and Active Directory. Cmdlets use a Verb-Noun naming convention. For example, `Write-Host` sends output to the terminal, while `Read-Host` prompts for user input.

Microsoft provides the Windows PowerShell Integrated Scripting Environment (ISE) for rapid development. PowerShell script files are identified by the .ps1 extension.

Figure 1. Windows PowerShell ISE



Screenshot courtesy of Microsoft.

VBScript

Visual Basic Script is a scripting language based on Microsoft's Visual Basic programming language. VBScript predates PowerShell. VBScript files are identified by the .vbs extension. VBScript is executed by the wscript.exe interpreter by default. Wscript.exe displays any output from the script in a desktop window or dialog. A script can also be run with cscript.exe to show output in a command prompt.

Note:

You would now normally use PowerShell for Windows automation tasks. You might need to support legacy VBScripts, though.

Batch Files

A shell script written for the basic Windows CMD interpreter is often described as a batch file. Batch files use the .bat extension.

Figure 2. An example of a Windows batch file

```
1  if exist L:\ (
2      net use L: /delete
3  )
4  net use L: \\MS10\LABFILES
```

Screenshot courtesy of Microsoft.

22.3.6 JavaScript and Python

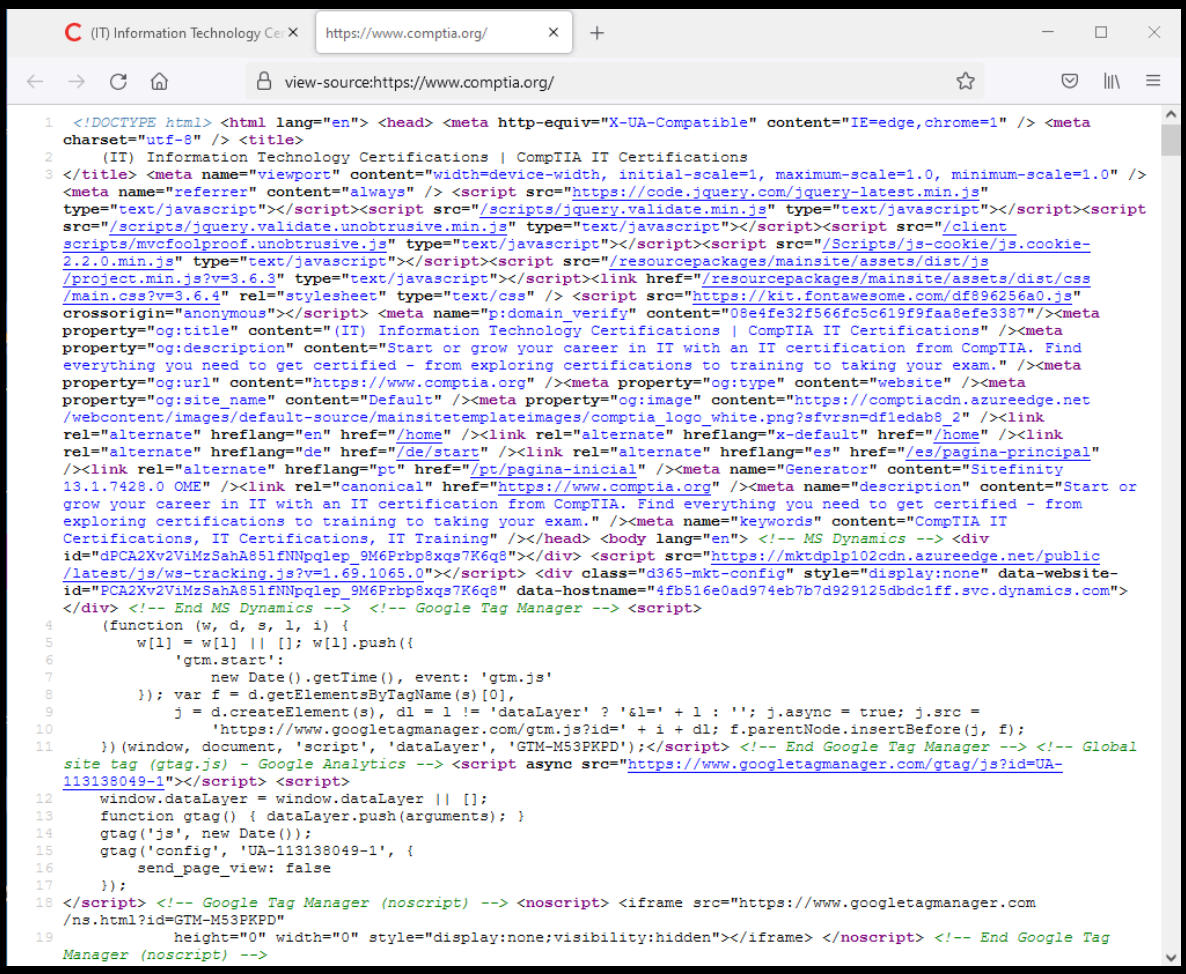
Bash and PowerShell/VBScript are closely tied to the Linux and Windows operating systems respectively. There are many other platform-independent scripting and programming languages.

JavaScript

JavaScript is a scripting language that is designed to implement interactive web-based content and web apps. Most web servers and browsers are configured with a JavaScript interpreter. This means that JavaScript can be executed automatically by placing it in the HTML code for a web page.

If not embedded within another file, JavaScript script files are identified by the .js extension. The Windows Script Host (wscript.exe and cscript.exe) supports JavaScript. JavaScript is also supported on macOS for automation (along with AppleScript). This is referred to as JavaScript for Automation (JXA).

Figure 1. JavaScript code embedded in a web page. Some code is loaded from .JS files from other servers; some code is placed within script tags.

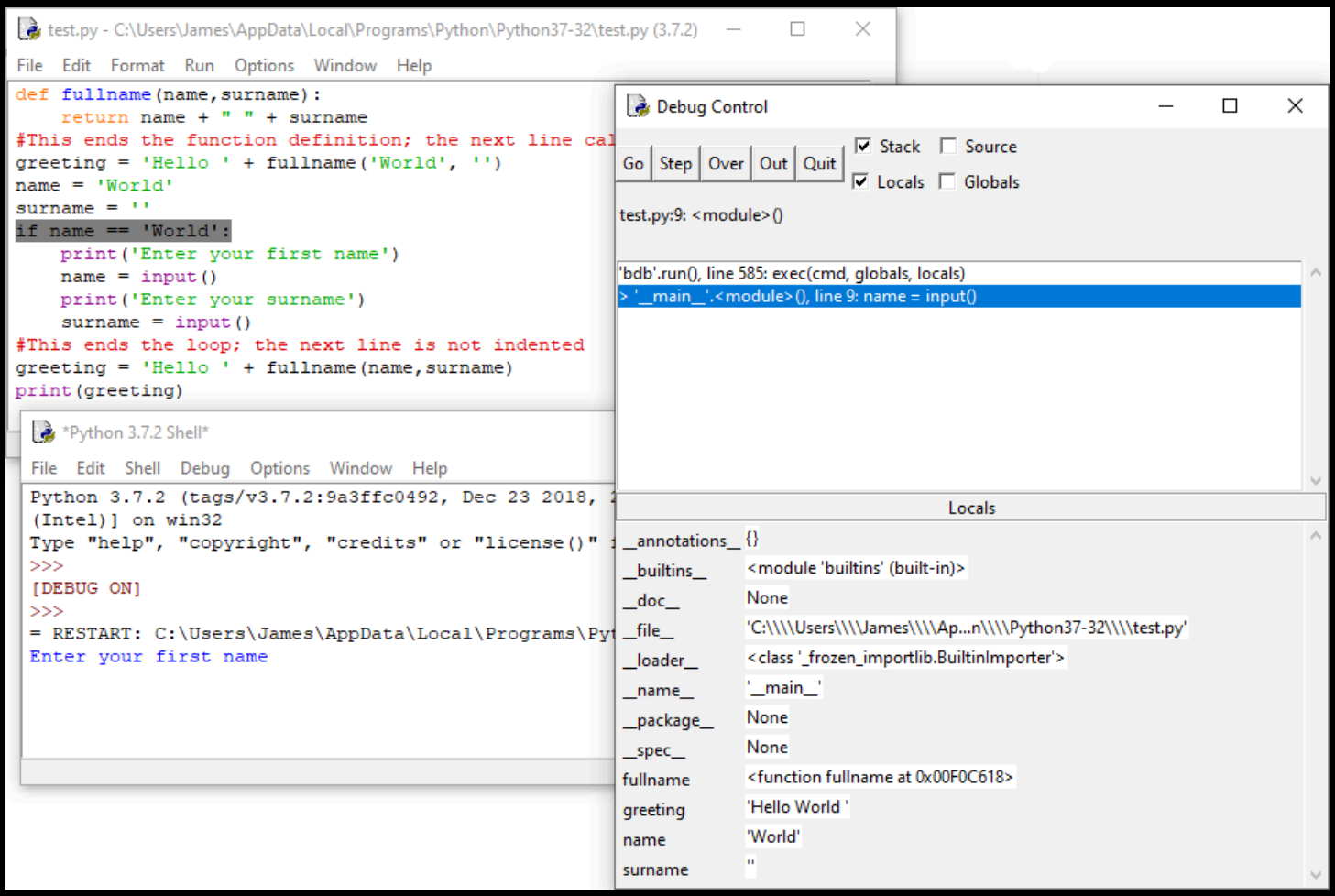


Python

Python is a general-purpose scripting and programming language that can be used to develop both automation scripts and software apps. A Python project can either be run via an interpreter or compiled as a binary executable. There are several interpreters, including CPython (python.org) and PyPy (pypy.org). CPython is the simplest environment to set up for Windows.

Python script files are identified by the .py extension. When using CPython in Windows, there is a console interpreter (python.exe) and a windowed interpreter (pythonw.exe). The extension .PYW is associated with pythonw.exe.

Figure 2. Python Integrated Development and Learning Environment (IDLE)



Description

The script prompts the user for their first and last name, then prints a greeting message. A separate "Debug Control" window shows debugging details, including the current execution point and variable values such as name, surname, and greeting. The script's output in the terminal displays the entered name and the generated greeting message.

Note: There are two major versions of Python: version 2 and version 3. Both to be installed at the same time. In Linux, using the keyword `python` executes a script as version 2, while `python3` executes a script in the version 3 interpreter. As of 2020, Python 2 is end of life (EOL), so scripts should be updated to version 3 syntax.

22.3.9 Scripting Best Practices and Considerations

Deploying any type of code comes with the risk of introducing vulnerabilities. This means that deployment of scripts must be subject to best practices.

Malware Risks

There are several ways that a custom script could be compromised to allow a threat actor to install malware or perform some type of privilege escalation.

- **If the interpreter is not a default feature, enabling it expands the attack surface. Threat actors use environments such as PowerShell to craft fileless malware.**

- **The threat actor could modify the source code to make it act as malware. In effect, the threat actor is using the script as a Trojan.**
- **The script could open a network port or expose some type of user form for input. If the script does not handle this input correctly, the threat actor could exploit a vulnerability to return unauthorized data or run arbitrary code.**

To mitigate these risks, all script source code should be subject to access and version controls to prevent unauthorized changes. Code should be scanned and tested for vulnerabilities and errors before it can be deployed. Scripts should be configured to run with the minimum privileges necessary for the task.

Inadvertent System-Settings Changes

Another risk is from non-malicious or inadvertent threats where a script performs some unforeseen or unexpected system change. One example is accidental DoS, where a script powers off a system rather than restarting it or locks out remote access, perhaps by changing a firewall configuration. Other examples include weakening the security configuration by enabling the script environment, creating port exceptions, disabling scanning software so that the script executes successfully, and so on. Scripts that can only be made to work by disabling security mechanisms are not safe enough to consider running. Test all code in a development environment, and ensure that any changes to hosts that are required to run the scripts are included and updated/monitored through new configuration baselines.

Browser or System Crashes Due to Mishandling of Resources

Another way for a script to cause accidental DoS is through mishandling of resources. Some programming languages, such as C/C++, require very careful use of coding techniques to avoid creating vulnerabilities in the way the instructions manipulate system RAM. Scripting languages don't suffer from this type of vulnerability (they are considered safe with respect to memory handling), but coding mistakes can still lead to situations where the script mishandles computer or storage resources. Some examples are:

- **Creating files that deplete disk storage resources, such as log files or temp files.**
  Using a faulty loop code construct that does not terminate and causes the script to hang.
- **Making a faulty API call to some other process, such as the host browser, that causes it to crash.**

Every script must be tested to try to eliminate these kinds of mistakes before it is deployed, and its execution should be monitored to pick up any bugs that were not found in the test phase.