Confidence in the Connected World

CIS Center for Internet Security®

CIS Controls®

V7.1

CIS Controls Microsoft Windows 10 Cyber Hygiene Guide

To navigate to a specific section in the document click the Bookmarks button in your PDF reader.

Contents

Figures

CIS Controls Microsoft® Windows® 10 Cyber Hygiene Guide

Acknowledgements

CIS (Center for Internet Security, Inc.) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors: Joshua M Franklin

Contributors: Aaron Wilson
Aaron Piper
Robin Regnier
Phil Langlois
Phyllis Lee

Introduction

The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others. While the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

We are at a fascinating point in the evolution of what we now call cyber defense. To help us understand the cyber threat, we have seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat-sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure. But all this technology, information, and oversight has become a veritable “Fog of More” with competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are distributed across multiple locations, many of which are not within our organization’s infrastructure.

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) non-profit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cybersecurity; deliver world-class cybersecurity solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

For additional information, go to https://www.cisecurity.org/

Purpose

Credit card breaches, identity theft, ransomware, theft of intellectual property, loss of privacy, denial of service – these cyber incidents have become everyday news. Victims include some of the largest, best-funded, and most security-savvy enterprises: government agencies, major retailers, financial services companies, even security solution vendors. Many of the victims have millions of dollars to allocate for cybersecurity, yet still fall short in their efforts to defend against common attacks. What is even more disturbing is that many of the attacks could have been prevented by well-known security practices such as regular patching and secure configurations.

What are the rest of us supposed to do? How do organizations with small budgets and limited resources respond to the continuing cyber problem? This guide seeks to empower the owners of small and medium-sized enterprises (SMEs) to protect their businesses with a small number of high priority actions based on the Center for Internet Security’s Critical Security Controls (CIS Controls). Historically, the CIS Controls utilized the order of the Controls as a means of focusing

an organization's cybersecurity activities, resulting in a subset of the first six CIS Controls referred to as cyber hygiene. However, many of the practices found within the CIS cyber hygiene control set can be difficult for organizations with limited resources to implement. This highlighted a need for a collection of best practices focused on balancing resource constraints and effective risk mitigation. As a result, CIS is proposing the following guidance to prioritize CIS Control utilization, known as CIS Implementation Groups (IGs).

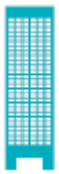
Implementation Group 1

A Group 1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these organizations is to keep the business operational as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally involves employee and financial information. However, there may be some small to medium-sized organizations that are responsible for protecting sensitive data and, therefore, will fall into a higher group. Sub-Controls selected for Group 1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Sub-Controls will also typical be designed to work in conjunction with small or home office Commercial-off-the-Shelf (COTS) hardware and software.

Implementation Group 2

A Group 2 organization employs individuals responsible for managing and protecting IT infrastructure. These organizations support multiple departments with different risk profiles based on job function and mission. Small organizational units may have regular compliance burdens. Group 2 organizations often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Sub-Controls selected for Group 2 help security teams cope with increased operational complexity. Some Sub-Controls will depend on enterprise-grade technology and specialized expertise to properly install and configure.

Implementation Group 3



A Group 3 organization employs security experts that specialize in the difference facets of cybersecurity (e.g., risk management, penetration testing, application security). Group 3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. A Group 3 organization must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Sub-Controls selected for Group 3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

While this approach provides generalized guidance for prioritizing usage of the CIS Controls, this should not replace an organization's need to understand their own organizational risk posture. Organizations should still seek to conduct their own care analysis and tailor their implementation of the CIS controls based on what is appropriate and reasonable given their resources, mission, and risks. Using these types of methods, such as those described in the CIS Risk Assessment Method (RAM), combinations of different implementation groups can inform risk-information

decisions about which sub-controls in their implementation group they may not want to implement, and in turn which higher group's controls they should strive for. The intention is to help an organization focus its efforts based on the resources they have available and integrate controls into any pre-existing risk management process.

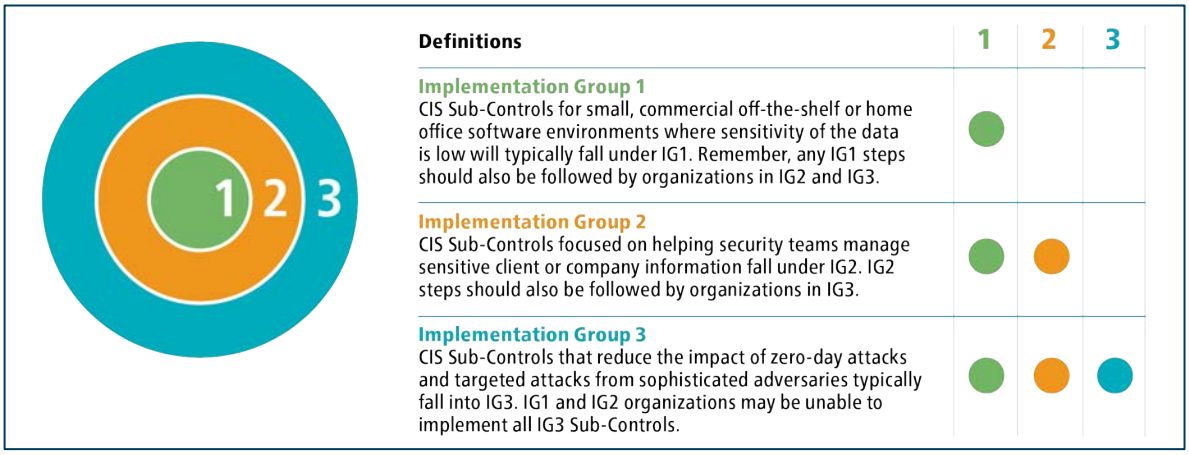


Figure 1 - Implementation Group Definitions

The IGs are self-assessed organizational categories based on relevant cybersecurity attributes. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be reasonable for an organization with a similar risk profile to the definition assigned in Figure 1, and resources to strive to implement. These IGs represent a horizontal cut across the CIS Controls tailored to that type of enterprise, where each IG builds upon the previous one. Accordingly, an organization implementing the sub-controls defined for their IG is moving towards a standard requirement of care as described in the CIS RAM.

This guide provides detailed information on how to accomplish each of the sub-controls within Implementation Group 1 (IG1). This guide builds upon the best practices established via the CIS Controls V7.1. Where possible, the document provides step-by-step guidance on how organizations utilizing the Microsoft Windows operating system and supporting platforms can meet applicable sub-controls.

Audience

This document is meant to help individuals and organizations comply with the set of cybersecurity protections detailed within IG1. The primary audience for this guide is IT contractors for small-, to medium-sized businesses, although it is beneficial to anyone concerned about the security threats listed in Figure 1 – Security Threats:

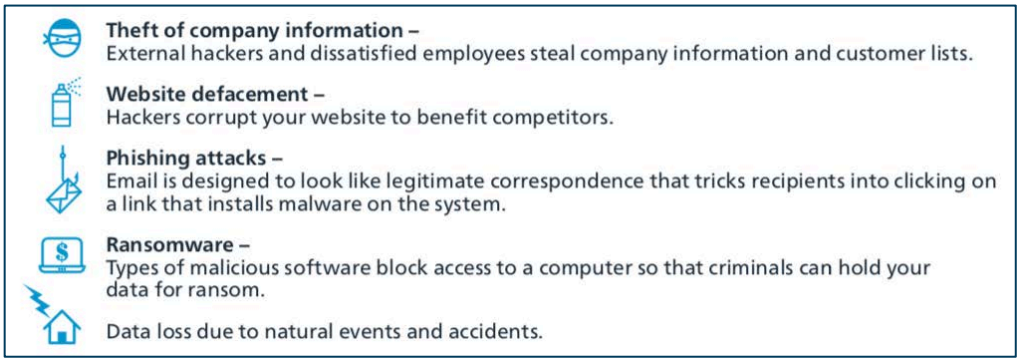


Figure 2- Security Threats

Assumptions

A set of assumptions were identified when developing this guidance:

- Individuals and organizations using this guidance lack large numbers of cybersecurity-focused professionals within their organizations.
- The systems being safeguarded may not be domain-joined, meaning that there is not a central location from which to deploy policy.
- The organization likely has few to zero servers.
- The organization likely uses some cloud services to provide key pieces of infrastructure, such as email.
- The IT environment is fairly static and does not change much over time.

Document Structure

The presentation of each sub-control in this document includes the following elements:

- **Category**: Some Sub-Controls require the implementation or configuration of technology and are labeled as *Technical*. Other Sub-Controls can be implemented via procedural or manual means and are labeled as *Procedural*. Depending on how they are implemented, some Sub-Controls can be both.
- **Purpose**: A description of the importance of the Sub-Control in blocking or identifying presence of attacks and an explanation of how attackers actively exploit the absence of this control. It helps to answer the question of *Why is this important?* Purpose also describes the types of threats that can be mitigated by implementing a particular Sub-Control. Phishing, ransomware, or cybersecurity accidents are examples of threats included within this element.
- **Automation:** When Sub-Controls are automated, they are implemented in a more consistent manner without the introduction of human error. The degree of difficulty of implementation is often a factor discussed here.

- **Guidance and Tools**: This section provides additional information for implementing the Sub-Control, alongside pointers to external guidance documents. Free and open source tools for accomplishing a given Sub-Control can also be found here.

The Appendices of this document includes the following sections:

- **Acronyms and References:** This section contains commonly used acronyms and abbreviations alongside references mentioned throughout the document.
- **Step-by-Step Instructions:** Many of the Sub-Controls contain step-by-step instructions for putting the cybersecurity control in place.

Relevant Microsoft Products

This guide is focused on implementing Windows products for the applicable Sub-Controls. Microsoft creates a variety of products such as:

- Microsoft Windows 10 Home
- Microsoft Windows 10 Pro
- Microsoft Windows Server
- Microsoft Office 365 (O365)

Microsoft Windows 10 Home and Windows 10 Pro are separate editions of Microsoft's Windows 10 operating system. Microsoft provides a useful guide to the differences between these two editions of Windows at the following link (https://www.microsoft.com/en-us/windows/compare). Windows 10 Pro will be the primary edition of the Windows 10 operating system discussed within this document. Windows Home provides the basics most users need to accomplish everyday tasks, such as writing documents, manipulating spreadsheets, and browsing the Internet. Windows Home is also not meant for commercial usage. However, most businesses need more power in order to get their job done, and Windows 10 Pro is designed to fill that niche.

Two common primary enterprise needs include management and security. Windows 10 Pro allows an organization to join a system to a domain. This means that a sever or domain controller will be able to remotely distribute policy and configuration settings from a single centralized system. These policies allow an enterprise to manage how employees can use their computer systems, such as locking their systems after a period of inactivity. Deploying policies is an extremely powerful enterprise feature that can also activate enterprise class security mitigations that may otherwise not be used. For instance, Windows 10 Pro contacts BitLocker, which is Microsoft's full disk encryption system. BitLocker can also encrypt any Universal Serial Bus (USB) and other extra drives.

Office 365 is Microsoft's subscription-based cloud offering that includes an entire suite of Microsoft's web-based applications. This includes standard business applications like Word, Excel, and Outlook. Office 365 also includes the Office 365 Admin Center, which provides access to Azure Active Directory. This feature allows an enterprise to join Windows 10 Pro systems to a

cloud-based domain. This provides many, but not all, of the security and management benefits of using a domain controller without needing to setup an instance of Microsoft Server on premises.

CIS Controls Assessment Module

The CIS Controls Assessment Module is designed to help organizations measure their implementation of the CIS Controls. The Controls Assessment Module functions as a module within CIS-CAT® Assessor v4 (Pro and Lite) and can be run much like other assessments, making it compatible with existing CIS-CAT functionality including remote assessments and the CIS-CAT Pro Dashboard. CIS-CAT stands for the CIS Configuration Assessment Tool; Assessor compares the configuration of target systems to the recommended settings in the CIS Benchmarks and the Controls Assessment Module, while the Dashboard provides a way to view and track Assessor output over time. CIS-CAT Assessor Lite is a limited free version of Assessor, while CIS-CAT Pro Assessor and CIS-CAT Pro Dashboard require CIS SecureSuite® Membership.

The first version of the Controls Assessment Module covers IG1 in Windows 10 environments, providing a combination of automated checks and survey questions to cover the 43 IG1 Sub-Controls. For the more procedural Sub-Controls, the Controls Assessment Module allows users to save yes/no answers documenting their implementation of those Sub-Controls at the organizational level. For Sub-Controls that are conducive to automation, specific settings in the environment are checked to generate a machine-specific pass or fail for that Sub-Control.

Although it is the goal of CIS for a Windows 10 system configured with this Windows 10 Implementation Guide to pass a Controls Assessment Module assessment, there are subtle differences for a subset of CIS Sub-Controls. The Controls Assessment Module currently checks for the set of CIS Sub-Controls listed below with the differences between Sub-Control assessment methodologies between this Windows 10 Implementation Guide and the Controls Assessment Module.

Table 1 - Comparison Control IDs Against Control Assessment Module and Windows 10 Guide

Ctrl ID	Controls Assessment Module	Windows 10 Guide
3.4	Passes if automatic updates are set to 'Auto Download and schedule the install'	Shows how to enforce Windows 10 updates
4.2	Passes if the Minimum Password Length meets or exceeds a specific minimum	Shows how to change password and enforce length
6.2	Passes if at least 1 Audit Policy Sub-Category is enabled	Shows how to configure according to the policy specified by Microsoft as detailed in the Enabling the System Event Audit Log section in Appendix B

Ctrl ID	Controls Assessment Module	Windows 10 Guide
8.2	Passes if any Antivirus is enabled and up-to-date	Shows how to configure Windows Defender
8.5	Passes if AutoPlay and AutoRun are disabled	Shows how to configure AutoPlay and AutoRun
9.4	Passes if all 3 Windows Firewall profiles are enabled and have a default deny rule for inbound traffic	Shows how to enable Windows Defender firewall via UI and LGPE
10.1	Passes if Windows 10 File History is turned on for at least 1 user	Shows how to use Windows File History
10.2	Passes if the date of the last successful Windows System Image backup occurred within a specified number of days	Shows how to use the Windows 7 Backup tool
10.4	Passes if native Windows encryption is turned on for the backup drives being used to store backups for File History and System Image backup (if enabled)	Shows how to turn on BitLocker
13.6	Passes if BitLocker is enabled on all drives	Encourages usage of CIS Benchmarks for iOS and Android
15.7	Passes if all wireless connections use WPA2	Shows how to check for network type
16.9	Passes if all enabled local user accounts have been logged into within a specified number of days	Shows how to view accounts on a system
16.11	Passes if Interactive Logon Machine inactivity limit is enabled and less than a specified timeframe	Shows how to configure Interactive logon limit

CIS Sub-Controls Identified as Implementation Group 1

CIS Control 1.4: Maintain Detailed Asset Inventory

Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.

Category
Procedural, Technical

Purpose
An accurate and up-to-date inventory of computer systems within a network is often the first step in securing an enterprise. This list of information systems is known as a *hardware asset inventory.* Having a definitive list of what hardware is supposed to be part of a network enables comparison against the list of systems that are in place. This allows for the identification of unauthorized devices that should not be connected. A hardware asset inventory also helps define what an organization needs to protect.

An asset inventory often extends beyond solely what is connected to the network. Many organizations utilize older smartphones, laptops, networking gear, and other technology that may not be connected, or even powered on; yet might still contain sensitive information if the data is exfiltrated outside of the network. In addition to physical systems, many enterprises use third-party services for website hosting or email that are hosted in the cloud. Accordingly, any third-party services and cloud platforms should be included in the asset inventory. Examples of what to track include:

- General computer workstations, laptops, phones, tablets;
- Physical systems and devices operated or possibly owned by another organization that are connected to the enterprise network (e.g., point of sale devices); and,
- Systems used by an organization that are cloud hosted.

Although asset management does not specifically mitigate any threats, it is the foundation for a large majority of cybersecurity activities. Cybersecurity expert Daniel Meissler points out that, "If You're Not Doing Continuous Asset Management You're Not Doing Security", and argues that it is one of the most important aspects of cybersecurity. Meissler states that lacking this asset inventory is one of the main reasons that companies get breached. *If you don't know what you are supposed to be defending, you can't properly defend it.*

Automation
This Sub-Control is automatable but not every enterprise will have the resources to do so. In this case, many organizations will perform manual asset tracking by hand. Manual asset tracking often uses a spreadsheet with predefined columns and rows to help companies track the right data. It is often cumbersome, prone to error, and takes a good deal of time to get right. However, even an inventory with some holes in it is better than no asset inventory at all. Automated asset inventory can include using a web application or program installed on an in-house computer to store and track information within a database. It can also include a scanning tool that will

automatically query devices with a variety of methods. There is a hybrid solution, where organizations use free or open source tools like those mentioned below and copy the results from those scans into a spreadsheet or other database.

Guidance and Tools

A variety of software is available in the market to solve this problem, but it may be too expensive for most. The following is a list of free tools and software which can help to ease the burden of asset tracking:

- *Nmap*: Famous multipurpose network scanner, used by system administrators and hackers across the world to identify which devices are connected to a network (https://nmap.org). Be careful to only scan networks for which permission was explicitly given. It is often impolite, and in many cases illegal, to scan networks owned by others.
- *Spiceworks*: This is a free IT inventory and asset management software to identify devices and software on a network (https://www.spiceworks.com).
- *ZenMap*: This tool utilizes Nmap and places a user interface on top of it to make the tool easier to use for those who do not feel comfortable using the command line (https://nmap.org/zenmap).
- *CIS Hardware and Software Asset Tracking Spreadshee*t: This free spreadsheet is created by CIS to help track enterprise systems and other assets. It can be modified as needed to meet an enterprise's unique needs. The primary elements within the spreadsheet are also described within the relevant appendix (https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/).

Step-by-step instructions for implementing this Sub-Control can be found in:
Hardware & Software Inventory.

CIS Control 1.6: Address Unauthorized Assets

Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.

Category
Procedural

Purpose
This Sub-Control is meant to ensure that a list of authorized assets can be compared against the list of devices that are actually connected to an enterprise network. Any difference between the devices on this list and what exists on the network should be investigated and will likely include phones, tablets, and laptops. It is possible that a device under investigation is actually authorized to be in place. In this case, it can be removed from the investigation list. If a device is not meant to be on the network, it should be removed from the network and thoroughly investigated. Unauthorized devices may be accessing enterprise network traffic, including proprietary or sensitive information. They also are in a position on the network from which to launch attacks and hack into organizational systems.

This Sub-Control helps to prevent unauthorized eavesdroppers on a public network. Attackers might be able to view enterprise traffic or change it while it is being sent. Eavesdroppers can be listening on wired and wireless networks. Physically finding a device can be a difficult task, as it is often hard to associate a device name (e.g., John's Android) or hardware network address media access control (MAC) address to a particular device by sight. Device names and MAC addresses can provide hints to the type of device, but they can also be faked to fool anyone trying to find the device. Changing a wireless fidelity (WiFi) network password may be a useful step to take if a specific device in question is unable to be identified, although this will only apply to wireless devices.

Automation
This Sub-Control is automatable but will require someone with a higher than average level of network know-how in order to install, configure, and regularly use the right software packages.

Guidance and Tools
Many modern wireless access points and routers have a feature that will show a network map of all devices currently connected to the access point. It is often possible to click on any device in question and remove it from the network.

CIS Control 2.1: Maintain Inventory of Authorized Software

Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

Category
Procedural

Purpose
An accurate and up-to-date inventory of all company software is nearly as important as tracking the hardware inventory, as detailed in Sub-Control 1.4. By tracking the software being used on organizational assets, it is possible to ensure that only authorized software is installed. This is known as creating an authorized software inventory. Unauthorized software may include older versions of previously authorized software applications, or software installed by an employee, unbeknownst to the enterprise (sometimes referred to as *shadow IT*). Unauthorized software also includes any malware or malicious code installed by an attacker that gained access to an enterprise system or network. Understanding the software installed on a system helps organizations to define their software attack surface and allows for a plan to be devised to remove that software.

Shadow IT

When unauthorized IT software is used for enterprise business, this is known as shadow IT. These IT systems, applications, and cloud platforms are in use without the knowledge and approval of management and are not tracked or secured.

Software should be tracked for all enterprise systems and devices, even if they do not have network access. An old, unpatched application running on a non-networked system may be connected to the enterprise network at some point in the future. Old phones, laptops, networking appliances, and other technology that are rarely powered on may still contain sensitive information. In addition to physical systems, some companies may rely upon cloud infrastructure for email and data storage. Virtualized systems are another asset type that can contain sensitive enterprise data. Software associated with cloud-based and virtualized systems should both be included in a software asset inventory. Therefore, examples of software on different types of systems that should be tracked to comply with this Sub-Control include:

- Software pre-installed on the operating system,
- Software installed by an organization,
- Cloud infrastructure and applications, and,
- Virtual machines and their hypervisors

Although asset management does not specifically mitigate any threats, it is the foundation for a large majority of cybersecurity activities. Organizations interested in a stretch goal to help address future threats can consider implementing CIS Sub-Control 2.4, which suggests the following information to be tracked:

- name,
- version,
- publisher,
- install date, and,
- operating system.

Automation

This Sub-Control is automatable but not all organizations will have the resources to do so. Many small- to medium-sized organizations will need to manually curate their software inventory. Manually tracking software information is generally done with a spreadsheet with predefined columns and rows to facilitate proper data collection. It is often cumbersome, prone to error, and takes a good deal of time to get right. Yet, even an incomplete inventory is better than no asset inventory at all. Automated software inventory management can include using a web application or program installed on an in-house computer to store and track information within a database. It can also include a scanning tool that will automatically query devices with a variety of methods.

Guidance and Tools

There is no universally agreed upon method for tracking software assets. A variety of software is available in the market to solve this problem but may be too expensive for many. The following is a list of free tools and software which can help to ease the burden of asset tracking:

- *Nmap*: Famous multipurpose network scanner, used by system administrators and hackers across the world to identify which devices are connected to a network (https://nmap.org). Be careful to only scan networks for which permission was explicitly given. It is often impolite, and in many cases illegal, to scan networks owned by others.
- *ZenMap*: This tool builds on top of Nmap, and puts a graphic user interface on top of it to make the tool easier to use for those who do not feel comfortable using the command line (https://nmap.org/zenmap).
- *Spiceworks*: This is a free IT inventory and asset management software to identify devices and software on a network (https://www.spiceworks.com).
- Netwrix: Variety of free tools to identify information about administrative access on any relevant systems (https://www.netwrix.com).
- OpenAudIT: Inventory applications and software on workstation servers and network devices (http://www.open-audit.org).
- *CIS Hardware and Software Asset Tracking Spreadshee*t: This free spreadsheet is created by CIS to help track enterprise systems and other assets. It can be modified as needed to meet an enterprise's unique needs (https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/).

Step-by-step instructions for implementing this Sub-Control can be found in:
Hardware & Software Inventory.

CIS Control 2.2: Ensure Software Is Supported by Vendor

Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

Category
Procedural

Purpose
The phrase *vendor supported software* means that a program or application being used for enterprise business is a product currently offered and available for purchase from the developer. Furthermore, a supported application is still generally under development, which means that software and security updates are regularly made available and distributed to customers. If an organization is using unsupported software, any computer system running that software will most likely be vulnerable to attack.

Software that is out of date often contains vulnerabilities and other software bugs that can be used by an attacker to gain a foothold within an enterprise network. The longer software goes without receiving an update, the more likely it is to have significant security problems. Therefore, triaging the number of bugs and their severity is key. Allowing unpatched and old software within an enterprise is one of the most dangerous practices possible from a security perspective.

Automation
This Sub-Control is not automatable. No automated method exists for a computer system to identify if software purchased from a vendor is currently supported.

Guidance and Tools
The primary thing that can be done is to understand the support structure from the developer for any software application *before it is purchased and installed*. This may involve researching alternative products and the reviews available online. Useful items to investigate before the software is purchased include:

- Length of pledged support – Support may be provided for 5 years, whereas others may only be supported for 6 months. This is one of the most critical factors.
- Cost of support – Many products will receive updates for free, yet others may charge for updates.
- Who will provide support – The original developer or some other developer may support the application.
- Support history – Pledges of support are often made, but sometimes not kept.

CIS Control 2.6: Address Unapproved Software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

Category
Procedural

Purpose
This Sub-Control is the natural progression from Sub Control 2.1. Once a software asset inventory has been created, each computer, phone, and/or tablet should be checked to ensure that the software installed on that system is authorized to be there. When unapproved software is identified, it should be uninstalled or otherwise removed. A regular cadence should be established to survey relevant systems for unauthorized software.

Unapproved software has not been reviewed by anyone within an organization that has decision authority for IT. Additionally, it has not been reviewed by a security professional to understand if the software meets an organization's minimum baselines for security. Unapproved software is commonly out of date and can contain known vulnerabilities that can be exploited. Unapproved software may also be malware, all of which should be avoided.

Automation
This is an automatable Sub-Control and multiple types of tools can used to alleviate this problem. Examples include typical IT asset management tools, that can help to track both hardware and software, alongside versions of software in use. Refer to Sub-Controls 1.4 and 2.1 for additional information regarding this category of software tools. Another category of software that can help is antivirus, which helps to identify malicious software installation and identify when it is on a system. Finally, whitelisting software will let an enterprise specify a list of applications that are allowed to run on enterprise systems.

Guidance and Tools
Examples include typical IT asset management tools, that can help to track both hardware and software, alongside versions of software in use. Refer to Sub-Controls 1.4 and 2.1 for additional information regarding this category of software tools. Another category of software that can help is antivirus, which helps to identify malicious software installation and identify when it is on a system. Finally, whitelisting software will let an enterprise specify a list of applications that are allowed to run on enterprise systems.

Step-by-step instructions for implementing this Sub-Control can be found in:
Uninstalling Software.

CIS Control 3.4: Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

Category
Technical

Purpose
Security patches are updates to a computer's operating system (OS) or installed software applications and are a basic part of IT maintenance. The patches the OS developers provide often contain new features, but also contain fixes to recently discovered security vulnerabilities. Over time, operating systems go "stale" and need to be updated. Without a constant stream of security patches, computer systems can be infected by malware that can read sensitive company data, or simply destroy it. Accordingly, patching systems is one of the primary ways an enterprise can protect itself from attackers.

Guidance and Tools
There are free products available to assist with patch management. By default, Windows 10 is configured to download and install updates automatically unless that is modified by a user or administrator.

- Itarian: This application offers a patch management solution for Windows (https://us.itarian.com/patch-management/free-windows-patch-management-software.php).
- Opsi: A more complicated solution that can help to manage both Windows and Linux platforms (https://www.opsi.org).

CIS Benchmarks: CIS offers PDFs with configuration guidelines for 140+ technologies (https://www.cisecurity.org/cis-benchmarks).

Step-by-step instructions for implementing this Sub-Control can be found in: Configuring Automated Operating System Patch Management via Windows Settings.

CIS Control 3.5: Deploy Automated Software Patch Management Tools

Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

Category
Technical

Purpose
Security patches are updates to a computer system's operating system or installed software and applying them is a basic part of IT maintenance. Just like patching the OS, patching these software applications is a basic part of cybersecurity. The patches from application developers may contain new features, but also contain fixes to recently discovered security vulnerabilities. Without a constant stream of security patches, old and insecure applications can have vulnerabilities exploited, and infected by malware that can read sensitive enterprise data, or simply destroy it.

Automation
Some operating systems can help to remind users to update certain applications, especially those obtained within the application marketplace that is part of the operating system. With today's platforms, app stores are not just on mobile devices. Microsoft Windows 10 has an app store called *Windows Apps* and Apple's store is called the *Mac App Store*. Both stores can be configured to automatically install software updates from the application developer that were initially installed via an app store.
Software obtained outside of an app store must be updated in an entirely different manner. Third-party software distributed outside the app store requires dedicated management software to patch it. In the end, keeping the total number of programs installed on a computer to the smallest number possible, helps with both management and security by reducing attack surface.

Guidance and Tools
In many instances, it may be worthwhile to attempt to only install applications from the Microsoft App Store as updates to those applications can be more easily managed. Not all business applications will be available in the Microsoft App Store and this will likely only be a partial solution.

- Itarian: This package offers a free patch management solution for Windows (https://us.itarian.com/patch-management/free-windows-patch-management-software.php).
- Opsi: Opsi is a more complicated solution that can help to manage both Windows and Linux platforms (https://www.opsi.org).
- PDQ: The free tier can assist in keeping systems up to date (https://www.pdq.com).
- Microsoft Store: If applications are installed via the Microsoft Application Store, they can be set to be automatically updated (https://support.microsoft.com/en-us/help/15081/windows-turn-on-automatic-app-updates).

Step-by-step instructions for implementing this Sub-Control can be found in:
Automatic Application Updates via the Microsoft Application Store.

CIS Control 4.2: Change Default Passwords

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

Category
Procedural

Purpose
Default passwords are the passwords that ship with computers, applications, routers, and other equipment. Default passwords are a very common way for computer systems, devices, and applications to be hacked. Lists of default passwords for operating systems, applications, and devices are readily available on the Internet for anyone to download and try. Therefore, enterprise passwords need to be changed from the defaults to something that is not easily guessable or easily available from a search engine.

If a password for a wireless router is guessed, an attacker will be able to add and remove network devices, which will allow them to read sensitive enterprise information. To guess a router's default password, it is often sufficient to identify the manufacturer and model of the device. Attackers may be able to find this information by viewing the device in person, or remotely based on a router's wireless network name (i.e., service set identifier (SSID)), MAC address, and network scans. Lists are easily available online with the default passwords for wireless routers commonly used in small and home offices. If a password for an application, device, or other system is guessed, an attacker may be able to read the enterprise information stored there or take control of the entire device.

Automation
Changing default passwords within software and network equipment is generally not automatable. Each software application or piece of network equipment must be individually investigated and changed.

One of the main issues with changing default passwords is the need to remember all the passwords. Writing passwords down on paper is considered an insecure practice. A better option is to use a password manager. Free examples include:

- KeePass: This is an open source password manager (https://keepass.info).
- LastPass: This is a popular password manager for personal use

CIS Benchmarks: The benchmark for an OS or application may contain passwords that should be changed, but not all products will have CIS Benchmarks, or have default passwords (https://www.cisecurity.org/cis-benchmarks).

Step-by-step instructions for implementing this Sub-Control can be found in:
Changing the default password on Windows 10 Pro.

CIS Control 4.3: Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar uses.

Category
Procedural

Purpose
Accounts on a computer system can have different types and sets of privileges. The accounts with the highest access privileges are called *administrative accounts*. Other terms for administrative account include *admin account* or *superuser* accounts. These accounts grant access to all a computer system's data and functionality. It follows that protecting these accounts is of the utmost importance. If administrative accounts are abused or taken advantage of, they can be used to compromise an entire system and potentially the other computers connected to them via a network. For example, if an administrative account is used to browse the web, and accidentally downloads malware, the malware will be able to run on a computer with the highest levels of access.

Yet, administrative accounts are needed for certain important tasks, such as installing new programs, updating the operating system, or adding new users. This Sub-Control states that administrative tasks need to be performed with a separate account solely dedicated to administrative tasks. Normal user accounts should be used for everyday business tasks, like using accounting software or performing market research via the web. If a vulnerability is exploited within a normal user account, the impact will be substantially less than if the same vulnerability is exploited under an admin account.

If someone can obtain administrative access on a computer system, they essentially have the keys to the kingdom. They will be able to steal passwords stored on the computer, which may be used in other computer systems or applications within a network. They will also be able to install a rootkit which is a type of malware that is sometimes undetectable, even by antivirus software. These types of information could compromise enterprise systems for months or even years.

Automation
This Sub-Control generally cannot be automated. Users must manually check to identify if their account is an administrator account and if it's not, establish separate administrative accounts.

Guidance and Tools

There is no standard that can be pointed to for how to keep everyday user accounts and administrative accounts separate. With that said, the following guidance can be useful:

- Passwords should be different for everyday accounts and administrative accounts.
- If multifactor authentication is not in use, the passwords for administrative accounts should follow current best practices for password strength.
- Once a task is completed that required administrative access, make sure to immediately logout of the account.

Step-by-step instructions for implementing this Sub-Control can be found in:
Identifying if an Account is an Administrator.

CIS Control 5.1: Establish Secure Configurations

Maintain documented security configuration standards for all authorized operating systems and software.

Category
Technical

Purpose
Establishing secure configurations means that each computer system within an enterprise must have the appropriate security settings applied. Many computers do not come with all the security settings appropriately configured “out of the box” as these settings tend to decrease the functionality and options afforded to users. Further complicating the situation, as operating systems and applications receive updates configuration settings can change. New configuration settings may be created, and others may be removed. This creates a constant problem that needs to be regularly monitored and addressed.

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use, not security. Open services and ports, default accounts or passwords, older (vulnerable) protocols, preinstallation of unneeded software; all can be exploitable in their default state. All these improper configuration settings can be taken advantage of by attackers. Properly configuring enterprise computer systems can help to defend against major types of malware and even network-based attacks.

Automation
This Sub-Control is completely automatable if an enterprise decides to acquire the appropriate software. Moving past this Sub-Control, some software tools can help organizations to maintain secure configurations over time, which can be quite difficult. Although initial configurations may be done by hand, monitoring for changes and out of date settings is best performed by software.

Guidance and Tools
Many tools are available to check and maintain secure configurations within an enterprise. Additionally, multiple organizations put out configuration guidance for systems and applications.

- OpenVAS: Tool to scan systems to check security baselines (www.openvas.org).
- DISA STIG: The DISA STIGs are a set of configuration guidance developed and maintained by the United States Department of Defense (DoD) (https://iase.disa.mil/stigs/Pages/index.aspx).

CIS Benchmarks: CIS offers free PDFs with configuration guidelines for 140+ technologies (https://www.cisecurity.org/cis-benchmarks).

CIS Control 6.2: Activate Audit Logging

Ensure that local logging has been enabled on all systems and networking devices.

Category
Technical

Purpose
On the surface, logging may appear to be a low priority activity, but it is a critical cybersecurity control to have in place within an enterprise. Once a security breach occurs, reviewing logs is often the primary way that computer incident responders identify who did what, and when they did it. Furthermore, if logging is enabled on network devices (e.g., routers), historical activities can be tracked for the entire enterprise network. Logs can also be helpful to an enterprise when performing general maintenance activities to understand the current status of computer systems and networks and be notified to take action if there is a problem.

Logging is not a prevention mechanism, meaning that logs do not stop attacks directly. Instead, logs help to provide *tamper detection*, which means if an unauthorized modification occurs within an enterprise computer system (or its data), it is possible to know that something was changed.

Automation
There are various methods of how to automate logging. Enabling logging on systems can be done manually on a system-by-system basis. Yet, logging is often considered a system configuration option and can be automated with software dedicated to assessing and implementing secure configurations. Moving past just enabling logs, systems known as SIEMs (security information and event management) can be utilized that ingest log data from all systems in an enterprise and perform data analysis to find breaches or network-wide issues or failures. SEIMs typically require a more advanced IT infrastructure and dedicated IT personnel to manage.

Guidance and Tools
There are many types of logs that can be enabled. When beginning to enable logging on enterprise systems, utilize software and hardware inventory lists to ensure that the proper types of logs were enabled for each system or application. Look to enable logs for both the operating systems and supported applications for all enterprise systems, and also survey network devices like firewalls and wireless access points to understand their logging capabilities. In order to enable logging on firewalls and wireless access points, documentation may be required for the unique network appliance in an enterprise.

CIS Benchmarks: The CIS Benchmarks offer a list of what logging settings should be enabled for various platforms and applications (https://www.cisecurity.org/cis-benchmarks).

Step-by-step instructions for implementing this Sub-Control can be found in Enabling the System Event Audit Log for Windows 10 Pro.

CIS Control 7.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure that only fully supported web browsers and email clients are allowed to execute in the organization; ideally only using the latest version of the browsers and email clients provided by the vendor.

Category
Procedural

Purpose
Web browsers and email clients are some of the most common applications that employees use to access the Internet. This means that browsers and email clients are on the front line of an organization's IT infrastructure and are regularly exposed to a variety of digital threats. In fact, they are arguably the most exposed applications within an enterprise. Because of this, browsers and email systems should be kept up to date since the most recent version of a software application includes the most recent security patches.

Attacks on email clients and browsers can lead to a variety of cybersecurity problems. One potential problem source is the installation of browser extensions, which are small applications that can extend a browser's functionality. These can be helpful and provide security benefits (such as managing passwords). Unfortunately, if an attacker is able to install a malicious browser extension, they can often severely compromise the security of a browser by viewing all web activity and potentially reading information that would normally be inaccessible.

Automation
Some browsers update automatically by default, like Chrome; whereas others will require an additional configuration. Email clients can be similarly setup to receive automated updates. Security tools can be utilized to understand when browsers, email clients, and other programs are out of date.

Guidance and Tools
Keeping browsers and email clients up to date is generally a fairly simple task. Besides using supported software in the first place, it is important to take the extra step to make sure that browsers and clients regularly receive security updates and patches that are made available. These updates are not installed by default on all browsers and email clients, meaning the browsers and clients need to be manually configured. Once browsers and email clients are properly configured, only periodic monitoring is required.

- US-CERT: Per-browser configuration instructions are provided by US-CERT (https://www.us-cert.gov/publications/securing-your-web-browser).

CIS Benchmarks: CIS offers free PDFs with configuration guidelines for common browsers (https://www.cisecurity.org/cis-benchmarks).

CIS Control 7.7: Use of DNS Filtering Services

Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

Category
Technical

Purpose
While the DNS can be difficult to grasp, the important details are relatively simple. DNS can be thought of as a phonebook for websites that translates a human understandable domain such as (www.cisecurity.org) to a series of numbers that a computer can understand (i.e., Internet Protocol (IP) address). Therefore, when a computer wants to connect to cisecurity.org, it uses DNS to look up where it can find example.com, much like how a phone book would be used to search a person's name to get their phone number. And all of this happens transparently in the background when requesting a webpage, so that individuals to solely need to remember the domain name instead of complex IP addresses.

This Sub-Control helps prevent enterprise infrastructure from connecting to known malicious servers that control, host, or distribute malware, or collect sensitive information. Many attackers will host a malicious domain like "evil.com" to enable malicious activities, such as tricking users into giving sensitive credentials (i.e., phishing) or control already infected systems. By using a DNS filtering service, an enterprise can ensure their systems are pointing to a filtered phonebook (DNS responses) that would not provide bad phone number to any known bad domains; thereby protecting an enterprise from being infected or communicating with malicious systems.

Automation
There are many ways that this Sub-Control can be implemented in an environment and it will mostly depend on how the enterprise is currently configured. This Sub-Control is completely automatable with the correct hardware and software being used in a network. Unfortunately, the implementation of this Sub-Control will likely require someone with specialized knowledge of networking and DNS, alongside an external trusted source for DNS information.

Guidance and Tools
Multiple organizations exist that provide DNS filtering. Some even provide this service free of charge such as Quad9. With a simple configuration change, enterprise systems will use the filtering service with little to no impact on an organization's Internet browsing all the while blocking bad traffic. Accordingly, the following resources can be of assistance:

- OpenDNS: Steps for setting up OpenDNS on Windows 10 (https://support.opendns.com/hc/en-us/articles/228007207-Windows-10-Configuration).
- Quad9: Steps for setting up Quad9 on Windows 10 (https://www.quad9.net/microsoft).

CIS Control 8.2: Ensure Anti-Malware Software and Signatures Are Updated

Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

Category
Technical

Purpose
Anti-malware, also known as anti-virus, is a well-known security technology. Anti-malware suites work by constantly monitoring all of the running applications on a system and alerting an enterprise administrator if a malicious program or other suspicious activity is detected. A list of suspicious applications and actions that the security technology looks for is created and kept up to date by the anti-virus company. That company regularly delivers updates to the suspicious applications and actions list on a regular basis, and these updates are called *signatures*. If signatures are not downloaded and installed on a regular basis, machines may be vulnerable to the most recent attacks. Because it is easy to forget, antivirus updates should be set to automatically download and install *on each and every computer or server in an enterprise.*

Malware is software specifically designed to attack computer systems, devices, and data. Malware is the catch-all term for spyware, adware, and all the other types of malicious software, and it is quick to change and hard to track. Malware can enter an enterprise through any number of points such as email attachments, malicious apps, web pages, and USB drives. Modern malware can be quite benign and just slow a computer system down, or be much more pernicious and pilfer passwords, steal proprietary company secrets, or delete all enterprise data.

Automation
This is an easy Sub-Control to automate and is worth the time spent to properly configure.

Guidance and Tools
Although there are free products designed to remove malware, many free antivirus tools may actually be malware themselves, or try to install malware on a computer system. The safest option is to use and properly configure the set of tools that comes with Windows 10. Microsoft provides two closely related products for free that come built-into every copy of Windows.

- Windows Defender Security Center: This application is a portal into a Windows system's overall security status, including the downloading of software updates (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-security-center/windows-defender-security-center).

Step-by-step instructions for implementing this Sub-Control can be found in:
Checking Windows Defender Security Center.

CIS Control 8.4: Configure Anti-Malware Scanning of Removable Media

Category
Technical

Purpose
Removable media includes USB drives, memory cards, and external hard drives - just to name a few examples. These devices are commonly used to store photos, videos, and many types of enterprise data. Removable media is also one method used by attackers to install malicious software on computer systems. This attack method can be used to infect traditional enterprise workstations, but also computer systems viewed as secure since they lack a WiFi or Internet connection. Entirely banning the use of removable media is often impractical for businesses. In order to combat this threat, enterprise systems should be configured to scan removable devices for malware before they can be read by users.

Malware is software specifically designed to attack computer systems, devices, and data. Malware can enter an enterprise through any number of points such as email attachments, malicious apps, web pages, and USB drives. This Sub-Control was specifically included due to the emerging technique of dropping USB drives embedded with malware in parking lots or other areas where employees are likely to pick them up and plug them into enterprise systems. One academic study dropped 300 USB sticks around a school which resulted in ~50% of them being inserted into computers. Many were inserted into a computer within 6 minutes.

Automation
This Sub-Control is somewhat automatable and is worth the expense to properly configure it. Windows Defender may not be able to scan removable media every time a new one is inserted, as scans will need to be configured and performed manually on every usage.

Guidance and Tools
Windows Defender, a program built-into Windows, can perform a scan of removable media devices. This functionality is called a “custom scan” within the tool. Third-party tools can also be purchased to scan removable devices every time one is inserted in an automated manner. This Sub-Control should be implemented for of the systems within an enterprise.

Step-by-step instructions for implementing this Sub-Control can be found in:
Scanning Removable Devices.

CIS Control 8.5: Configure Devices to Not Auto-Run Content

Configure devices to not auto-run content from removable media

Category
Technical

Purpose
Removable media includes USB drives, memory cards, and external hard drives - just to name a few examples. These devices are commonly used to store photos, videos, and many types of enterprise data. Removable media is also one method used by attackers to install malicious software on computer systems. This attack method can be used to infect traditional enterprise workstations, but also computer systems viewed as secure since they lack a WiFi or Internet connection. Entirely banning the use of removable media is often impractical for businesses. If software on a USB device is allowed to automatically run, it may be able to install malware with limited to no user interaction.

Malware is software specifically designed to attack computer systems, devices, and data. Malware can enter an enterprise through any number of points such as email attachments, malicious apps, web pages, and USB drives. This Sub-Control was specifically included due to the emerging technique of dropping USB drives embedded with malware in parking lots or other areas where employees are likely to pick them up and plug them into enterprise systems. One academic study dropped 300 USB sticks around a school which resulted in ~50% of them being inserted into computers. Many were inserted into a computer within 6 minutes. https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots/

Automation
This Sub-Control is automatable natively in Windows 10 Pro. There is a setting within Windows 10 Pro that provides control on how content is run from removable devices. If a computer is joined to a domain, these policies can be deployed across all the computers in a network.

Guidance and Tools
Removable devices should not be trusted. How enterprise systems treat removable devices is controllable via the AutoPlay within the Windows 10 Pro Control Panel. Configuring the devices to *Ask Me Every Time* will give administrators the ability to make this decision before programs are run.

Step-by-step instructions for implementing this Sub-Control can be found in: Configuring AutoPlay on Windows 10 Pro.

CIS Control 9.4: Apply Host-Based Firewalls or Port-Filtering

Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Category
Technical

Purpose
Computers are already setup with a default set of networking features right out of the box. This is typically a permissive set of configurations that allows computer systems to connect to whatever resources average users need. Host-based firewalls help to manage these network configurations, block external unsolicited attempts to connect to a computer system, lessen the impact of malware, and log network traffic for future analysis. Indeed, it is easier to download malware onto an enterprise computer if there is no firewall in place. Malware installed on an enterprise system can pilfer or destroy sensitive enterprise data, perform a Denial of Service (DoS) on various systems, or look to infect other aspects of the network. By properly configuring the built-in firewall an enterprise can help to reduce the ways that a system can be attacked. Additionally, it can help to stop downloaded malware from communicating home and work to prevent its installation in the first place.

Automation
This Sub-Control is completely automatable within Windows 10 Pro.

Guidance and Tools
Properly enabling the firewalls built into operating systems goes a long way towards properly implementing this control. If a computer is joined to a domain, the built-in firewalls can be automatically configured across all the computers within an enterprise network. Windows 10 comes with a firewall that will help to implement this Sub-Control. Third-party solutions are also available that can accomplish the same tasks for Windows and also support other platforms.

- Windows Defender Firewall with Advanced Security: This built-in host-based firewall helps any Windows 10 Pro user meet this Sub-Control (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security).
- Check Point Zone Alarm: This is a popular free firewall that can be installed on enterprise computer systems (https://www.zonealarm.com/software/free-firewall).

CIS Benchmarks: CIS offers free configuration guidelines for common operating systems and their firewalls (https://www.cisecurity.org/cis-benchmarks).

Step-by-step instructions for implementing this Sub-Control can be found in:
Enabling Windows Defender Firewall.

CIS Control 10.1: Ensure Regular Automated Backups

Ensure that all system data is automatically backed up on a regular basis.

Category
Technical

Purpose
A backup is a duplicate of a computer system's data. If an attacker breaches a network or computer system, their first step will often be to change system configurations to ensure they have continued access in the future. In the process of doing so, attackers will sometimes make subtle alterations to data that can jeopardize an organization's effectiveness at a later date. Backups also help to protect against many types of malware, including newer variants such as ransomware and destructive malware, which may encrypt or simply delete an organization's data.

Backups also help to harden an organization against natural disasters like fire and floods. Additionally, over time, systems will fail and a plan needs to be in place to make sure that a business can recover from whatever incident occurs. Automated backups taken on a regular basis are a key component of an enterprise disaster recovery plan.

Automation
This Sub-Control is entirely automatable with very little effort on a Windows 10 system. Configuring this Sub-Control enterprise-wide across all systems can take a fair amount of IT knowledge to initially install. Backups are often setup by configuring an application to backup information to an external computer dedicated to backups, or to an external hard drive.

Guidance and Tools
Most operating systems come with built-in backup programs and utilities, which will need to be properly installed, setup, and configured. It is best practice to manually check enterprise backups from time to time to make sure that backup systems are working as intended, and can actually be utilized in case of a disaster. The following are examples of free backup utilities:

- Microsoft *Backup and Restore*: A backup utility tool installed on Microsoft operating systems (https://support.microsoft.com/en-us/help/17127/windows-back-up-restore).
- Amanda Network Backup: Free, open source backup tool (http://www.amanda.org).
- Bacula: Open source network backup and recovery solution (http://blog.bacula.org).

Step-by-step instructions for implementing this Sub-Control can be found in:
Configuring Microsoft Backup and Restore.

CIS Control 10.2: Perform Complete System Backups

Ensure that all the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

Category
Technical

Purpose
A backup is a duplicate of a computer system's data, but different types and degrees of backups exist. A backup is commonly viewed as a small collection of a system's overall data. Often only a few important folders are backed up, such as containing photos, receipts, contracts, or tax information. This information may be stored on another computer system, external hard drive, removable media, or cloud service. This strategy is insufficient for protecting an organization. Flavors of backups include incremental, differential, or complete. A complete system image is a snapshot of all data and settings on a system.

If a system is breached by an attacker, infected with malware, or involved in an accident (e.g., fire, flood), it often takes a long time to bring a system or network back online. This could include reinstalling and re-configuring all the enterprise systems and applications. Complete system backups rectify this issue by backing up not just important folders, but by backing up the entire computer, which can be pushed to new systems. Although this approach is a more complex solution, it makes recovery from a disaster or computer incident significantly faster. Backups protect against many types of malware including ransomware and destructive malware.

Automation
This Sub-Control is entirely automatable, although it requires a medium to advanced level of IT knowledge to initially setup and configure. It is often implemented by configuring a specific application to backup information to an external storage location with sufficient free space.

Guidance and Tools
It is best practice to manually check backups from time to time to make sure that any type of backups that an organization is relying upon is working as intended. Microsoft provides a system image creation and backup utility within Windows 10 Pro. There may be a need to obtain additional tools and services for backing up non-Windows systems. The following are examples of free backup utilities that can be used to take system images:

- EaseUS: This free program can be configured to take system images (https://www.easeus.com/backup-software/tb-free.html).
- Amanda Network Backup: Free, open source backup tool (http://www.amanda.org).
- Bacula: Open source network backup and recovery solution (http://blog.bacula.org).

Step-by-step instructions for implementing this Sub-Control can be found in:
Creating System Images with Windows 10 Pro.

CIS Control 10.4: Protect Backups

Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

Category
Technical, Procedural

Purpose
Backups can help an enterprise recover from a variety of disaster situations, whether the cause is malicious actors or accidents. Yet, backups can be physically and digitally targeted by attackers looking to hurt an enterprise. Backups that are connected to a network can be altered or deleted by malware, and physical backup drives can be stolen or suffer fires, floods, and other natural disasters. Backups need to be protected from these threats in order to be useful when the time comes. Digital mitigations include authenticating users before access and encrypting backups. Physical mitigations include keeping backup drives locked away from thieves, and outside of the same fire zone. This means that if a fire or flood were to strike an organization's physical location, the backups would not be affected. This is sometimes accomplished by using third-party backup services to store data offsite. These backups need to be protected as well.

There are two primary groups of threats to backups: digital and physical. Digital threats include local and remote attempts to access backups without being properly authenticated. Additional issues include altering or deleting backups. Physical threats include theft of physical backups or natural disasters (e.g., fires, floods).

Automation
This Sub-Control can be somewhat automated. Third-party services can use a virtual private network (VPN) when backing up enterprise information to an offsite server. Microsoft's BitLocker can encrypt any backups stored on a system. Physical protection of backups cannot be automated.

Guidance and Tools
Beware – encryption software can be dangerous if the password or encryption key is forgotten. If the password or key is lost, any enterprise data encrypted under that password or key will be unrecoverable.

- Veracrypt: This tool is an open source free utility that provides full disk encryption and can also encrypt removable drives, such as those used for backup (https://www.veracrypt.fr/en/How%20to%20Back%20Up%20Securely.html).
- EaseUS®: This free program can encrypt system images (https://www.easeus.com/backup-software/tb-free.html).

Step-by-step instructions for implementing this Sub-Control can be found in:
Configuring BitLocker for Windows 10.

CIS Control 10.5: Ensure All Backups Have at Least One Offline Backup Destination

Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

Category
Procedural, Technical

Purpose
Over the past few years a new type of malware has become popular that prevents enterprises from accessing their own data. This malware requires affected organizations to pay money in order to regain access to their data, whereas a related form of this malware may instead block access and never provide it ever again. Malware that requires money to obtain access once again is called *ransomware*. Ransomware uses cryptography to block access to a system's data via encryption. If the data is never provided back, it is considered *destructive malware*.

Besides user education and antivirus software, one of the best defenses against ransomware is backing up data to another system before there is a problem. But backups alone would not completely prevent this malware from accomplishing its goals. Typical backups may be connected to another system or network, meaning backup data can still be attacked. Therefore, regular backups should be stored in an unconnected, off-the-network, manner.

Keeping offline backups helps organizations recover and restore systems when ransomware or destructive malware hits a system. A common way for this malware to get into a network is to be installed via email attachments or downloads for websites. Both of these types of malware have impacted law enforcement, hospitals, governments, and academic institutions and cost millions of dollars to recover.

Automation
This is a very difficult Sub-Control to automate. Keeping offline backups means that once a backup is created, it needs to be manually removed from the network and stored elsewhere.

Guidance and Tools
The following documents can provide additional assistance in defending against ransomware:

- US-CERT: Ransomware - What It Is and What You Can Do About it (https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf).
- National Cyber Security Centre of the United Kingdom (UK): Mitigating Malware (https://www.ncsc.gov.uk/guidance/mitigating-malware).
- NIST National Cybersecurity Center of Excellence (NCCoE): Data Integrity (https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf).

CIS Control 11.4: Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Install the latest stable version of any security- related updates on all network devices.

Category
Technical

Purpose
Network devices include wireless routers, sometimes called wireless access points, and the networking appliance provided from an Internet service provider (ISP). An ISP is a telecommunications company that provides access to the Internet for companies and individuals. ISP provided appliances are confusingly referred to by multiple interchangeable terms such as *modem* or *cable box*. Some ISPs can provide a single network device that acts as modem, wireless access point, and firewall all in one. Regardless, all networking equipment needs to be regularly updated – even devices from the ISP. To update the software or firmware on any of these network appliances, it will often be necessary to access the device via an administrator account. This is commonly done via a web browser. The correct settings to update the system will be provided by the relevant ISP and/or network device manufacturer.

Older software on wireless access points and cable boxes or modems can lead to a malicious actor accessing sensitive enterprise information via the device. This can occur via vulnerabilities in protocols supported by the router or how users are authenticated to the router. If an attacker gains access to the device, they may be able to change network passwords, grant any computer access to the network, or potentially modify data in transit.

Automation
The degree of automatability available for this Sub-Control depends on the network appliances that are in use within an organization. Some network appliances can be set to auto-update all software and firmware. Others will not have this capability and will need to be manually updated on a regular basis.

Guidance and Tools
It is not possible to list all the models of network appliances provided by an ISP, but the following links are provided to show how to update the software and firmware on some of the most common network devices from United States ISPs.

- Comcast®: Comcast provides information on how to update their modem (https://www.xfinity.com/support/articles/using-your-own-modem-with-new-speeds).
- Verizon®: Verizon provides guidance for how to update their router (https://www.verizon.com/support/residential/internet/equipment/routers).
- AT&T®: AT&T customers can update their network devices via this guidance (https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1175558?gsi=Lb27wrtt).

CIS Control 12.1: Maintain an Inventory of Network Boundaries

Maintain an up-to-date inventory of all the organization's network boundaries.

Category
Technical

Purpose
Network boundaries define how data flows and traverses an enterprise network. Wired and wireless boundaries will exist, alongside logical boundaries. Logical boundaries sometimes include subnetworks (e.g., subnets), or virtual local area networks (vLANs). Generally, information cannot flow from one subnet to another without a networking device such as a firewall or router acting as a gatekeeper. This establishes trust boundaries between network segments. Therefore, a survey should be conducted to understand current trust boundaries in an enterprise network.

Understanding network boundaries can be challenging in a network that developed organically. The simplest example of a network boundary is the demarcation between a wireless and wired network. Another commonly seen example of a network boundary is the external network, and the internal *intranet* which generally is not accessible from outside of the trust boundary. Additionally, another important boundary to keep in mind is when a single organization has multiple physical locations. Often IT will work to logically connect all their physical locations together.

Specifically noting which networks are within a trust boundary, and then regularly checking them helps to prevent from accidentally trusting an untrustworthy device or network component. For instance, public users such as customers should not be granted access to the intranet, which often contains sensitive enterprise information.

Automation
This Sub-Control is generally not automatable. System owners and administrators will need to manually annotate and define network boundaries. This task needs to be performed on a fairly regular basis.

Guidance and Tools
Network scanning and monitoring tools can help test predefined network boundaries. Over time, internal networks can be misconfigured, and the networking tools can help to test of network segments are actually segmented.

- *Nmap*®: Famous multipurpose network scanner, used by system administrators and hackers across the world to identify which devices are connected to your network (https://nmap.org). This tool can identify network devices, ports, and simple configuration settings. Only scan networks you own, as doing otherwise is often impolite, and in many cases illegal.

- *ZenMap*: This tool builds on top of Nmap, and puts a graphic user interface on top of it to make the tool easier to use for those who do not feel comfortable using the command line (https://nmap.org/zenmap).

CIS Control 12.4: Deny Communication Over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary into, or out of, the network at each of the organization's network boundaries.

Category

Technical

Purpose

The overarching CIS Control 12 details precautions that should be taken for *boundary defense*, which is the notion of establishing and protecting a perimeter around an organization's externally facing networking equipment. Sub-Control 12.4 manages how communication is controlled on networking devices, such as firewalls. In order to accomplish this, the firewall configuration and ruleset in use should be carefully reviewed, monitored, and curated. If an enterprise-grade firewall is not in use, many of the dual-use modems/wireless access points from the ISP will often have a firewall built into the system which can be enabled.

A large majority of attacks launched against an organization will attempt to enter networks through a firewall. Firewalls often act the default entry point into a network and can deny communication over certain ports. Because of this they are under nearly constant attack and must be configured properly to protect the organization's assets sitting behind them. A firewall is typically envisioned to protect against basic attacks using a variety of protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Network Time Protocol (NTP).

Automation

Expensive enterprise tools can be purchased that require skilled technical staff to monitor and verify router configurations. This is generally not automatable for small- to medium-sized businesses.

Guidance and Tools

It is not possible to list all of the models of networking equipment. The following links are provided to show how to enable the built-in firewalls on some of the most common modems/wireless access points from United States Internet Service Providers (ISPs):

- Comcast: Comcast provides information on how to configure their modem (https://www.xfinity.com/support/articles/advanced-xfinity-wireless-gateway-features).
- Verizon: Verizon provides guidance for how to configure their router (https://www.verizon.com/support/residential/internet/security/home-network).
- AT&T: AT&T customers can configure their network devices via this guidance. (https://www.att.com/esupport/article.html#!/smb-internet/KM1188420?gsi=xDPL7tW0).

CIS Benchmarks: CIS offers in-depth guidance for many types of firewalls and other network appliances (https://www.cisecurity.org/cis-benchmarks).

CIS Control 13.1: Maintain an Inventory of Sensitive Information

Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.

Category
Procedural

Purpose
Sensitive data can be stored on smartphones, point of sale (POS) terminals, and backend systems. Enterprises should have a listing of their sensitive information, and which computer systems retain that data. Those that do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on internal networks can have a hard time preventing unauthorized access. If sensitive enterprise information is stored on an unknown or unprotected system, the information is more likely to be accessed in an unauthorized manner. Any listing of sensitive information in formation should also be properly labeled. If sensitive enterprise information is not labeled correctly, then it may be accidentally distributed to unauthorized outside parties.

Automation
This Sub-Control is generally not automatable. It is most often necessary to manually identify and list sensitive files and other applicable information through usage of lists and labels within files or documents.

Guidance and Tools
Sensitive information can be tracked in a spreadsheet in a similar manner to hardware and software assets. CIS offers a free spreadsheet to track sensitive information within the enterprise contained within the Appendix of this document. The definitions of, and policies surrounding the usage of labels for data classification should be understood by all employees handling sensitive information. This in turn means that all sensitive, confidential, or proprietary information should be clearly labeled for internal use. Ultimately, what constitutes sensitive information is defined by local laws and the needs of an enterprise. Examples of sensitive information include:

- Personally Identifiable Information (PII);
- Trade secrets or proprietary information;
- Financial information (e.g., taxes, debit card numbers);
- Cryptographic keys;
- Passwords; and
- Biometric data.

CIS Control 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Category
Technical

Purpose
A breach of sensitive enterprise data and systems can cost time, money, and bring an organization out of compliance with local laws governing sensitive information. Sensitive data and computer systems infrequently accessed may not receive the regular maintenance and attention necessary to properly manage them. Therefore, systems that are infrequently used should be removed from service across the entire enterprise network. This helps to reduce enterprise attack surface leaving fewer systems that can be targeted. Older and infrequently used systems may fall into disrepair. These systems are not likely to receive regular software updates, which means the operating system and applications will likely contain vulnerabilities that can be exploited to access the system and any data.

Automation
There is no way to automate the implementation of this Sub-Control. Individuals will be needed to manually label sensitive data, and identify which systems store that sensitive data. Putting this Sub-Control into place will often require a hardware asset inventory as detailed in Sub-Control 1.4, alongside a sensitive information inventory as detailed in Sub-Control 13.1.

Guidance and Tools
Systems that are irregularly accessed and maintained should not be network connected while hosting sensitive enterprise information. If the systems are necessary to ensuring the goals of the organization, consider attempting to use them in a non-networked fashion or virtualizing the system.

CIS Control 13.6: Encrypt Mobile Device Data

Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

Category
Technical

Purpose
Smartphones and tablets used by employees for work activities contain a treasure trove of sensitive enterprise data. This includes both personal devices and those provided by the company. This is true for upper management, rank and file, and all employees in between. It is commonplace for employees to use a phone to obtain company email. Therefore, an organization's sensitive email, with proprietary secrets, financials, and more, is stored on a device that an employee could easily misplace or have stolen. One of the best ways to help protect against these failures is to encrypt a company's information while on the device.

Automation
This Sub-Control is automatable if the correct combination of hardware, software, and policy is purchased. The correct software to obtain will depend on the way that enterprise devices are provided to employees such as with Bring Your Own Device (BYOD) scenarios. Enterprise mobility management (EMM) systems can force all of the smartphones or tablets accessing company email to encrypt mobile data. This Sub-Control can also be solved in a manual fashion with the correct configuration options without much effort.

Guidance and Tools
Mobile data is often secured by default on mobile devices, but this is not always the case. For each phone accessing enterprise email, the appropriate encryption setting must be selected. This will look different on each type of phone, so it may be difficult to identify step-by-step instructions. A vast majority of users will have phones from Samsung®, Google®, or Apple®, therefore identifying and learning how to encrypt data on each of these platforms will often be sufficient. For additional information on how to secure mobile devices, reference the CIS Mobile Companion Guide. It was created with many of the industry's leading experts and provides created detailed guidance for how to secure mobile devices.

CIS Benchmarks: CIS provides detailed instructions for how to secure Google's Android® and Apple's iOS mobile platforms. Instructions for encrypting the device can be found within these two documents (https://www.cisecurity.org/benchmark/google_android). (https://www.cisecurity.org/benchmark/apple_ios).

CIS Control 14.6: Protect Information Through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

Category
Technical

Purpose
Different types of employees will need varying levels of access within an enterprise. Users with more sensitive roles and job responsibilities may need additional access, such as Human Resources and Finances, whereas users with more simple workplace needs will necessitate fewer permissions. This means that access to data, systems, and files should be provided according to business needs. Administrative or super user access should not be provided to all employees.

Users with large amount of system access can easily make accidental changes that affect multiple users and systems. Sometimes these changes will not be easily recoverable, like deleting an entire network drive. Another scenario worth considering is if a user with broad privileges has their accounts compromised, the attacker would be able to access everything that user is able to access.

Automation
User access can be accomplished through Windows Active Directory Group Policy. This functionality can also be controlled through Windows Intune. Not all systems will be domain joined – for instance firewalls will also need access control decisions made and enforced. Ultimately access control decisions will need to be made by a human.

Guidance and Tools
Correctly configuring access control on a computer system can be a complex task.

- Qualys Browser Check: A tool to check if a browser is up-to-date with all its patches (https://browsercheck.qualys.com).
- OpenVAS: A tool to scan systems to check security baselines (www.openvas.org).

CIS Benchmarks: CIS offers free PDFs with configuration guidelines for 140+ technologies, which can be used to correctly configure users, applications, and other access control lists (https://www.cisecurity.org/cis-benchmarks).

CIS Control 15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

Category

Technical

Purpose

The Advanced Encryption Standard, or AES, is an algorithm used encrypt information standardized by the United States Government in 2001. It is considered a modern, strong cipher that has withstood attempts to break it for years. This purpose of this Sub-Control is to make sure that an organization's wireless traffic is strongly encrypted. AES is built into most wireless access points, or wireless routers, that can be bought at major electronics stores. AES is utilized with Wireless Protected Access version 2, or *WPA2*. Using Wireless Equivalent Privacy (WEP) or Wireless Protected Access (WPA) version 1 does not meet this Sub-Control, as AES will not be the algorithm used to encryption wireless information. Both WEP and WPA also have other significant flaws and should not be used. It is easier for an attacker to sniff wireless communications than wired communications, and by properly setting up AES, anyone on the wireless network will not be able to understand the transmitted network traffic.

Automation

This Sub-Control is entirely automatable for many types of wireless traffic, including WiFi. Simply selecting the proper configuration settings on a wireless access point will make sure AES is being used for all devices that connect to the network.

Guidance and Tools

AES should be enabled for all wireless networks within an enterprise. This includes 2.4 Gigahertz (GHz) and 5 GHz, as these are two completely separate wireless networks that must be properly configured. It's not possible to list all of the models of wireless routers, but the following links are provided to show how to enable encryption on some of the most common wireless access points from United States ISPs.

- Comcast: Comcast provides information on how to configure their modem (https://www.xfinity.com/support/articles/change-wifi-security-mode).
- Verizon: Verizon provides guidance for how to configure their router (http://www.verizon.com/support/smallbusiness/internet/fiosinternet/networking/setup/zyxeladapters/128755.htm).
- AT&T: AT&T customers can configure their network devices via this guidance (https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1049997?gsi=1ysnu3).

Step-by-step instructions for implementing this Sub-Control can be found in: Identifying if a Wi-Fi Connection is Using AES.

CIS Control 15.10: Create Separate Wireless Network for Personal and Untrusted Devices

Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

Category
Procedural

Purpose
Some computers, tablets and smartphones are more trustworthy than others. If a device is bought, configured, and safely used by an employee or enterprise, it is likely more trustworthy than a completely unknown device that an enterprise has never seen before. This level of trust can be extended past enterprise devices and into a company's networks. Devices that are trusted and used only for company tasks should be kept on a completely separate network from personal devices owned by employees or guests. This will keep devices that are misconfigured, infected with malware, or insecurely built from being used to infect a network and its systems. These devices may already harbor malware that could steal sensitive enterprise data or attack other computers and devices on a network. One infected device can place every device within the network in danger.

Automation
Making a clearly identified guest network available for personal and guest devices helps employees and guests know which networks are for enterprise use and which are not. There is no easy way to automate this Sub-Control. Separate networks will need to be created and properly configured at each wireless access point. Many popular wireless access points come with the ability to broadcast a guest network built right in.

Guidance and Tools
The following resources show how to create guest networks on some of the most common wireless access points from United States ISPs.

- Verizon: Verizon provides guidance on separating networks (https://www.verizon.com/cs/groups/public/documents/adacct/guest-wifisetupguide-smb.pdf).
- Comcast: Comcast provides guidance on utilizing guest networks (https://www.xfinity.com/support/internet/help-guests-get-online/).

CIS Control 16.8: Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

Category
Technical

Purpose
Extraneous accounts can be used to attack the system they are associated with, but also to compromise other nodes on a network. These accounts can be created on accident, for testing purposes, or be leftover accounts from contractors or employees no longer employed at an organization. Attackers often find and exploit legitimate, but inactive user accounts, and use them to impersonate legitimate users. When this occurs, it makes tracking the activities of attacker behavior quite difficult for those responding to a breach or performing forensic analysis. This Sub-Control states the need for disabling unassociated accounts but not deleting them. Deletion is not recommended as this will not preserve the audit trail and hamper any future computer incident investigations.

Unassociated accounts are often known as “stale” or “ghost” accounts on a system, and are a weak link for attackers. Accounts that have not been used by an employee are valuable accounts for an attacker to overtake. This is due in large part since the original account owners are not actively using the account, so it is difficult for an enterprise to notice if the account is being used maliciously.

Automation
This Sub-Control is not entirely automatable. Products and scripts can be written to highlight suspect accounts, but the ultimate decision on whether accounts should be disabled may need to be made by a human.

Guidance and Tools
Regardless of the edition of Windows 10 that is in use, all local and remote accounts on enterprise computer systems should be regularly checked and audited. This also extends to smartphones, network appliances, and any system that enterprise utilize accounts for user access.

Step-by-step instructions for implementing this Sub-Control can be found in:
Viewing Accounts on a Windows 10 System.

CIS Control 16.9: Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity.

Category
Technical, Procedural

Purpose
System and user accounts establish identity and access on information systems. Operating system privileges and granular file permissions can be assigned to individual users and groups of users (i.e., roles). When an organization is using Active Directory and domain controllers, each employee is generally assigned an account and assigned roles for what they are allowed to do within an organization's entire network architecture. Local accounts unique to a system are often also utilized. When employees leave an organization, or even change organizational units, their privileges are removed. Yet it is possible to go a step further and automatically disable accounts after a predetermined period of time. Deleting accounts is not always recommended as this may disturb user, system, or application logs, or other information that may be needed to audit user activity in case an incident is discovered in the future.

Dormant accounts are often known as "stale" or "ghost" accounts on a system, and are a weak link for attackers. Accounts that have not been used by an employee are valuable accounts for an attacker to overtake. This is due in large part since the original account owners are not actively using the account, so it is difficult for an enterprise to notice if the account is being used maliciously.

Automation
Products and scripts can be written to highlight suspect accounts, but the ultimate decision on the length of time before an account should be disabled will need to be made by a human.

Guidance and Tools
There is no standard for the time interval before inactive accounts should be disabled. The length of time is sometimes 15 – 30 days, whereas others recommend 90 days. Enterprises requiring a higher level of security should utilize shorter timeframes.

Step-by-step instructions for implementing this Sub-Control can be found in:
Viewing Accounts on a Windows 10 System.

CIS Control 16.11: Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

Category
Technical

Purpose
Using a password to regularly log into a computer can cause trouble for a user, especially if a computer quickly locks. Yet too often computers are left unattended without being locked. Unlocked computers allow anyone to access the information and applications open on a system. A point of sale (POS) system, tax information, and even an employee's personal information will be available to anyone who walks up to an unattended enterprise workstation. This Sub-Control applies to more than just a computer system since smartphones and tablets can also be left unlocked.

This Sub-Control is important because it protects from very basic, low-effort, and easy to do attacks. People with very little technical skill can walk up to a computer and access a company's information if there is no lock on the system. If someone with technical knowledge accessed a system without a lock screen, depending on how the computer is setup, they can install malware and potentially access passwords used by employees. In a worst-case scenario, they can potentially bring enterprise computer systems and networks down if passwords are reused, or if the computer they are on is setup to manage other devices.

Automation
This type of policy can be controlled and monitored automatically if you have your systems joined to a domain. This is a fairly basic configuration setting that can be completely accomplished automatically.

Guidance and Tools
There is no universally agreed upon time frame for how quickly a computer should lock. Locking after one or two minutes of inactivity may be too quick, and cause frustration while trying to read emails, articles, and spreadsheets. Many organizations recommend 5 minutes as a balance between security and usability. With that said, the following should be kept in mind:

- All computers, phones, and tablets should have their settings changed to lock after a predetermined time. Although you may not be able to enforce it, at least asking employees who use their phones to access work emails to put a password or lock on their personal phones and tablets.
- Employees should be regularly reminded of the dangers of leaving their computer systems unlocked.

Step-by-step instructions for implementing this Sub-Control can be found in:
Locking a Workstation via Windows Settings.

CIS Control 17.3: Implement a Security Awareness Program

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

Category
Procedural

Purpose
Employees are the first line of defense in any good security program. In some sense, the phrase "you are only as strong as your weakest link" is very true in security. Sometimes all it takes is one employee to unknowingly install a malicious program on their computer to lead to a security breach. This is why it is important that all employees know practice a basic awareness of how to keep themselves and the company secure. This starts with a security awareness program.

Many of the top security threats taking advantage of the human factor of security. These include social engineering type attacks such as phishing, spear phishing, vishing, pretexting, baiting, and others. Many threats take advantage of human tendency or emotion. They look to trick employees who are not paying attention to detail or who get caught believing an emotional story.

Automation
There are third-party training platforms available which can reduce the overhead of implementing a security awareness program. Third-party training platforms are engaging and up-to-date but may be too costly for small organizations.

Guidance and Tools
A good security awareness program is more than just an onboarding program or annual training. The U.S. Department of Health and Human Services (HHS) provides material for cybersecurity awareness training. The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) has a monthly security newsletter that people can subscribe for a free monthly newsletter targeted at end users (https://learn.cisecurity.org/ms-isac-subscription). Here are some key components of a good security awareness program:

- Acceptable use policy: This policy should be in place to lay out the expectations an organization has around its security. This should explain to the employee that they have responsibilities for security in their everyday work.
- New employee onboarding training: New employees need to know organizational expectations for security. This training can be formal training provided by third-parties, or may be informal training provided by their supervisor.
- Management awareness: Employees need to hear and feel that management takes security seriously and is counting on them to do their part. This can be accomplished by dedicating a moment to security in corporate wide meetings or announcements.
- Posters and spotlights: Hanging security awareness posted, like those from SANS (https://www.sans.org/security-resources/posters), or sending out Security Spotlight emails on a regular basis are a good way to continually emphasis security to employees.

- Annual refresher training: Employees should be asked to go through a security awareness refresher once a year.

CIS Control 17.5: Train Workforce on Secure Authentication

Train workforce members on the importance of enabling and utilizing secure authentication.

Category
Procedural

Purpose
Especially with the move to a cloud-first and mobile-first world, employees now more than ever need to be trained to properly manage their user accounts. In many cases, their user account is the only line of defense to prevent an attacker from infiltrating an organization's enterprise infrastructure. Employee user account security is important even if an enterprise company has a local network. Storing passwords on sticky notes, sharing password with co-workers, or using the same password for all accounts are all examples of poor practices which can be exploited by attackers leading to significant harm for a company.

Account takeovers are a common approach for attackers to gain a foothold within an organization and begin taking data or control. With access to a legitimate account, attackers will often attempt to move horizontally to take over other accounts, launch phishing campaigns which appear legitimate, and look to obtain sensitive. Additionally, it can be very difficult to detect and track an attacker who has taken over a legitimate account. Finally, users may share personal passwords with enterprise accounts. Personal accounts may be a victim of a breach, and the username and password for the enterprise account is no always changed.

Automation
There are third-party training platforms available which can provide up-to-date information on secure workforce authentication, but these may be too costly for small organizations. Many platforms and services provide the ability to setup two factor authentication (2FA).

Guidance and Tools
Employees should be trained on how to setup user accounts and keep them secure. This training should be provided upon hire and should be included in the annual security awareness training. It is critical that a company also establish that each employee has a unique account for themselves. To the extent possible, do not permit shared accounts. Although shared accounts may be advantageous for licensing and other purposes, they are less than ideal security conditions. The Electronic Frontier Foundation provides a useful poster on secure authentication.

Here are a few keys points all employees should know about their accounts:

- Use strong, unique passwords: Create passwords which are 14 characters or more.
- Setup 2FA on all possible accounts: This adds an additional and critical step to a website's login process. 2FA uses a smartphone or hardware device to identify someone to a website. Visit twofactorauth.org for instructions on setting up 2FA on popular websites.
- Do not share passwords: It is not possible to track who performed what action when multiple users have the same password.

- Do not use the same password for all accounts: The best practice is to use unique passwords for every account. At a minimum, do not use passwords used for personal use for business use.
- Do not use any personally identifiable information in your passwords: Names, birthdays, and street addresses may be easy to remember but they are also easily found online and should always be avoided in passwords to ensure the greatest strength.
- Avoid using similar passwords that change only a single word or character: This practice weakens account security across multiple sites.

CIS Control 17.6: Train Workforce on Identifying Social Engineering Attacks

Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.

Category
Procedural

Purpose
Social engineering attacks are one of the more common and successful types of attacks. This is because they prey upon human tendencies and emotions. Even if not always successful, any successfully social engineering attack can have a tremendous impact on an organization. While these types of attacks are often preventable, they are getting more and more sophisticated and harder to spot. This is why is important for employees to know what to look for and how to spot suspicious activity in their email, over the phone, and even in person.

Social engineering attacks include phishing, spear phishing, vishing, pretexting, baiting, tailgating, and quid pro quo. Phishing is the most common type of social engineering attack, and occurs when an attacker is able to get a victim to perform some action such as disclosing sensitive information like an enterprise password. Another form of phishing will trick the user to navigating to a website that downloads malicious software and subsequently installs it on an enterprise system.

Automation
There are third-party training platforms available which can reduce the overhead of implementing a security awareness program for identifying social engineering attempts. Third-party training platforms are engaging and up to date but may be too costly for small organizations.

Guidance and Tools
Social engineering attacks are best defeated by an aware and skeptical employee base. Employees need to be aware of their tendencies and maintain a healthy skepticism of anyone or any communication which is not from a trusted, known party. Holding regular social engineering awareness trainings along with regular corporate communications which show examples of social engineering attacks are good exercises. Conducting role-playing training for employees to be exposed to this type of tactic will help employees respond appropriately in real world scenarios.

- Google: This high-quality video can be used to train employees on how to Stay Safe from Phishing and Scams.
- NIST: This high-quality video can be used to train employees on how to identify social engineering attack titled You've been Phished.
- Much of the guidance provides in 17.5 can be useful for this Sub-Control.

CIS Control 17.7: Train Workforce on Sensitive Data Handling

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.

Category
Procedural

Purpose
The act of labeling data according to its sensitivity is a type of data classification. It often involves placing a “PROPRIETARY”, “SENSITIVIE”, OR “CONFIDENTIAL” mark on a document. These markings allow organizations to more easily make the appropriate security decisions to govern their own data. This often involves allocating additional resources and developing policies to protect sensitive company information. For instance, placing trade secrets on a cloud platform may not be wise if their secrecy is pivotal to the business continuing normal operation. If an organization does not perform data classification, it is more likely that unintentional data loss may occur. Therefore, clearly labeling data prevents intentional and unintentional data breaches.

Automation
This Sub-Control is generally not automatable. Third-party organizations offer platforms that can help to train users in the proper way to handle sensitive information.

Guidance and Tools
Proper sensitive data handling begins with having a sensitive data policy. This policy should detail what information is considered sensitive, how employees should identify it, and how to handle the data. One this policy is in place; it is important that employee be trained on how to follow the policy and be reminded of the importance of seeking approval for any exceptions. Be sure to include the follow in the policy and subsequent training:

- How to identify sensitive information.
- How to transmit sensitive information within the organization.
- When it is appropriate and how to transmit sensitive information outside the organization.
- How to direct outside organizations to transmit sensitive data to you.
- Where to digitally store sensitive information.
- What to do if you find sensitive information in an unauthorized location.
- When it is appropriate to print sensitive information, how to store printed copies, and how to dispose of it.
- How long to retain sensitive information and how to securely dispose of it.
- How to seek exceptions to sensitive data policy.

Step-by-step instructions for implementing this Sub-Control can be found in:
Sensitive Information Tracking.

CIS Control 17.8: Train Workforce on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

Category
Procedural

Purpose
People play a huge role in preventing data breaches, often more critical than any technological solution. Employees must be regularly exposed to, and reminded of, causes of data exposure and data breaches. The following is a non-exhaustive list:

- Loss of device with sensitive information;
- Leaving sensitive information in an insecure area;
- Downloading sensitive information to temporary or download folders which are not secure;
- Sending sensitive information over insecure communication channels (e.g., unencrypted email, text messages);
- Sending sensitive information to the wrong recipient;
- Insufficiently reviewing newly created data for its proper sensitivity level;
- Assigning permissions to sensitive information to the wrong person;
- Improperly segmenting data based on need to know; and,
- Improperly setting access controls on sensitive data.

Automation
This Sub-Control is generally not automatable. Network appliances can be put into place such as a firewall, data loss prevention, intrusion detection system, or an endpoint protection suite (e.g., antivirus), to prevent data exposure. Third-party organizations offer platforms that can help to train users to recognize the symptoms of accidental and unintentional ways to affect the security of an organization.

Guidance and Tools
It is important regularly training workforce members, but not overwhelm them. Do not expect them to be cybersecurity experts. The key is identifying key events and continuing to remind them to report any and all suspicious happenings, even if they are unsure. By regularly reminding employees of accidental causes of data breaches, they will be more mindful and can understand the risks associated with their actions.

CIS Control 17.9: Train Workforce Members on Identifying and Reporting Incidents

Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.

Category
Procedural

Purpose
As with most incidents, the earlier a security incident is identified and a response is initiated, the less severe the incident will likely become. It is also true that earlier detection often leads to more information being available about the incident. This information may be key to stopping an ongoing attack and to understanding certain details such as how the attack was conducted and what impact it caused. One of the key details required in many states laws is information on how the breach occurred, how many people were impacted, and what was done to remedy the attack. Reducing the impact and understanding the details of the breach are both much more achievable with earlier detection and response. Employees are key to this early detection. Employees should be trained on the types of things to look for and how to report suspicious behavior or events.

Automation
This Sub-Control is generally not automatable. Network appliances can be put into place such as a firewall, intrusion detection and prevention system, or an endpoint protection suite (e.g., antivirus) to stop incidents from occurring in the first place. Third-party organizations offer platforms that can help to train users to recognize the symptoms of an incident.

Guidance and Tools
It is important not to overwhelm workforce members or expect them to be security experts. It is unreasonable to expect non-IT staff to become cybersecurity experts; however, it is important they report suspicious happenings and occurrences. The key is identifying key events and continuing to remind them to report these if seen. Here is a non-exhaustive list of some events to train employees to report:

- Emails asking for sensitive information that are out of context or from unknown senders.
- Emails from an unknown sender who is asking the person to click a link.
- Phone calls from unknown, unverifiable source asking for sensitive information or to make changes to their account.
- Unknown people in areas of the office designated for employees only.
- Sensitive data is observed in a non-secure physical or digital location.
- Removable media that is not labeled and not claimed by an employee.
- Evidence of unknown programs running on their computer, such as a Windows User Account Control (UAC) prompt for an unrecognizable program.

CIS Control 19.1: Document Incident Response Procedures

Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.

Category
Procedural

Purpose
If an organization continuously operates for a long enough period of time, it is likely that they will suffer a cyber breach. Even if a breach never occurs, it is best to plan for the possibility, even if just from a legal liability standpoint. When a data breach occurs, it can feel like multiple extremely important events are all taking place at the same time. Important processes, procedures, and security critical tasks can be forgotten during this time frame. That is in part why a series of written procedure for how to handle a cyber incident before it occurs is needed.

The threats surrounding this Sub-Control mostly revolve around the inappropriate handling of a cyber incident while it is active. This means accidents from internal employees tasked with responding to the breach. This is especially true if the breach is the first one an organization has experienced. Improper data breach handling can lead to the breach getting worse, for instance malware getting deeper into a network and having additional access to sensitive data.

Automation
There is no way to automate this this Sub-Control. Yet this does not mean that an incident response plan and associated response procedures must be made from scratch. Incident response procedures can be procured from other similar organizations that already have them in place. These procedures can be modified to fit most organizations' needs.

Guidance and Tools
Many organizations offer useful incident response guidance.

- Open Trust Alliance: This guidance contains checklists of considerations for developing a response plan and provides templates that can be incorporated (https://otalliance.org/system/files/files/initiative/documents/2017_cyber_incident_breach_response_guide.pdf).
- Carnegie Mellon: The university makes their Incident Response Plan available, can be used as a resource for others (https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf).
- State of Oregon: The Oregon State Government provides a template for an Incident Response plan (https://www.oregon.gov/das/oscio/documents/incidentresponseplantemplate.pdf).

CIS Control 19.3: Designate Management Personnel to Support Incident Handling

Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

Category
Procedural

Purpose
During an incident, many important decisions will need to be made in a short timeframe. For this reason, it is necessary for management personnel with the authority to make those decisions to be involved in the incident handling process. Designated management personnel should have a clear understanding of their role in the process ahead of time, before incidents occur. Backup personnel should also be designated in case the corresponding primary personnel are unavailable when an incident arises.

Automation
There is no way to automate this this Sub-Control. Yet this does not mean that an incident response plan and associated response procedures must be made from scratch. It is possible to obtain incident response procedures from other similar organizations that already have them in place. These procedures likely nominate management and technical roles for certain response positions, and these can be can be modified to fit an organization's needs.

Guidance and Tools
Many organizations offer useful incident response guidance.

- Open Trust Alliance: This guidance contains checklists of considerations for developing a response plan and provides templates that can be incorporated (https://otalliance.org/system/files/files/initiative/documents/2017_cyber_incident_breach_response_guide.pdf).
- Carnegie Mellon: The university makes their Incident Response Plan available, can be used as a resource for others (https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf).
- State of Oregon: The Oregon State Government provides a template for an Incident Response plan (https://www.oregon.gov/das/oscio/documents/incidentresponseplantemplate.pdf).

CIS Control 19.5: Maintain Contact Information for Reporting Security Incidents

Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.

Category

Procedural

Purpose

Incidents often necessitate the involvement or notification of multiple third-party organizations. Depending on the nature of the incident, it may be necessary to contact law enforcement, other government agencies, vendors and business partners, or Information Sharing and Analysis Center (ISAC) partners. It is best to have the contact information for these organizations consolidated, up-to-date, and easily accessible, as it may be difficult and time-consuming to try to look up all of this information while an incident is taking place. Keep in mind that some cyber incidents may result in limited access to networks and files during incident response, so having this information available in varied locations or formats (including a hardcopy) can also be helpful.

Automation

There is no way to automate this this Sub-Control. Yet this does not mean that an incident response plan and associated response procedures must be made from scratch. It is possible to obtain incident response procedures from other similar organizations that already have them in place. These procedures likely nominate management and technical roles for certain response positions, and these can be modified to fit an organization's needs.

Guidance and Tools

Many organizations offer useful incident response guidance.

- Open Trust Alliance: This guidance contains checklists of considerations for developing a response plan and provides templates that can be incorporated (https://otalliance.org/system/files/files/initiative/documents/2017_cyber_incident_breach_response_guide.pdf).
- Carnegie Mellon: The university makes their Incident Response Plan available, can be used as a resource for others (https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf).
- State of Oregon: The Oregon State Government provides a template for an Incident Response plan (https://www.oregon.gov/das/oscio/documents/incidentresponseplantemplate.pdf).

CIS Control 19.6: Publish Information Regarding Reporting Computer Anomalies and Incidents

Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.

Category
Procedural

Purpose
The types of computer incidents regularly affecting a company can be useful when devising training activities. Each incident is an opportunity for learning, and then using those lessons to improve the process that is already in place. Besides feeding back into computer incident response activities, this information can also be communicated to contractors and employees of an organization as part of the regular user education process for cybersecurity. Understanding the general threats a company faces can help employees to make better decisions the next time around, responding more appropriately, and ultimately mitigating the impact of an incident.

Publishing information about previous computer incidents helps personnel prevent improper handling of an incident. Improper incident handling can lead to malware accessing your sensitive enterprise data for longer periods of time as it may not be properly removed. Another issue of significance is that improper incident handling may violate local and federal laws about the privacy of data and breach notifications.

Automation
This Sub-Control generally cannot be automated. Yet this does not mean that an incident response plan and associated response procedures must be made from scratch. You can obtain incident response procedures can be procured from other similar organizations that already have them in place. These procedures can be modified to fit your needs.

Guidance and Tools
The following can be useful when looking to report computer anomalies and incidents:

- NIST: The Computer Security Incident Handling Guide from NIST provides detailed information for how to handle a computer incident (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf).
- US Department of Justice: The US DoJ provides guidance on how to report a cybersecurity incident (https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf).

Acronyms and Abbreviations

2FA	Two Factor Authentication
AES	Advanced Encryption Standard
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COTS	Commercial Off the Shelf
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DoJ	Department of Justice
EMM	Enterprise Mobility Management
FIOS	Fiber Optic Service
FTP	File Transfer Protocol
GHz	Gigahertz
HHS	Health and Human Services
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IG	Implementation Group
IP	Internet Protocol
ISP	Internet Service Provider
ISAC	Information Sharing and Analysis Center
IT	Information Technology
LGPE	Local Group Policy Editor
MAC	Media Access Control
NIST	National Institute of Standards and Technology

NTP	Network Time Protocol
O365	Microsoft Office 365
OS	Operating System
PAN	Personal Area Network
PDF	Portable Document Format
PII	Personally Identifiable Information
RAM	Risk Assessment Method
SIEM	Security Information and Event Management
SME	Small- and Medium Enterprises
SP	Special Publication
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
vLAN	Virtual Local Area Network
VPN	Virtual Private Networking
WEP	Wireless Equivalent Policy
WiFi	Wireless Fidelity
WPA	Wireless Protection Access
WPA2	Wireless Protection Access Version 2
WPAN	Wireless Personal Area Network

Links and Resources

- CIS Controls: https://www.cisecurity.org/controls/
- SANS Institute: https://www.sans.org/findtraining/
- Microsoft Windows 10 Versions: https://www.microsoft.com/en-us/windows/compare
- Daniel Miessler Blog: https://danielmiessler.com/blog/continuous-asset-management-security
- Nmap: https://nmap.org
- Spiceworks: https://www.spiceworks.com
- Zenmap: https://nmap.org/zenmap
- Netwrix: https://www.netwrix.com
- Open Audit: http://www.open-audit.org
- 10apps Manager: https://www.thewindowsclub.com/10appsmanager-windows-10
- Itarian: https://us.itarian.com/patch-management/free-windows-patch-management-software.php
- Opsi: https://www.opsi.org
- CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks
- PDQ: https://www.pdq.com
- Automatic Updates for Windows 10: https://support.microsoft.com/en-us/help/15081/windows-turn-on-automatic-app-updates
- Keepass: https://keepass.info
- Lasspass: https://www.lastpass.com/password-manager
- OpenVAS: www.openvas.org
- DISA STIGs: https://iase.disa.mil/stigs/Pages/index.aspx
- US CERT – Securing Your Web Browser: https://www.us-cert.gov/publications/securing-your-web-browser
- OpenDNS: https://support.opendns.com/hc/en-us/articles/228007207-Windows-10-Configuration
- Quad9: https://www.quad9.net/microsoft
- Windows Defender Security Center: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-security-center/windows-defender-security-center
- Elie Bursztein: https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots
- Microsoft Windows Firewall: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security
- ZoneAlarm: https://www.zonealarm.com/software/free-firewall
- Microsoft Windows Backup and Restore: https://support.microsoft.com/en-us/help/17127/windows-back-up-restore
- Amanda: http://www.amanda.org
- Bacula: http://blog.bacula.org
- Easeus: https://www.easeus.com/backup-software/tb-free.html
- Veracrypt: https://www.veracrypt.fr/en/How%20to%20Back%20Up%20Securely.html

- US CERT Ransomware Notice: https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
- NCSC Mitigating Malware: https://www.ncsc.gov.uk/guidance/mitigating-malware
- NIST SP 1800-11: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf
- Xfinity Using Your Own Modem: https://www.xfinity.com/support/articles/using-your-own-modem-with-new-speeds
- Verizon Routers: https://www.verizon.com/support/residential/internet/equipment/routers
- AT&T U Verse Setup: https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1175558?gsi=Lb27wrtt
- Xfinity Wireless Gateway Features: https://www.xfinity.com/support/articles/advanced-xfinity-wireless-gateway-features
- Verizon Home Network Security: https://www.verizon.com/support/residential/internet/security/home-network
- AT&T SMB Support: https://www.att.com/esupport/article.html#!/smb-internet/KM1188420?gsi=xDPL7tW0
- CIS Mobile Companion Guide: https://www.cisecurity.org/white-papers/cis-controls-mobile-companion-guide-2/
- CIS Google Android Benchmark: https://www.cisecurity.org/benchmark/google_android
- CIS Apple iOS Benchmark: https://www.cisecurity.org/benchmark/apple_ios
- Qualys Browsercheck : https://browsercheck.qualys.com
- Xfinity Change WiFi Security Mode: https://www.xfinity.com/support/articles/change-wifi-security-mode
- Verizon Network Setup: http://www.verizon.com/support/smallbusiness/internet/fiosinternet/networking/setup/zyxeladapters/128755.htm
- AT&T U Verse Setup: https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1049997?gsi=1ysnu3
- Verizon Guest WiFi Setup: https://www.verizon.com/cs/groups/public/documents/adacct/guest-wifisetupguide-smb.pdf
- Xfinity Help Guests Get Online: https://www.xfinity.com/support/internet/help-guests-get-online/
- HHS Security Awareness Training: https://www.hhs.gov/sites/default/files/fy18-cybersecurityawarenesstraining.pdf
- MSISAC Subscription: https://learn.cisecurity.org/ms-isac-subscription
- Two Factor Auth: http://twofactorauth.org/
- Google Stay Safe from Phishing Scams: https://www.youtube.com/watch?v=R12_y2BhKbE
- NIST You've Been Phished: https://www.nist.gov/video/youve-been-phished
- OTA Alliance Cyber Incident Breach Response Guide: https://otalliance.org/system/files/files/initiative/documents/2017_cyber_incident_breach_response_guide.pdf
- CMU Incident Response Plan: https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf
- Oregon Incident Response Plan: https://www.oregon.gov/das/oscio/documents/incidentresponseplantemplate.pdf

- DoJ Best Practices Victim Response and Reporting Cyber Incidents: https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf
- NIST SP 800-61: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

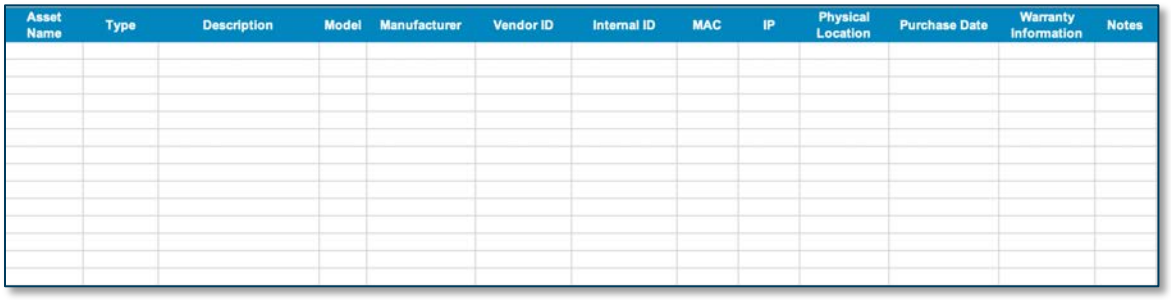
Appendix A: Example Asset and Information Tracking Spreadsheets

Sample Hardware Asset Tracking Spreadsheet

Elements of a *Hardware Asset Tracking Spreadsheet* can include the following:

- Asset Name: Common name of the asset,
- Type: The type of the asset (e.g., workstation, firewall, router),
- Description: A description of the asset and what it's used for,
- Model: The model of the asset,
- Manufacturer: The organization that created the asset,
- Internal ID: Any identifier used internally to name a manufacturer,
- MAC: The MAC address of the asset,
- IP: The IP address of the asset, but this may change over time,
- Physical Location: The location within the organization that the asset is located. This may be *N/A* for virtual or cloud-based systems,
- Purchase Date: The date the asset was acquired by the organization,
- Warranty Information: Relevant warranty information needed for the manufacturer,
- Other Notes: Other notes as needed.

Feel free to expand upon this spreadsheet as you see fit.



Asset Name	Type	Description	Model	Manufacturer	Vendor ID	Internal ID	MAC	IP	Physical Location	Purchase Date	Warranty Information	Notes

Figure 3 - Sample Hardware Asset Tracking Spreadsheet

Sample Software Asset Tracking Spreadsheet

Elements of a Sensitive Information Tracking Spreadsheet can include the following:

- Software Product Name: Common name of the software asset,
- Type: The type of software product (e.g., Software as a Service (SaaS), Local instance),
- Description: A description of the asset and what it's used for,
- Version: The version of the software that was acquired and is currently being used. This may be multiple versions on different platforms,
- Developer: The developer of the software product,
- License Type: The specific category of license for the package that was purchased (e.g., Home, Premium),
- License Key: The activation token needed to reuse the software on a different system,
- Date Purchased: The date the software package was obtained,
- Other Notes: Any other relevant notes for this software product.

Feel free to expand upon this spreadsheet as you see fit.

Name	Type	Description	Version	Developer	License Type	License Key	Date Purchased	Notes

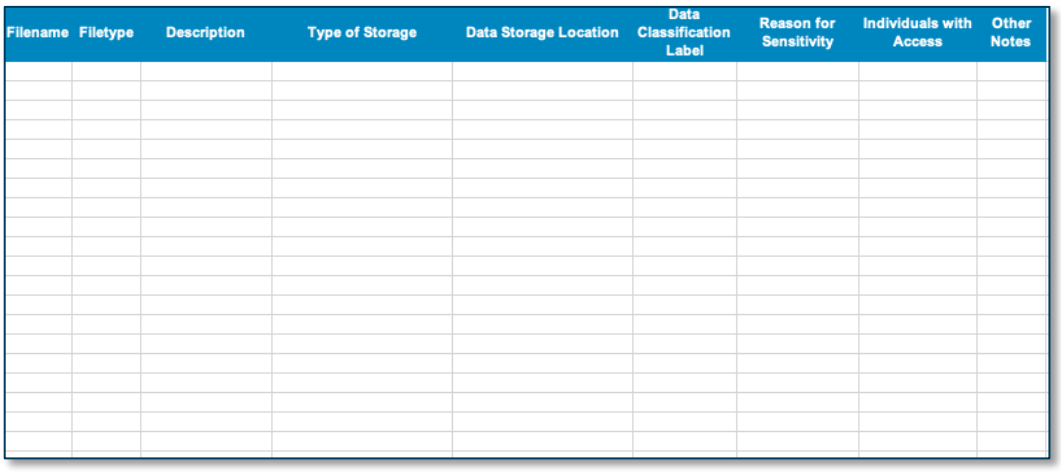
Figure 4 - Sample Software Asset Tracking Spreadsheet

Sample Sensitive Information Tracking Spreadsheet

Elements of a Sensitive Information Tracking Spreadsheet can include the following:

- Filename: The filename of the sensitive data in question,
- Filetype: The filetype of the sensitive data in question. This may be *N/A* if it's a physical file,
- Description: A description of the data and why it's considered sensitive,
- Type of Storage: Electronic or physical. If the data is duplicated in both forms, make separate entries for each,
- Data Storage Location: The physical or electronic location that the information is stored in or at,
- Data Classification Label: If data classification labels are used, they can also be reflected here. This may include sensitive, trade secret, proprietary, or other classifications as needed,
- Reason for Sensitivity: The type of reason why the data is considered sensitive, which may be similar to the data classification label. This includes trade secret, under non-disclosure agreement (NDA), or under a regulatory framework like HIPAA,
- Individuals with Access: A list of the authorized people that can access the sensitive information,
- Other Notes: Any other relevant notes for information.

Feel free to expand upon this spreadsheet as you see fit.



Filename	Filetype	Description	Type of Storage	Data Storage Location	Data Classification Label	Reason for Sensitivity	Individuals with Access	Other Notes

Figure 5 - Sample Sensitive Information Tracking Spreadsheet

Appendix B: Step-by-Step Instructions to Implement Sub-Controls

Uninstalling Software

This process relates to CIS Control 2.6: Address Unapproved Software. Follow these steps to uninstall unapproved software:

1. Click the Windows Start button. The Windows Start menu displays with the search bar.
2. Enter “settings” in the search field.
3. Click the search icon. Windows displays Settings options for the computer.

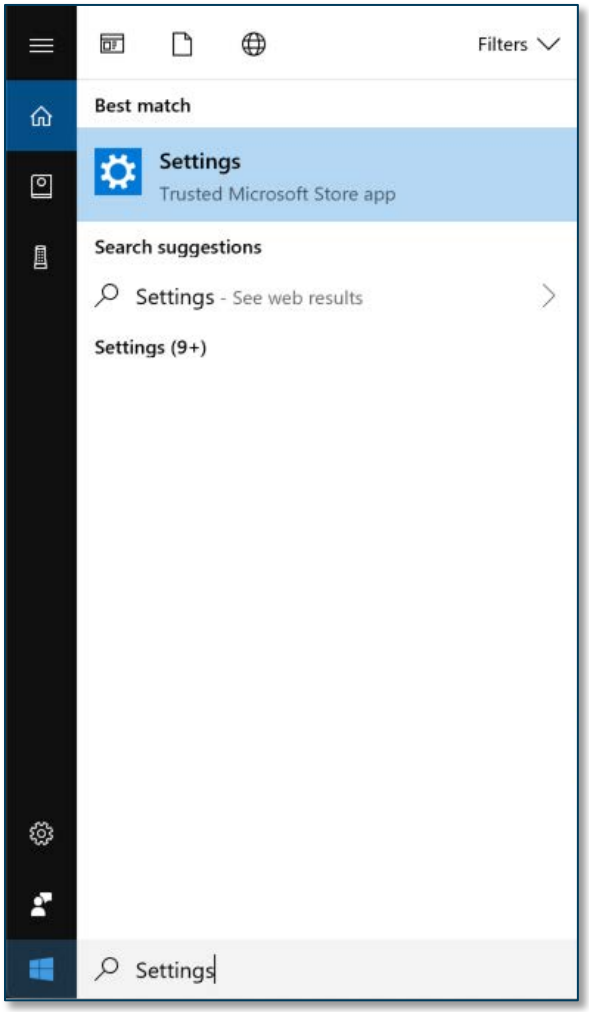


Figure 6 - Searching for Settings

4. Select the Windows Settings app. The Windows Settings Home Screen displays.

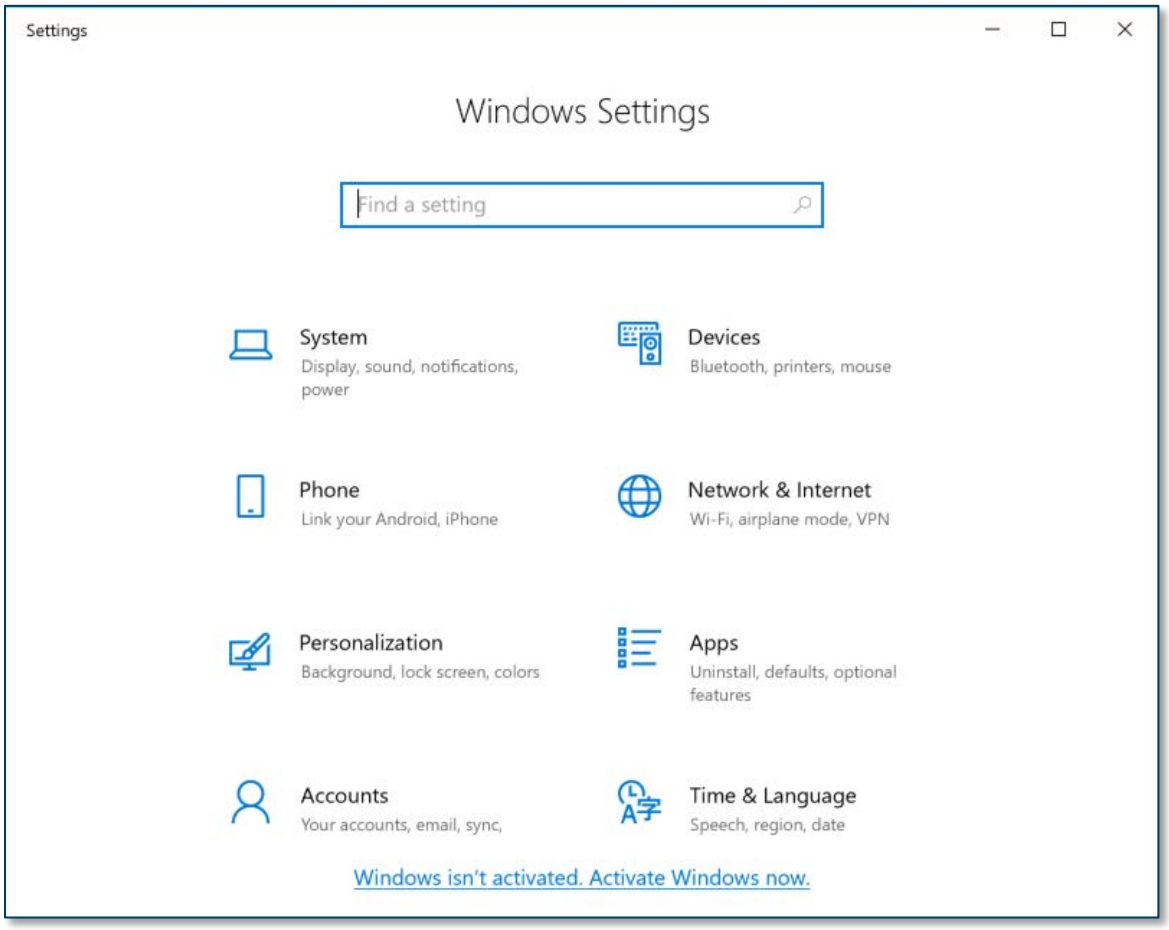


Figure 7 - Windows Settings Home Screen

5. Click *Apps.* The Apps and Features window opens with a list of installed applications. All installed applications on the Windows 10 machine are available here. Select the application that should be uninstalled. Note that some of the listed apps cannot be uninstalled.

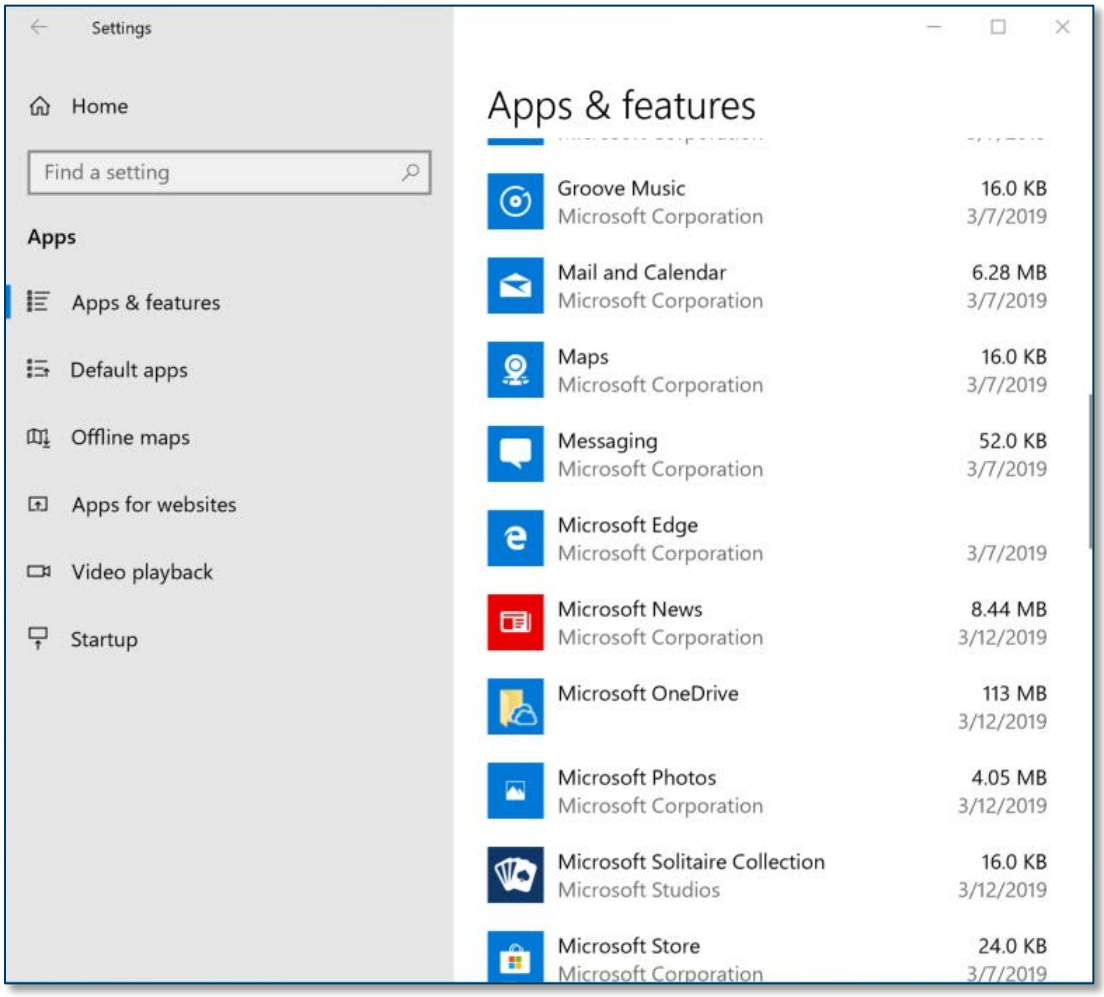


Figure 8 - Listing of Installed Applications

6. Select the app to remove. The item expands with “Move” and “Uninstall” buttons.
7. Select *Uninstall*. A confirmation dialog box opens with “This app and its related info will be uninstalled”, and an “Uninstall” button.

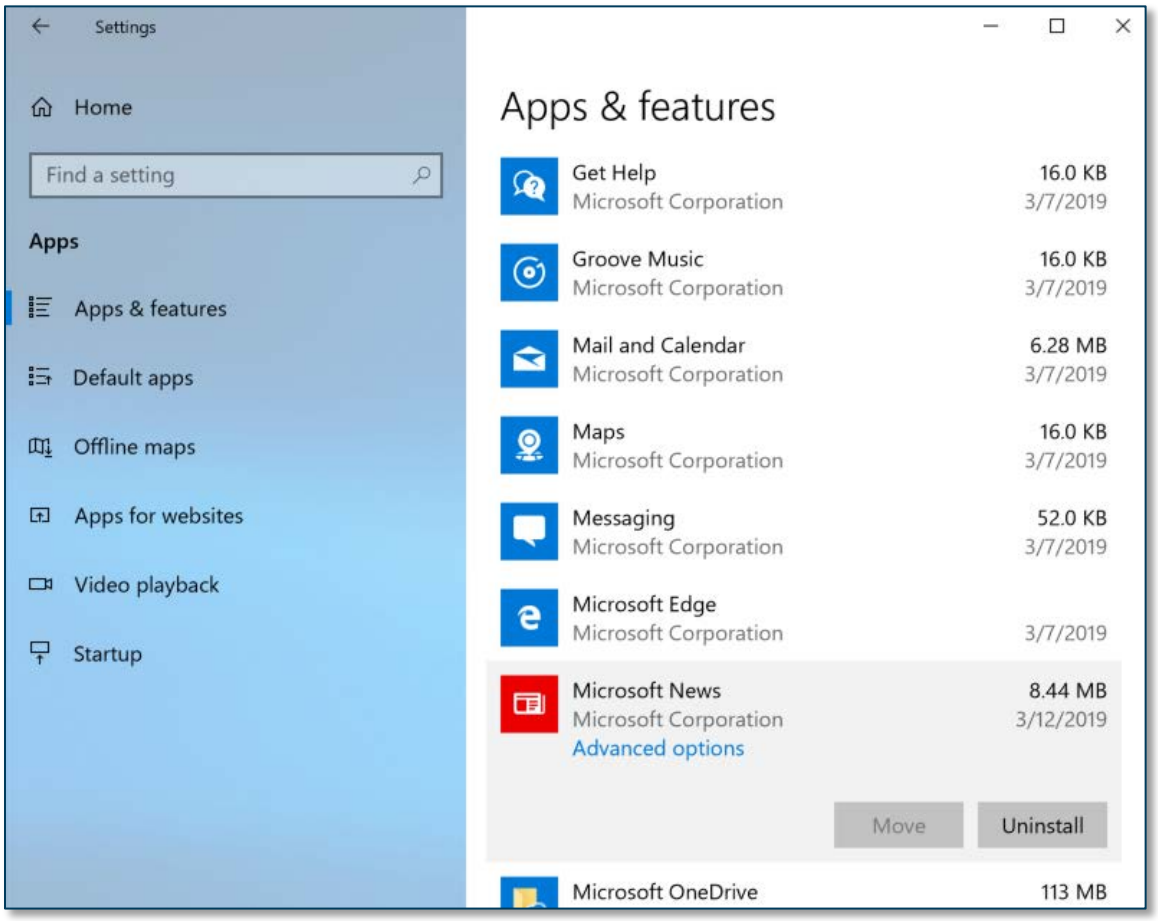


Figure 9 - Selected Installed Application

8. Select *Uninstall* another time to confirm. Windows uninstalls the application.

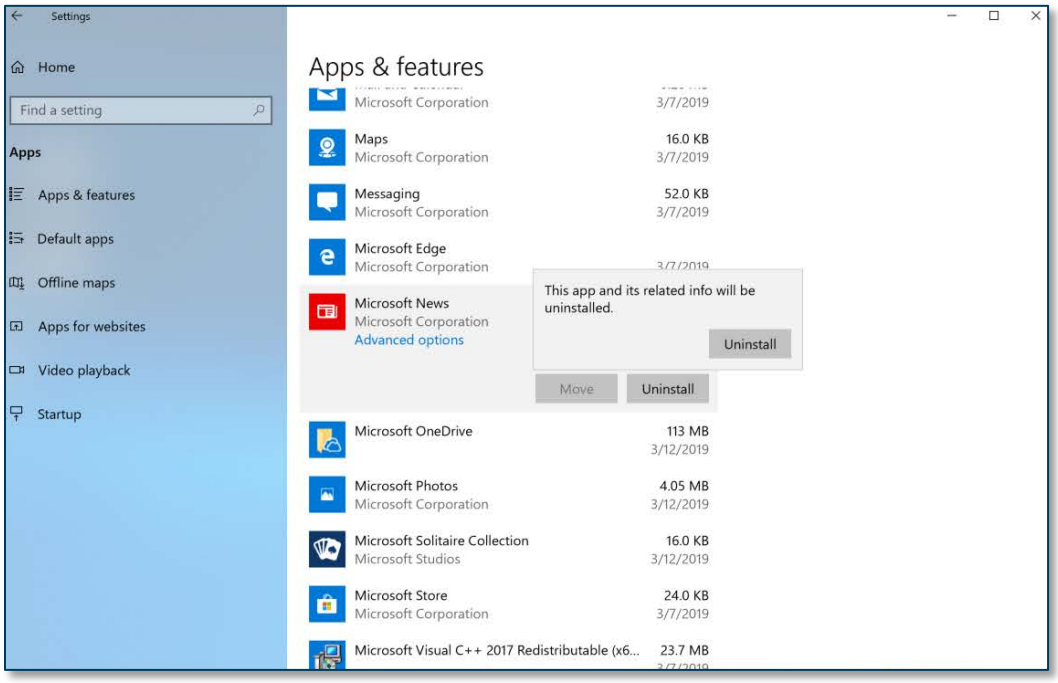


Figure 10 - Uninstalling an Application

Configuring Automated Operating System Patch Management Tools via Windows Settings

This process relates to CIS Control 3.4: Deploy Automated Operating System Patch Management Tools. Follow these steps to configure automated operating systems patch management tools.

Note: The local group policy method used in the next section is the preferred way of implementing this Sub-Control.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “windows update” in the search bar. The Start Menu populates with Windows update options.

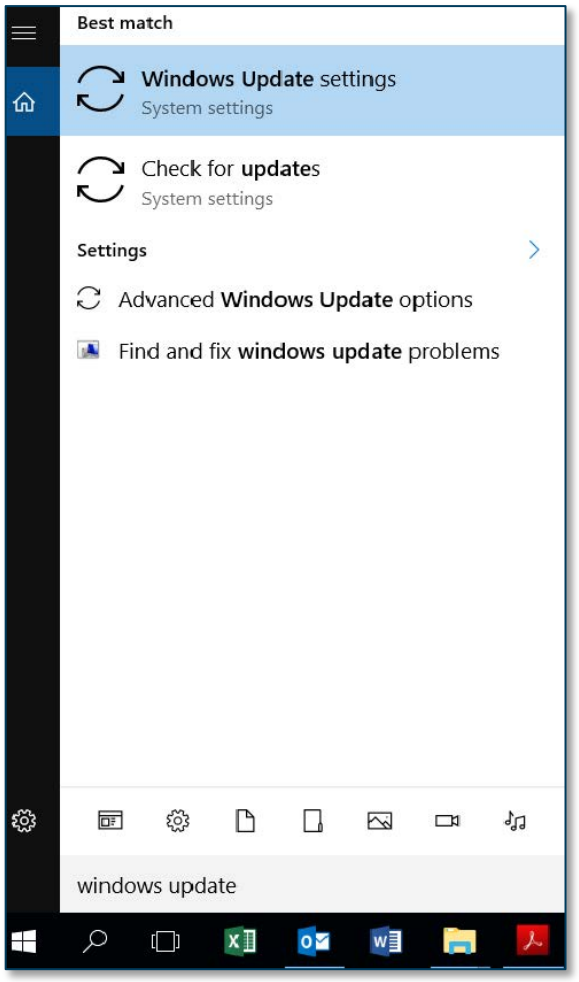


Figure 11 - Searching for Windows Update Settings

3. Select *Windows Update Settings*. The Windows Update panel displays. This screen shows the status of updates for the computer. If there are updates, they will be listed.

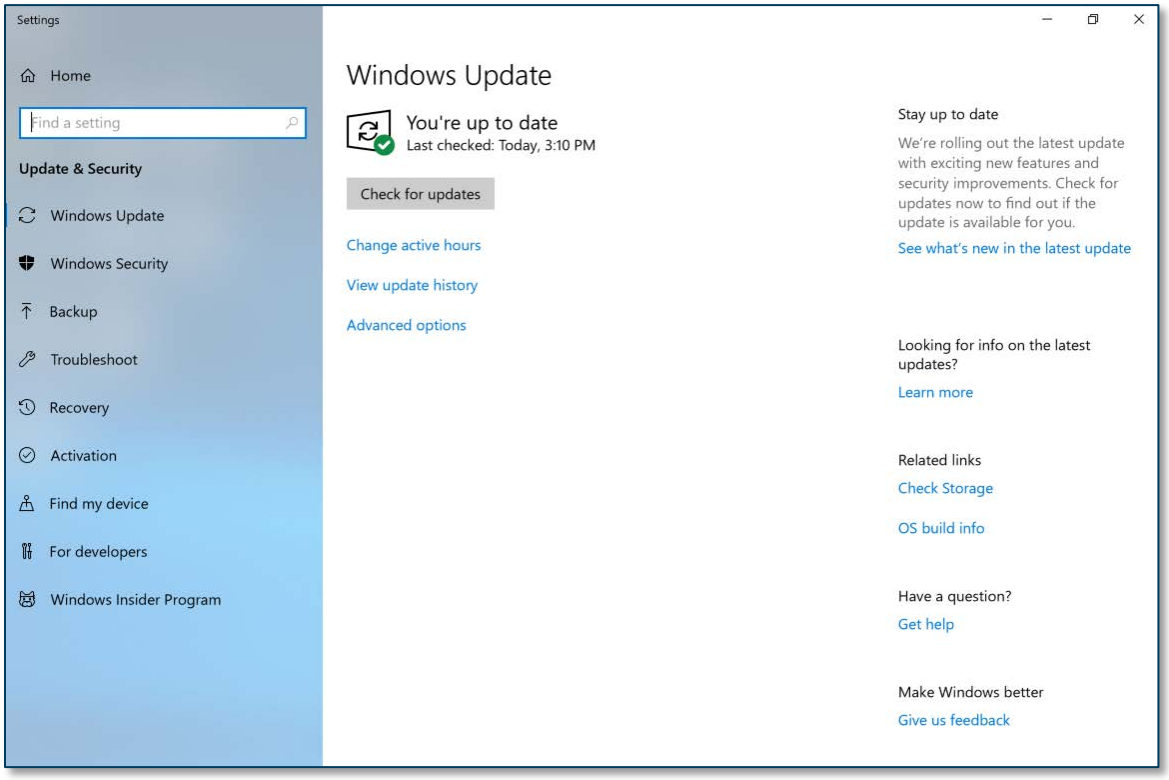


Figure 12 - Windows Update Status

4. Select *Check for updates* to see if updates are available. Selecting *Advanced options* will provide additional system update settings.
5. Select *Advanced options*. Ensure that *Pause Updates* is set to *Off*.

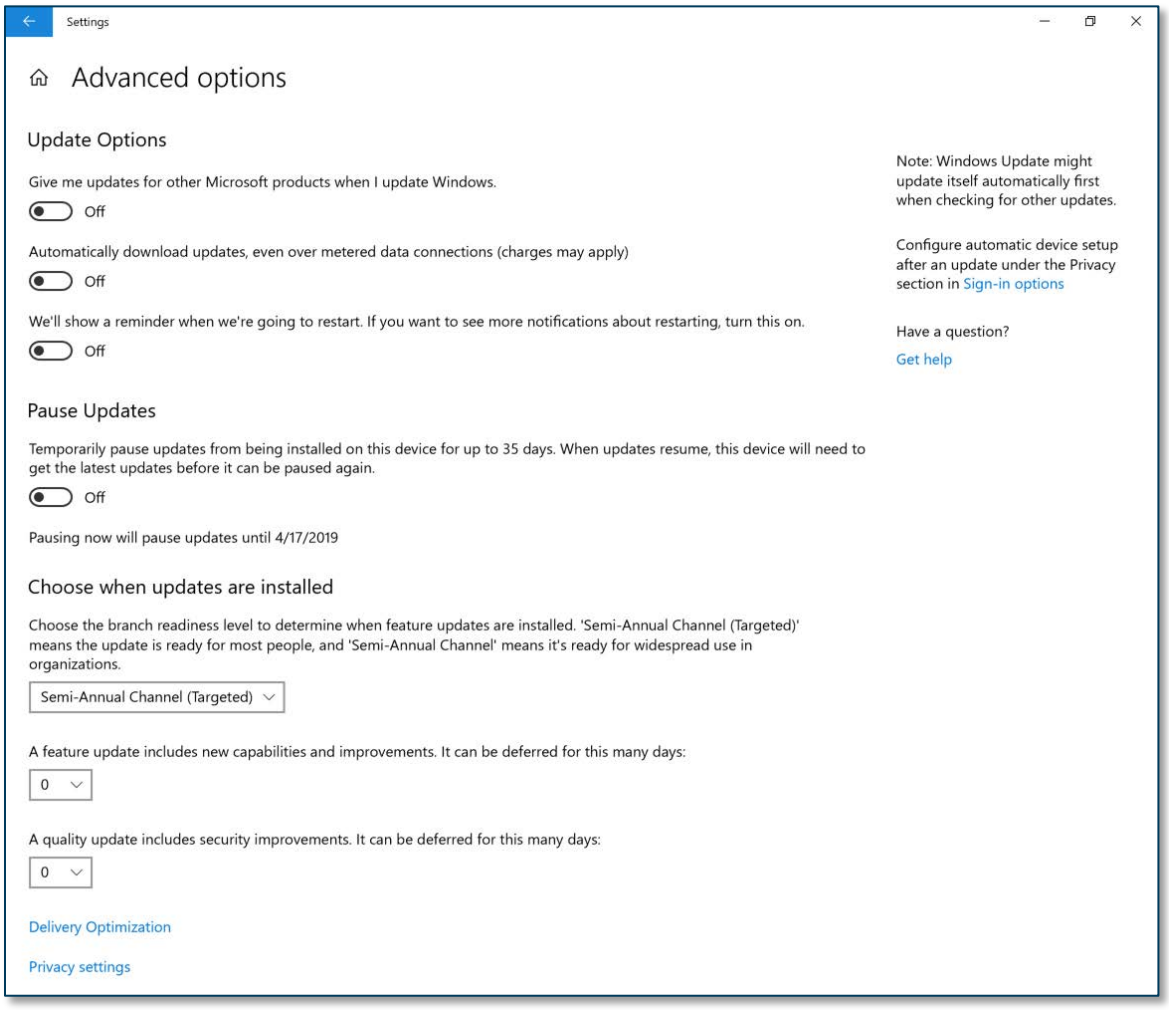


Figure 13 - Advanced Update Options

Configuring Automated Operating System Patch Management Tools via LGPE

This control applies to CIS Control 3.4: Deploy Automated Operating System Patch Management Tools.
Note: The LGPE can be used to configure device settings for patching Windows 10 Pro.

1. Click *Start*. The Windows Start menu displays with the search bar.
2. Enter “local group” in the search bar. Figure 13 illustrates the LGPE search.

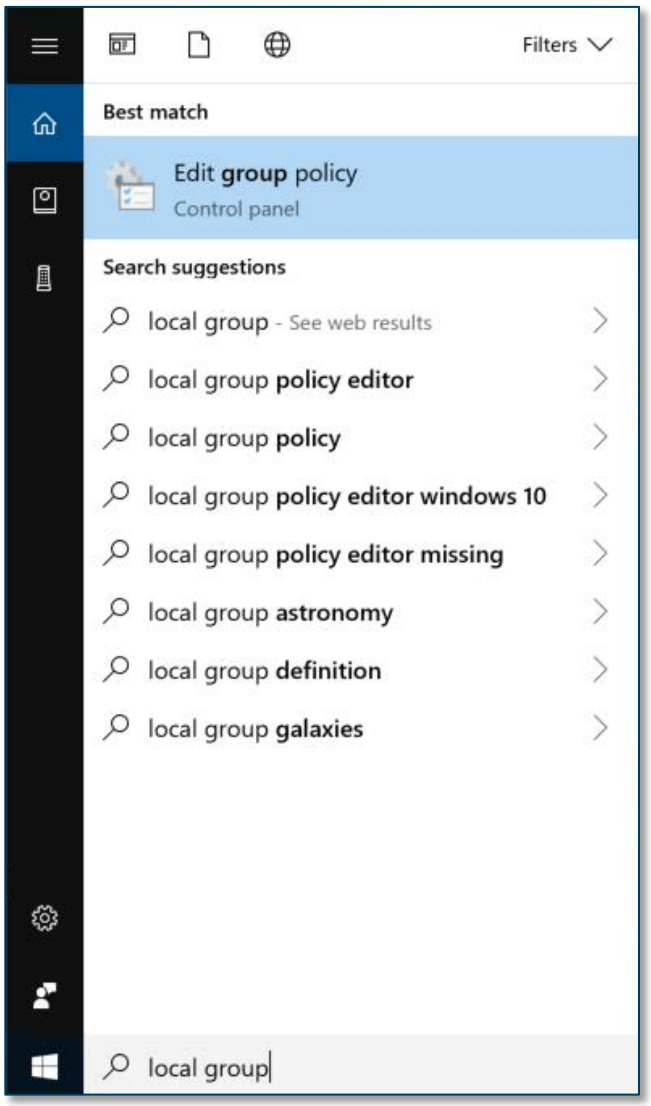


Figure 14 - Searching for LGPE

3. Select the Local Group Policy Editor option in the search list. The Local Group Policy Editor Home Screen displays. See Figure 14.

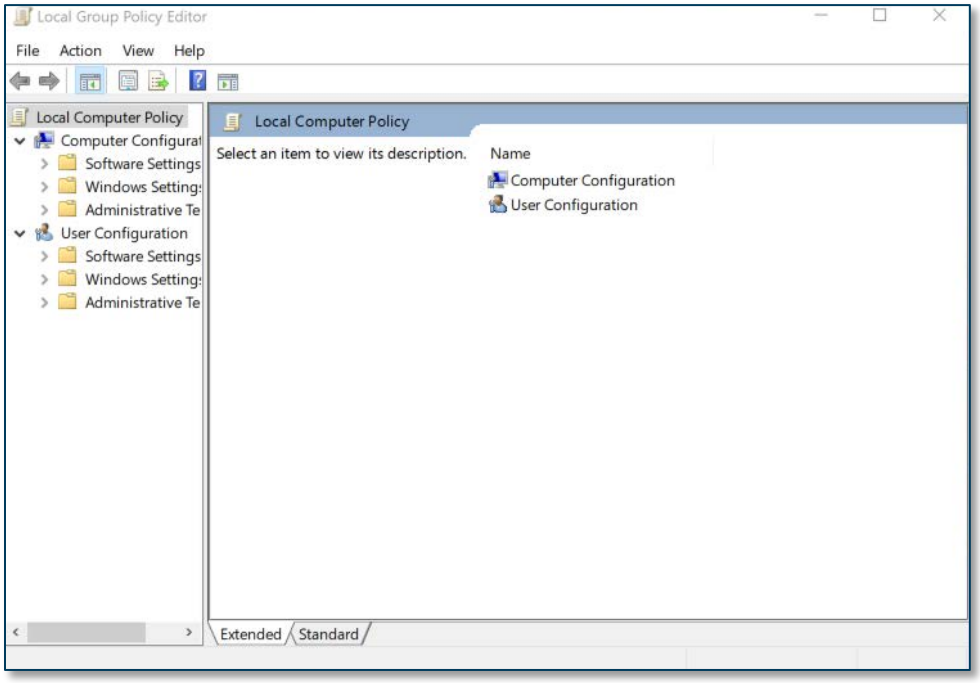


Figure 15 - LGPE Home Screen

4. Select *Computer Configurations*, then select *Administrative Templates,* and then *Windows Components*. The *Windows Components* folder displays with its subfolders.

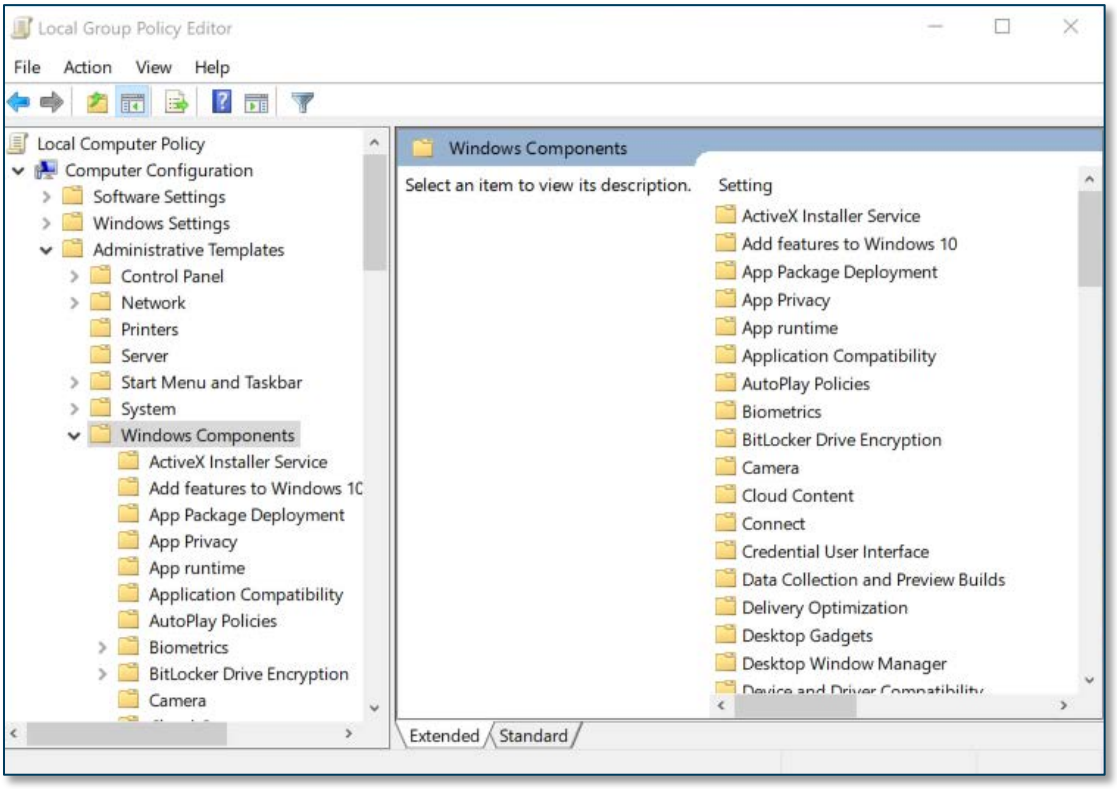


Figure 16 - LGPE Windows Components

5. Select *Windows Update* and double click *Configure Automatic Updates*.

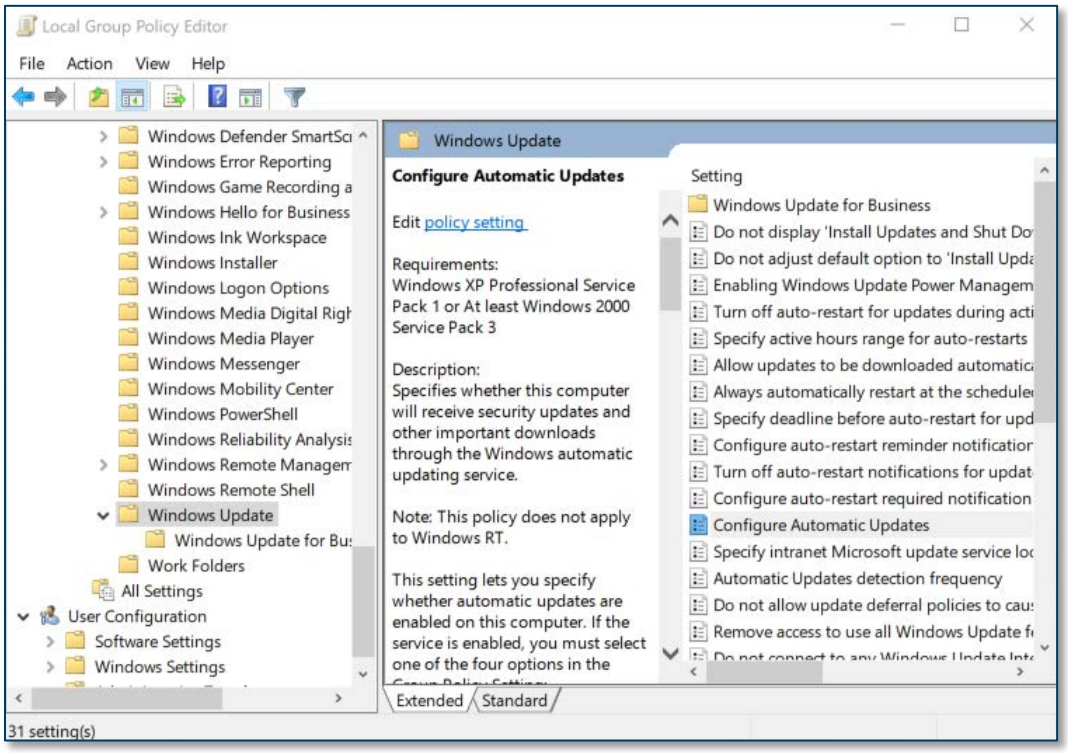


Figure 17 - LGPE Windows Update Settings

6. Ensure that *Enabled* is selected.
7. Ensure *Configure automatic updating* is set to *4 – Auto download and schedule the install*. Select *OK*.

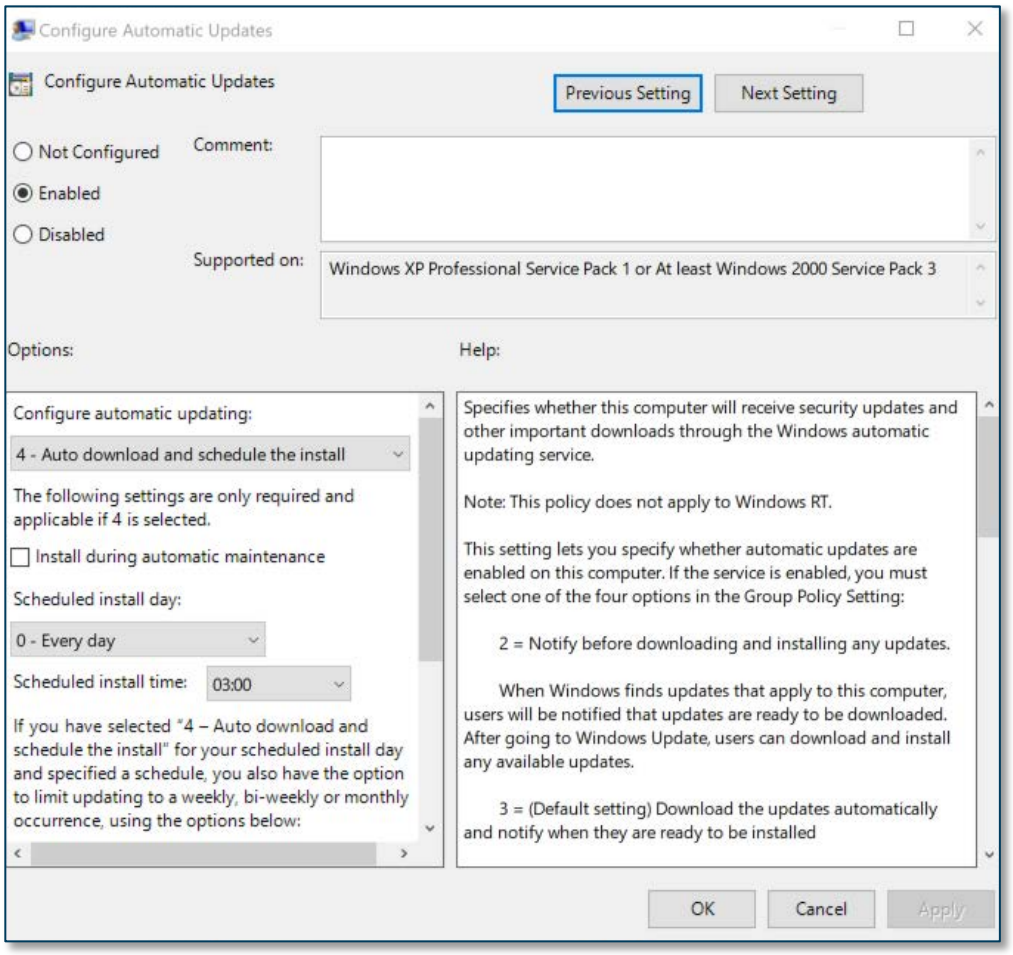


Figure 18 - Auto Download Home Screen

Automatic Application Updates via the Microsoft Application Store

This control applies to CIS Control 3.5: Deploy Automated Software Patch Management Tools. Follow these steps to apply automatic application updates.

1. Click *Start*. The Windows Start menu displays with the search bar.
2. Enter “Microsoft Store” in the search field.

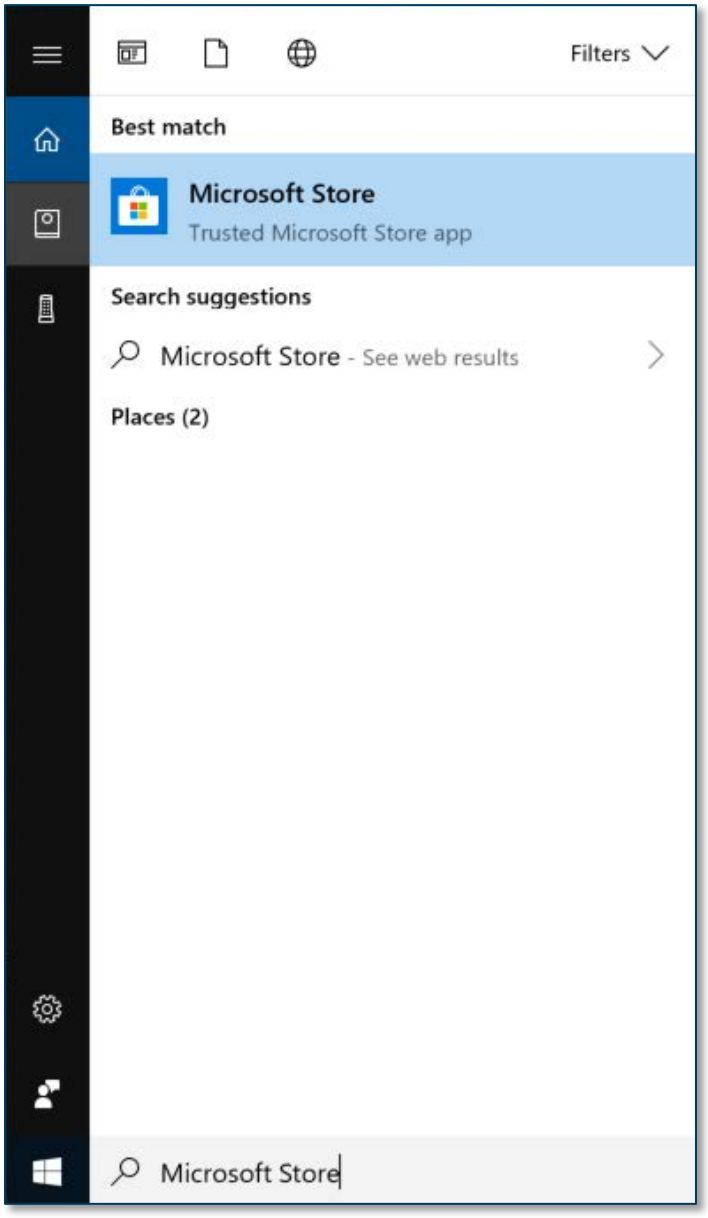


Figure 19 - Searching for the Microsoft Store

3. Select the Microsoft Store app in the search results. The *Microsoft Store Home Screen* displays.

4. Select the three dots (. . .) in the top right under the “x”. The Settings drop-down list displays.

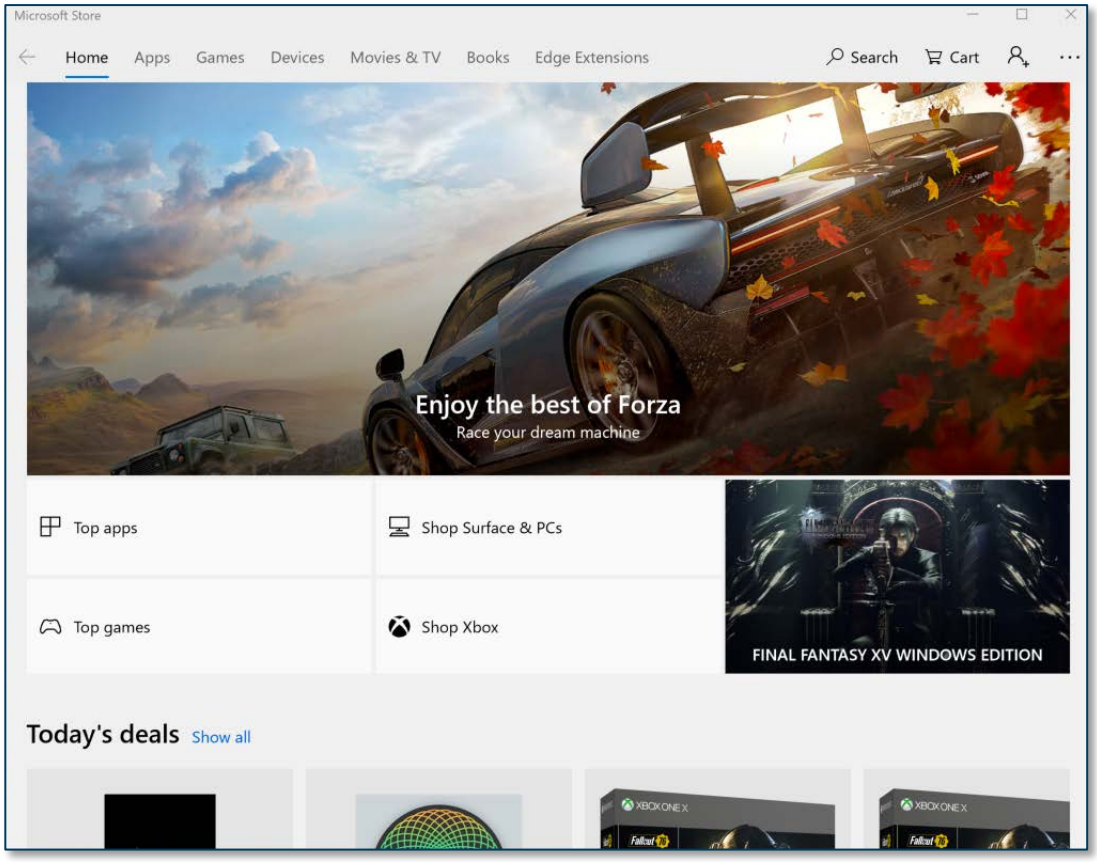


Figure 20 - Microsoft Store Home Screen

5. Select *Settings*. The Settings screen displays.

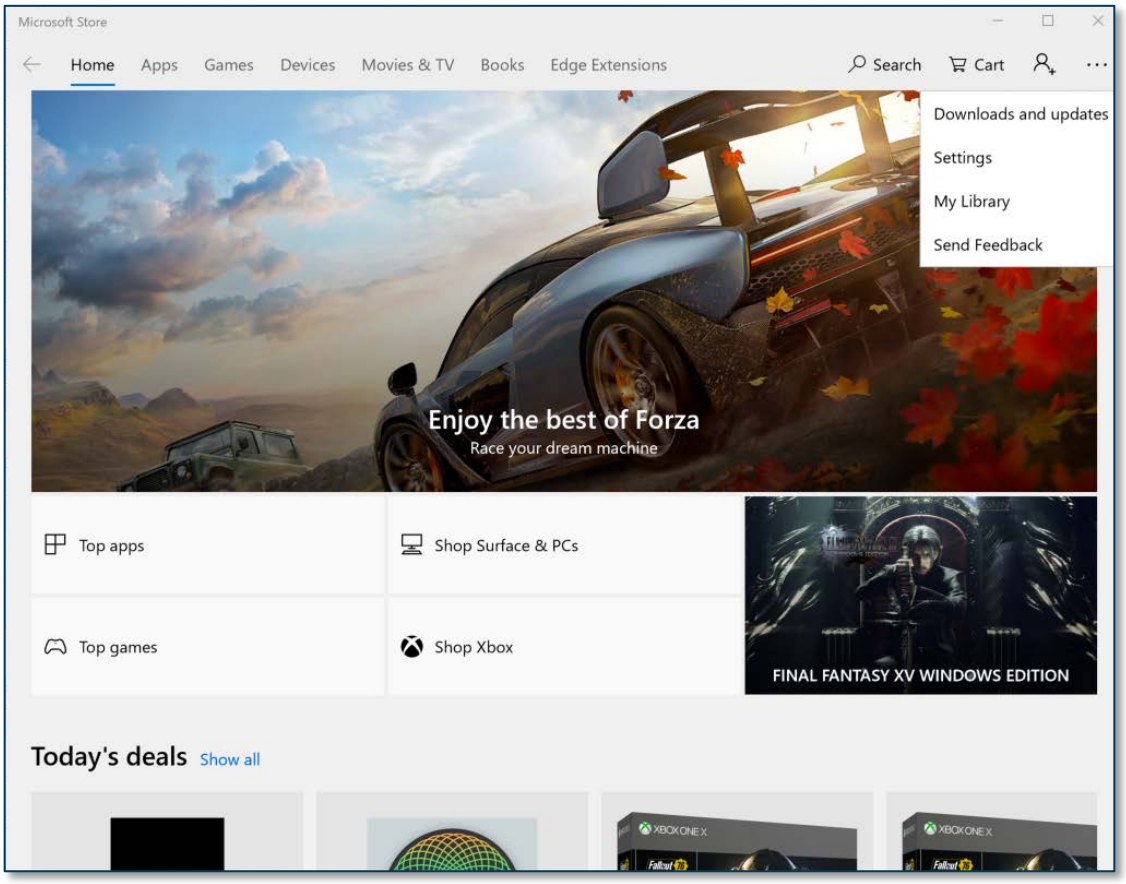


Figure 21 – Available Settings in Microsoft Store

6. Ensure that *Update apps automatically* is set to *On*.

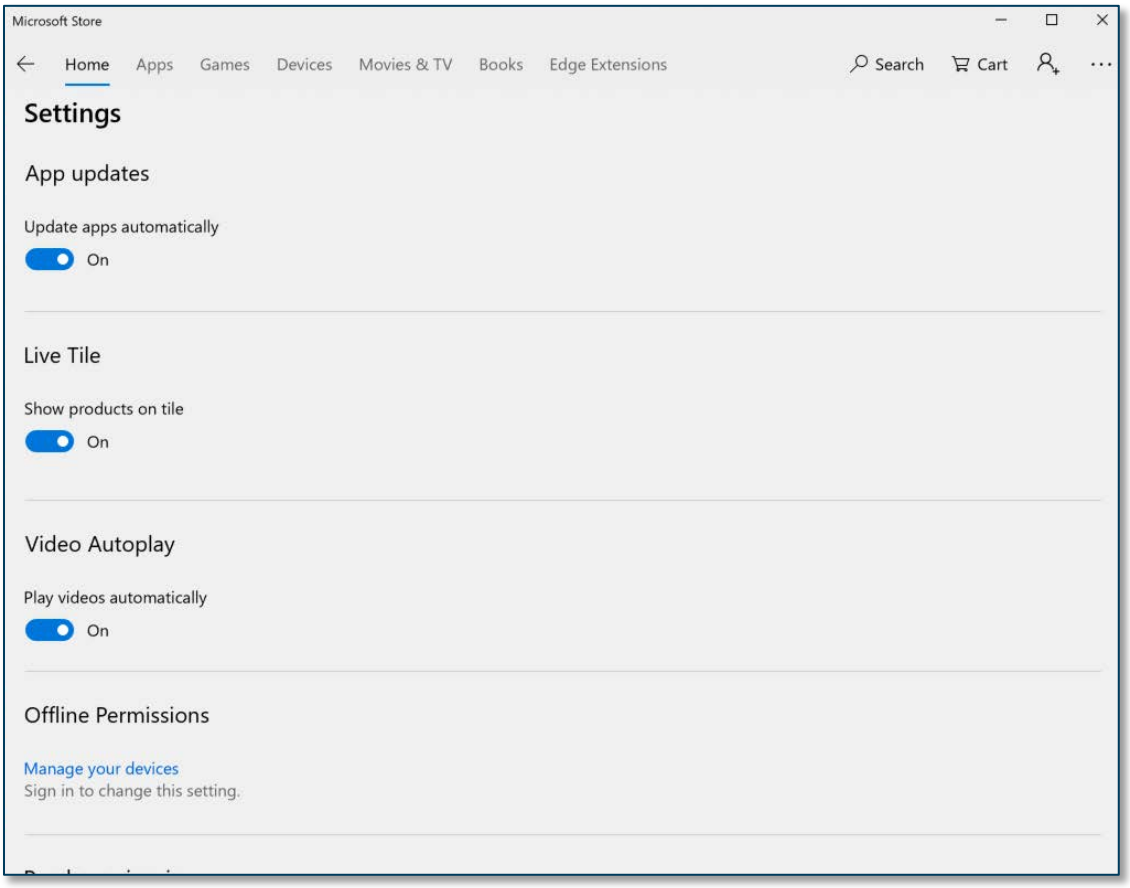


Figure 22 - Detailed Settings in Microsoft Application Store

Note: More steps are required to partially fulfill this Sub-Control.

1. Click *Start*. The Windows Start menu displays with the search bar.
2. Enter “windows update” in the Search field.

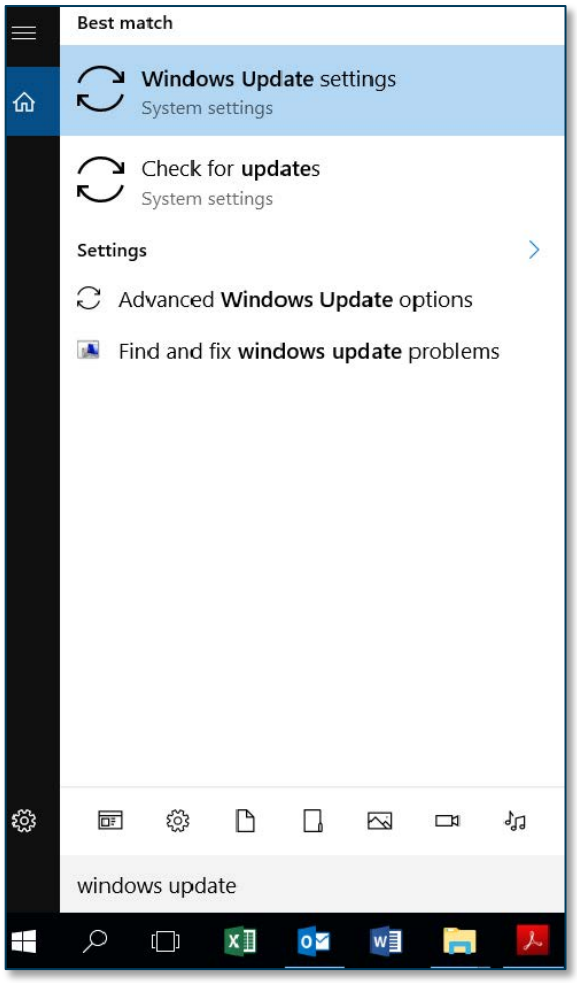


Figure 23 - Searching for Windows Update Settings

3. Select *Windows Update settings*. The *Windows Update* panel displays. This screen shows the status of updates.

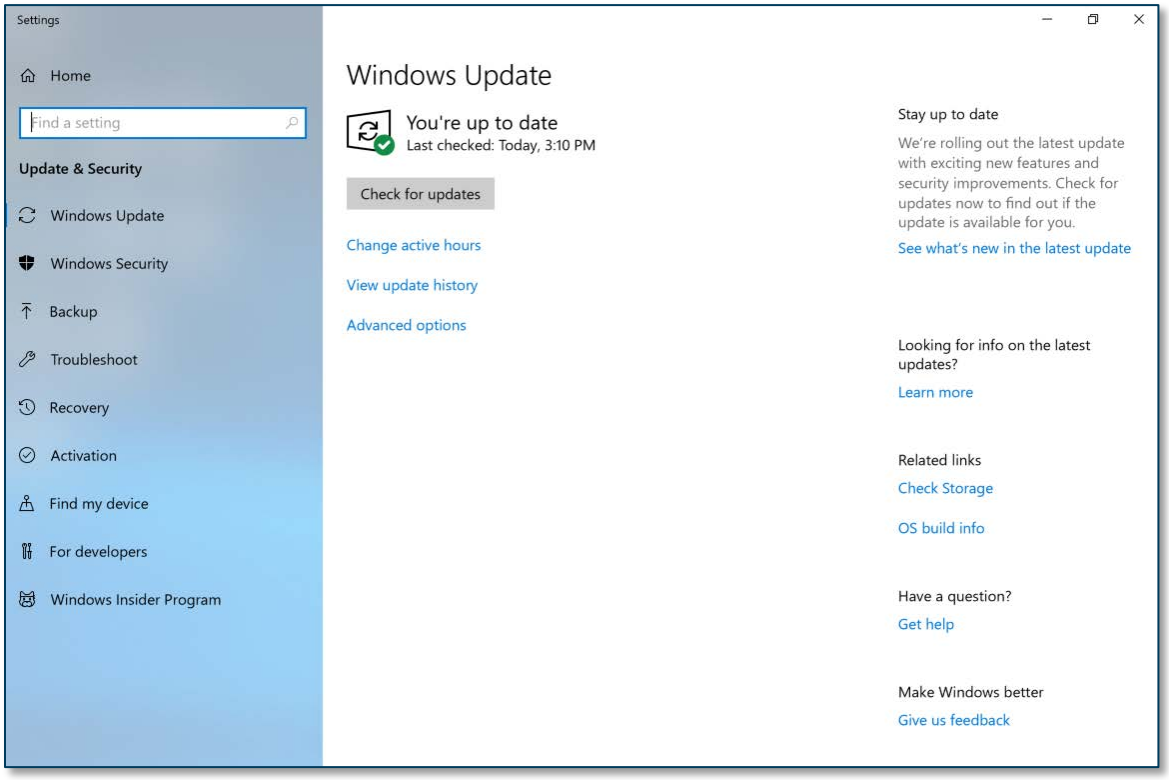


Figure 24 - Windows Update Home Screen

4. Select *Advanced options*. The *Advanced options* screen opens with additional system update settings shown in Figure 24.

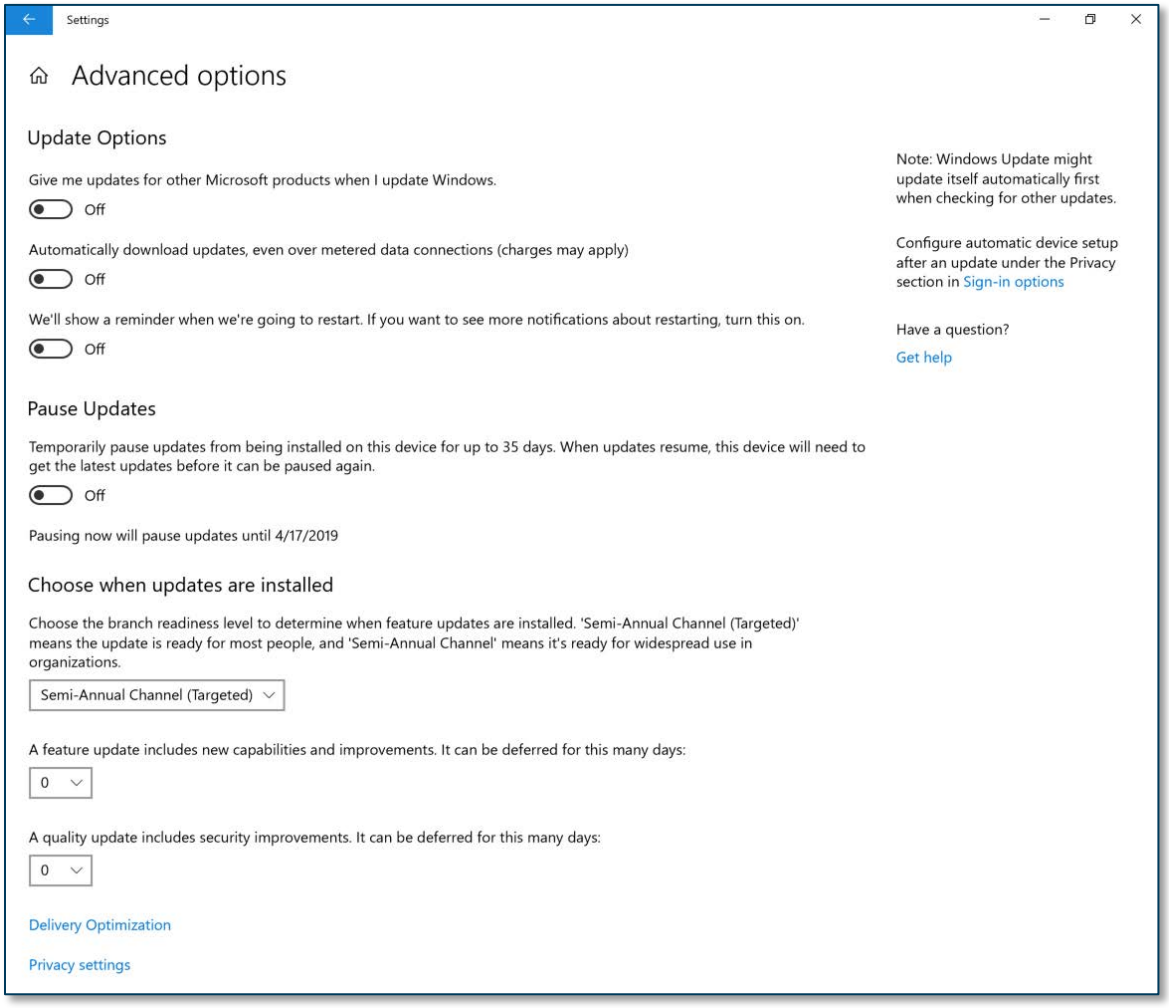


Figure 25 - Windows Update Advanced Options

5. Select *Give me updates for other Microsoft products when I update Windows* to automatically download updates for applications like Microsoft Word or Microsoft Excel. Refer to Figure 25.

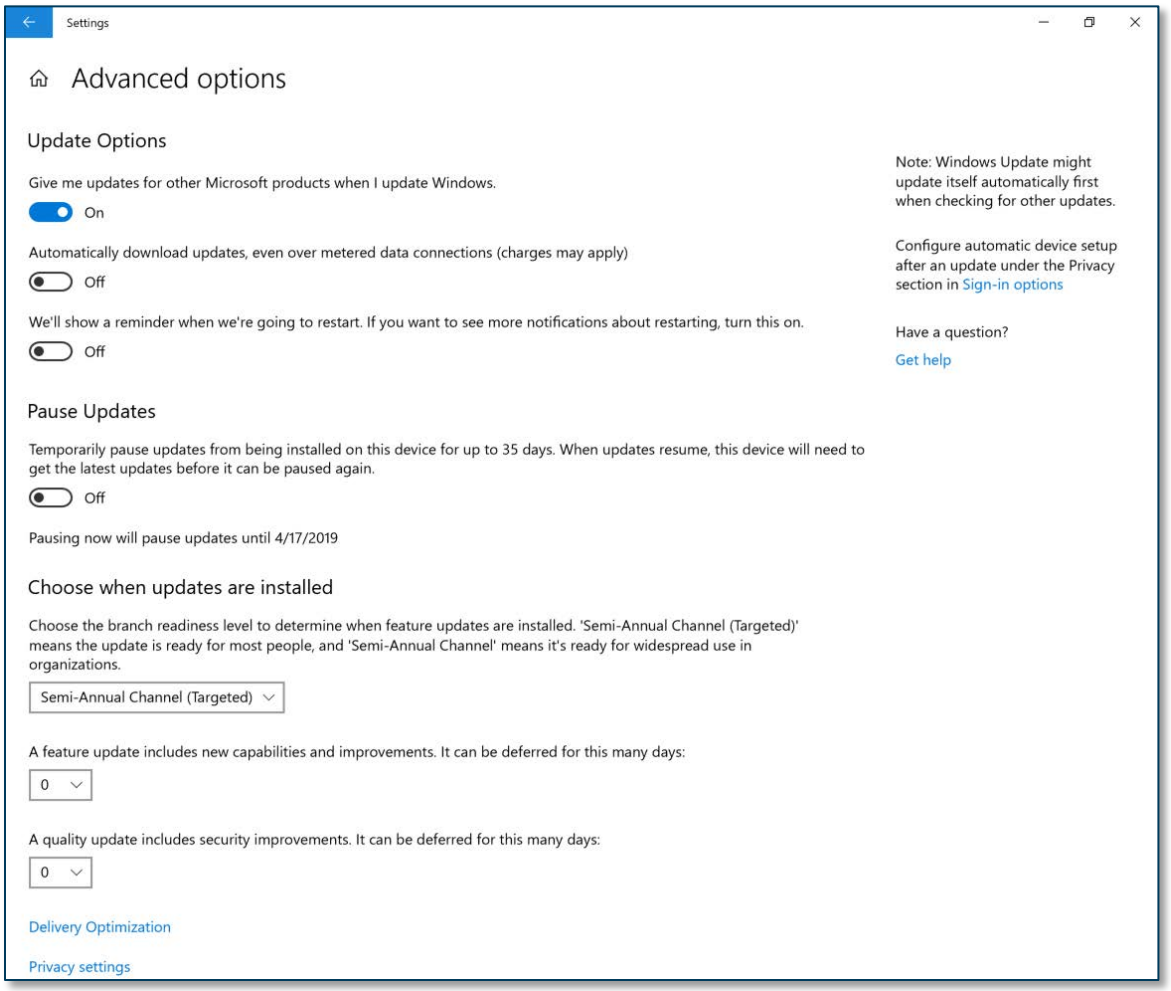


Figure 26 - Advanced Windows Update Options

Changing the Default Password

This control applies to CIS Control 4.2: Change Default Passwords. Follow these steps to change default passwords.

Note: The best method of achieving this Sub-Control is via local group policy in the next section.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “settings” in the search bar.
3. Click the search icon. Windows displays settings options for the computer.

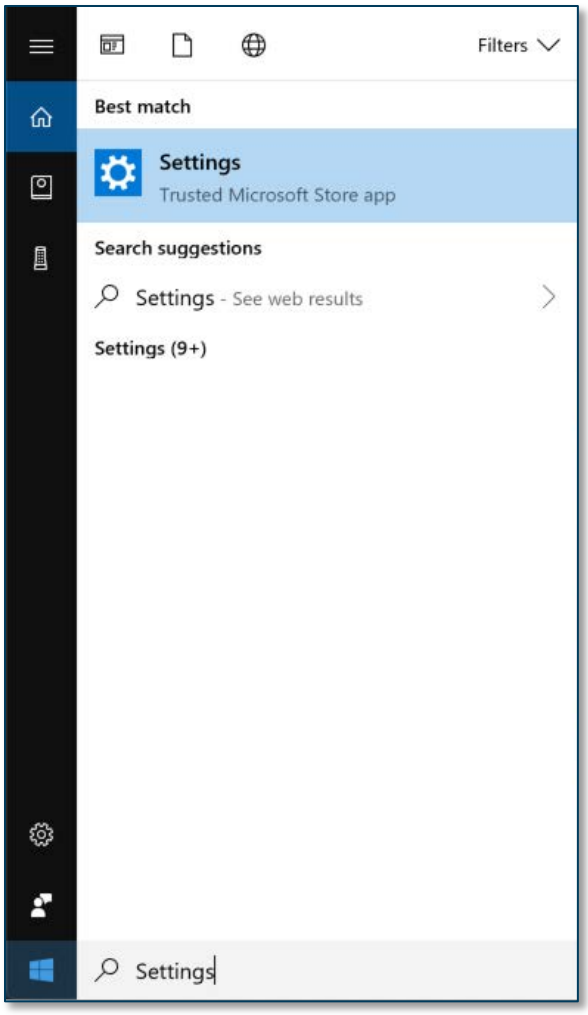


Figure 27 - Searching for Windows Settings

4. Select the Settings app. The *Windows Settings Home Screen* displays.
5. Select *Accounts*. The *Your info* screen displays.

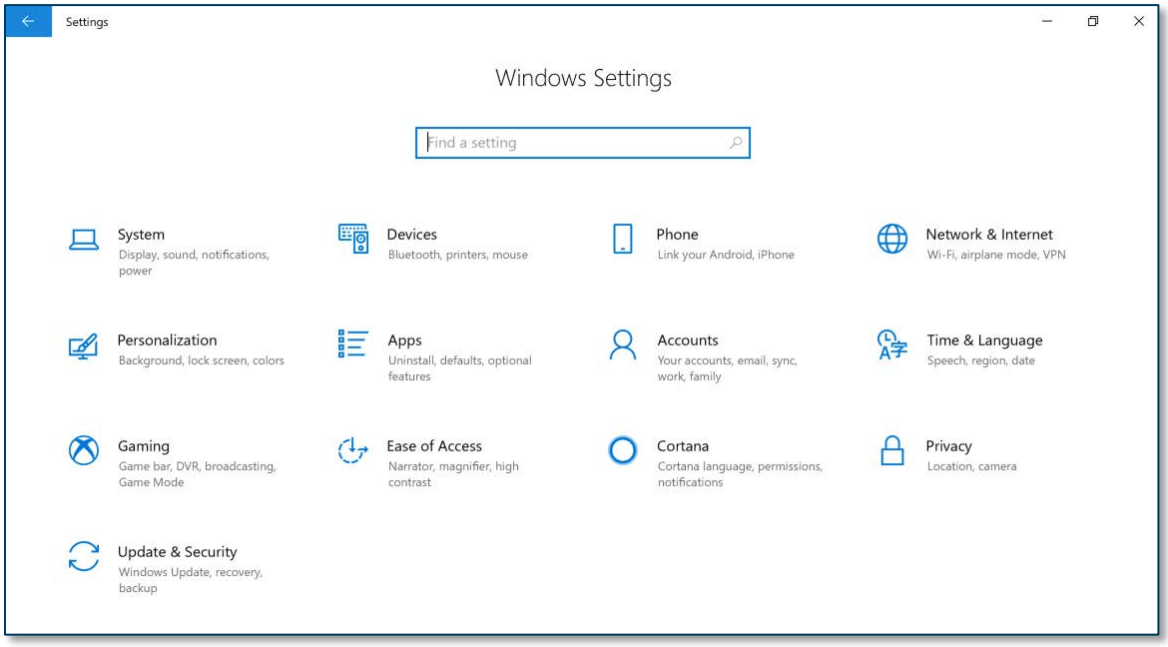


Figure 28 - Windows Settings Home Screen

6. Select *Sign-in options*. The *Sign-in options* screen displays.

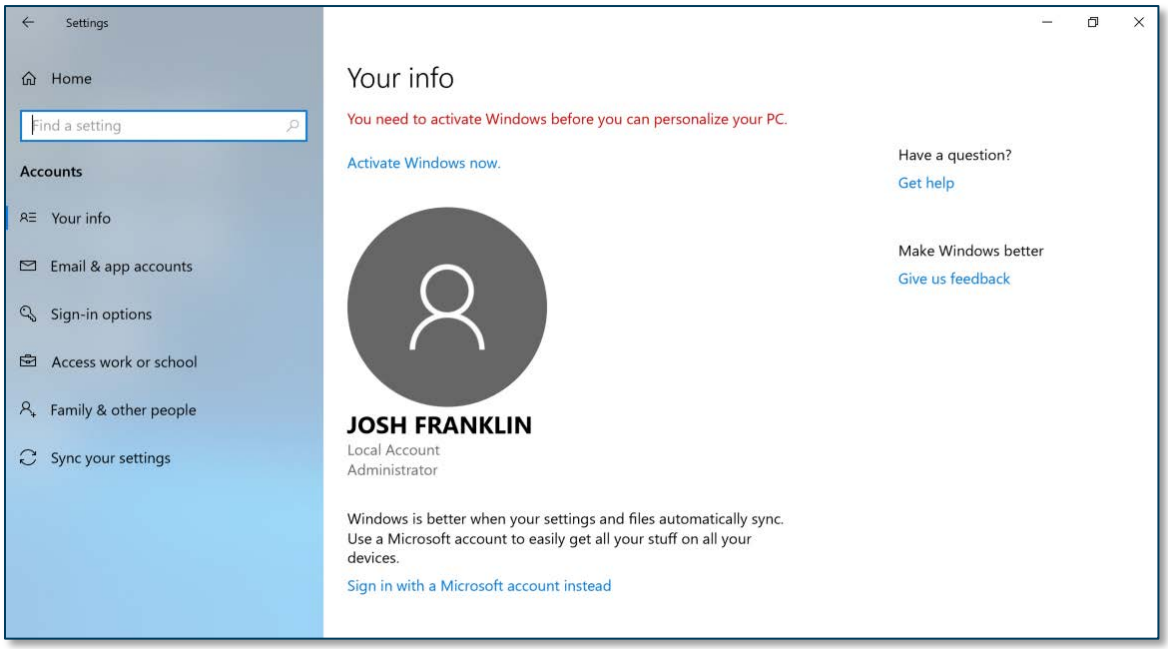


Figure 29 - Windows Accounts Home Screen

7. Select the *Change button* in *Change your account password*. The *Change your password* dialog box opens.

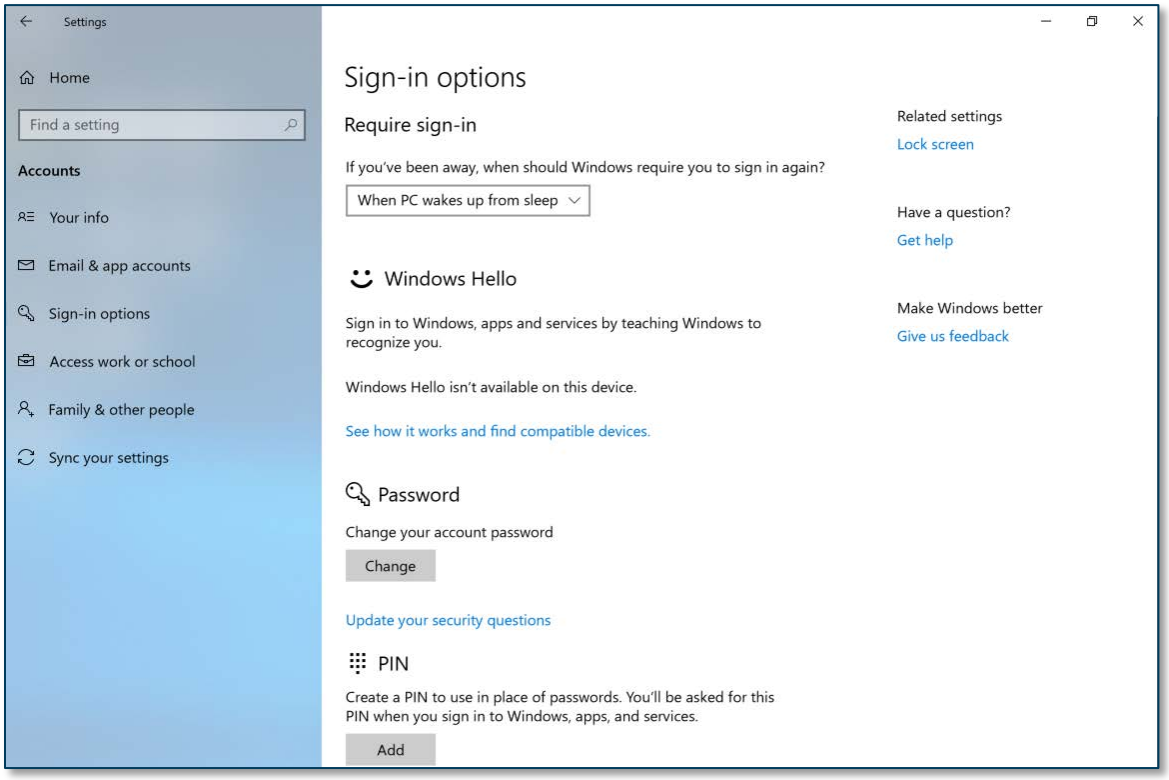


Figure 30 - Sign-in Options Home Screen

8. Enter the current password in the “Current password” text field. Select the “Next” button to continue. (An image for this step was intentionally not provided.)
9. Enter the new password into the password field. Ensure the password is not a commonly used one or one that has been used before.

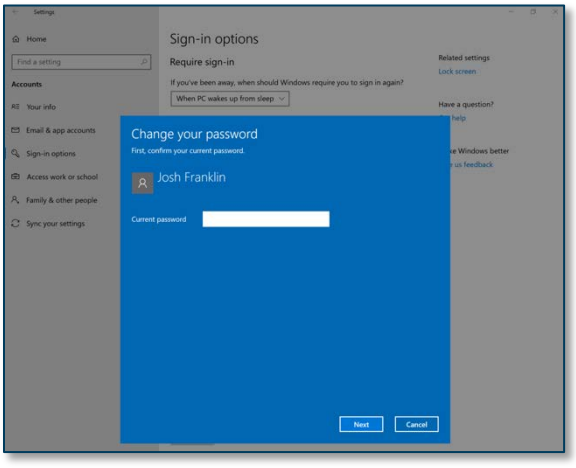


Figure 31 - Changing a Windows Password

Enforcing Password Length via LGPE

This process applies to CIS Control 4.2: Change Default Passwords. Use this process to enforce password length.

Note: The Local Group Policy Editor can be used to enforce a minimum password length. The CIS Windows 10 Benchmark recommends a 14-character password.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “local group” to open the Local Group Policy Editor. Figure 31 illustrates the Local Group Policy Editor search.

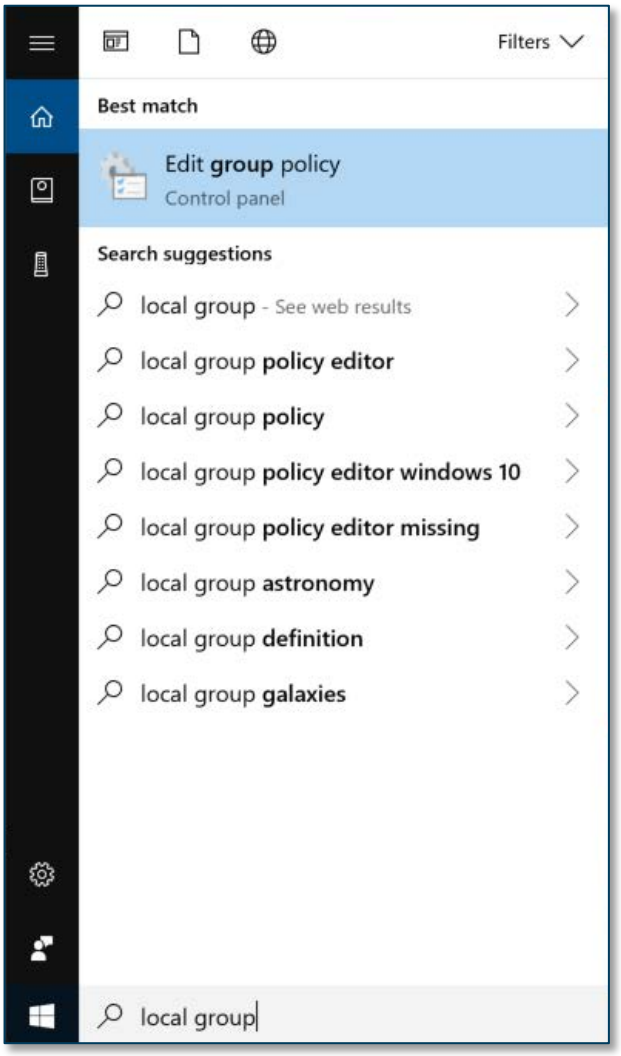


Figure 32 – Searching for LGPE

3. Select “Edit group policy” in the search list. The Local Group Policy Editor Home Screen displays.

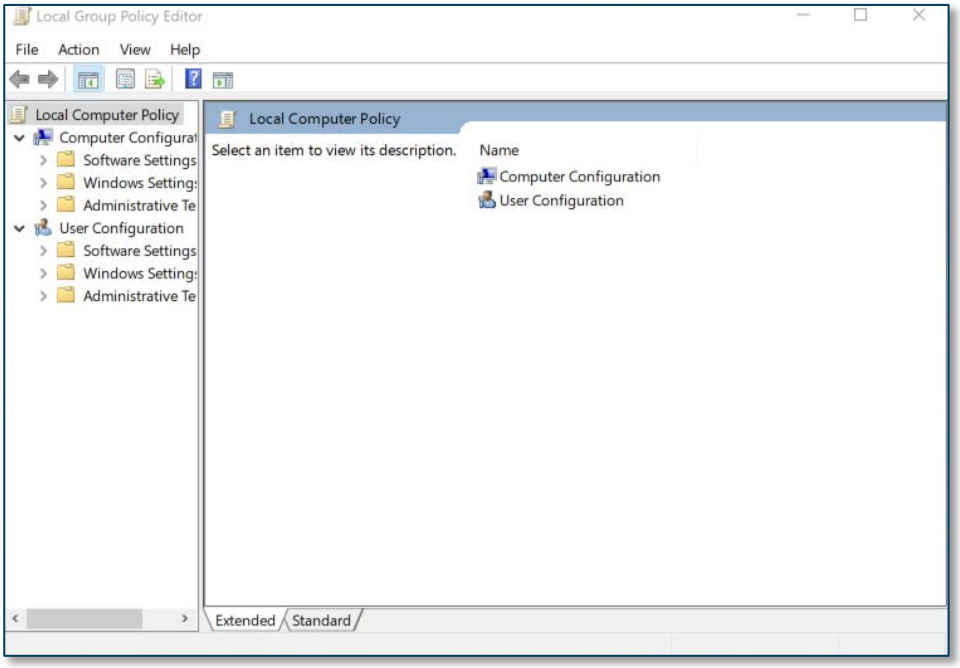


Figure 33 - LGPE Home Screen

4. Under *Computer Configuration*, expand *Windows Settings, then* select and expand *Security Settings*. The subfolders of *Security Settings* display.

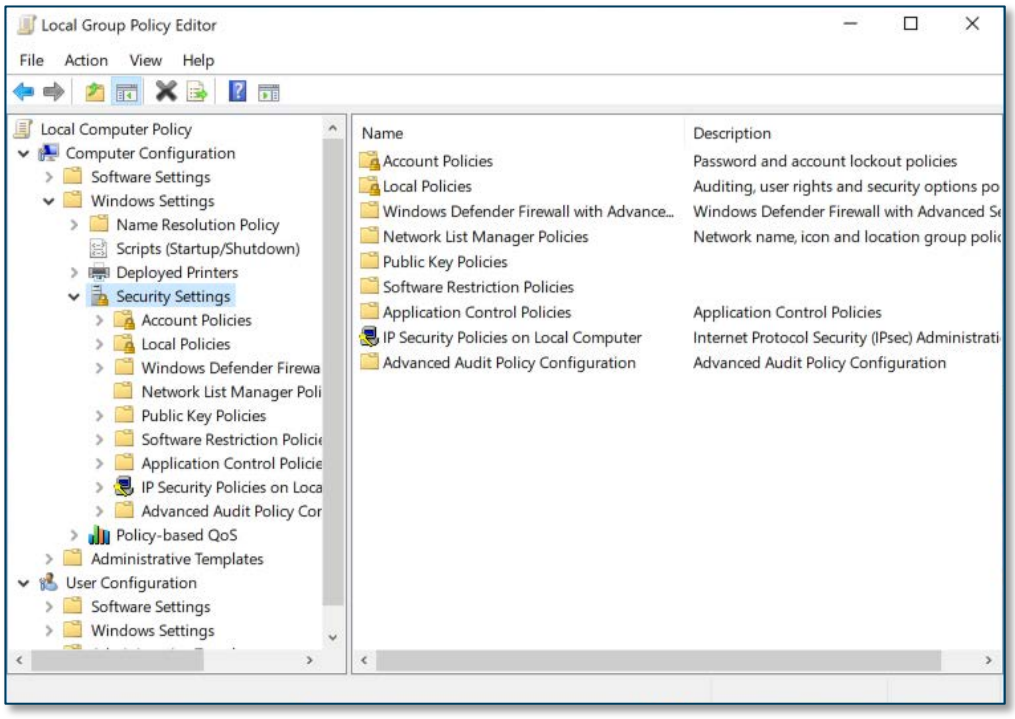


Figure 34 - LGPE Security Settings

5. Select *Account Policies*, then *Password Policy,* followed by *Minimum password length.*

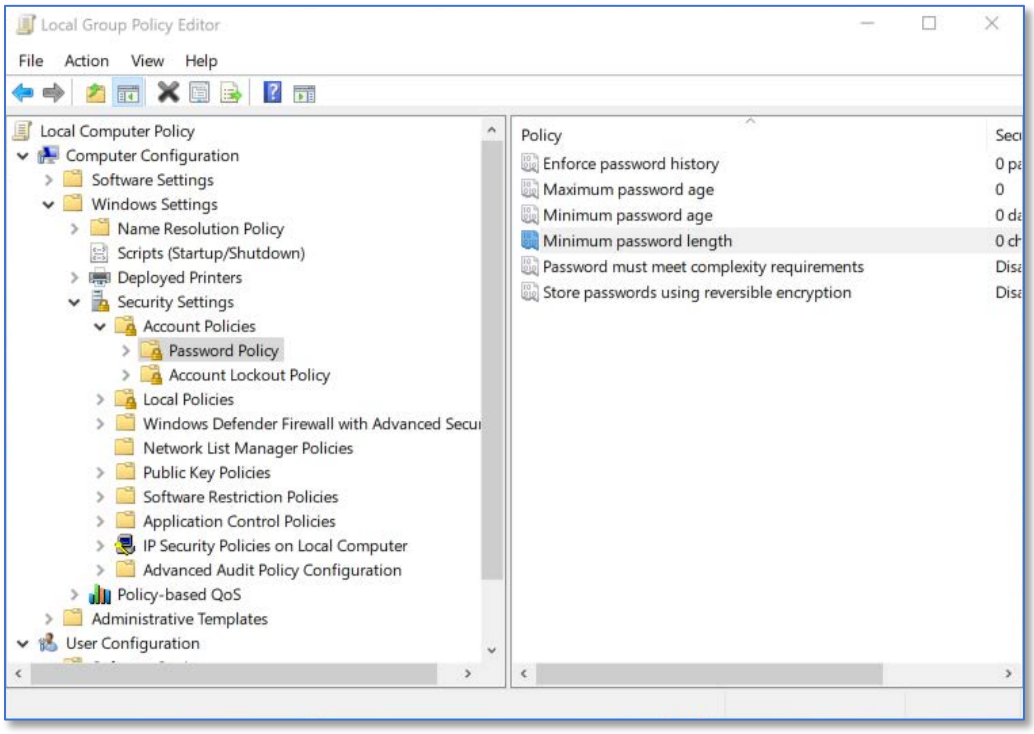


Figure 35 - LGPE Minimum Password Length

6. Enter “14” as the minimum password length. Select *Apply*. The minimum password length is set to 14 characters.

Note: Setting a required minimum password length will not automatically make users change their current password to meet policy. Users will need to manually update their password to meet the requirement, but Windows will ensure that future passwords are at least 14 characters long.

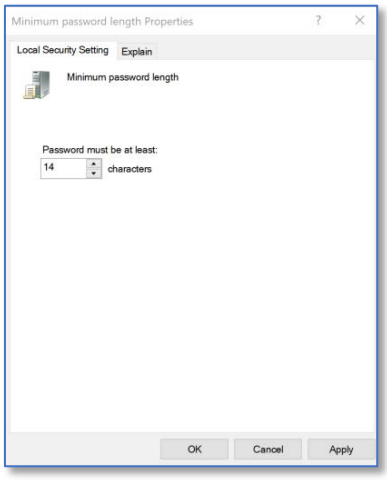


Figure 36 - Selecting Minimum Password Length

Identifying if an Account is an Administrator Account

This process applies to CIS Control 4.3: Ensure the Use of Dedicated Administrative Accounts.

1. Click Start. The Windows Start menu displays with the search bar.
2. Enter “settings” in the search field.
3. Click the search icon. Windows displays settings options for the computer.
4. Select the Settings app. The Windows Settings window opens.

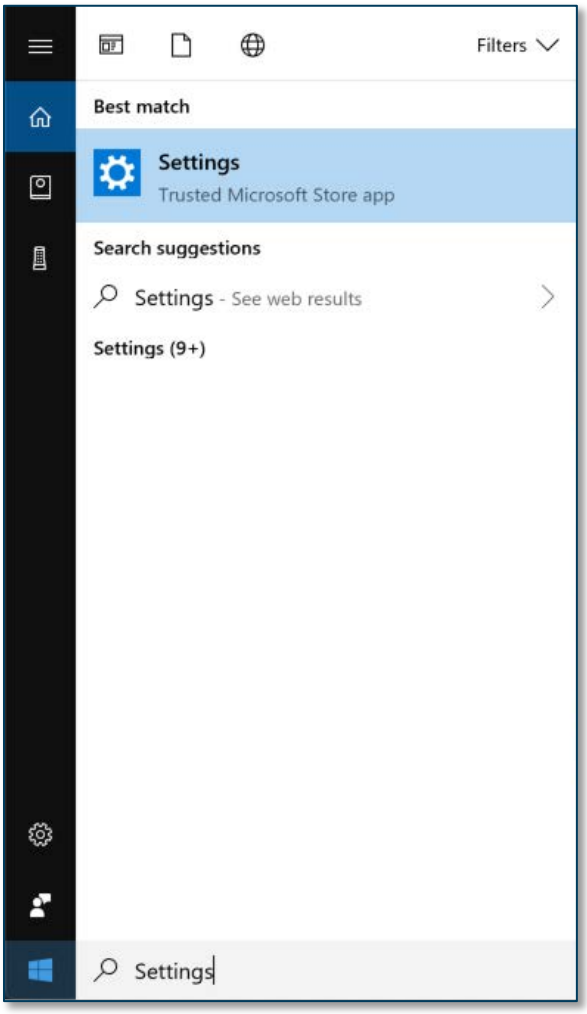


Figure 37 - Searching for Windows Settings

5. Select *Accounts*. The *Your info* screen opens.

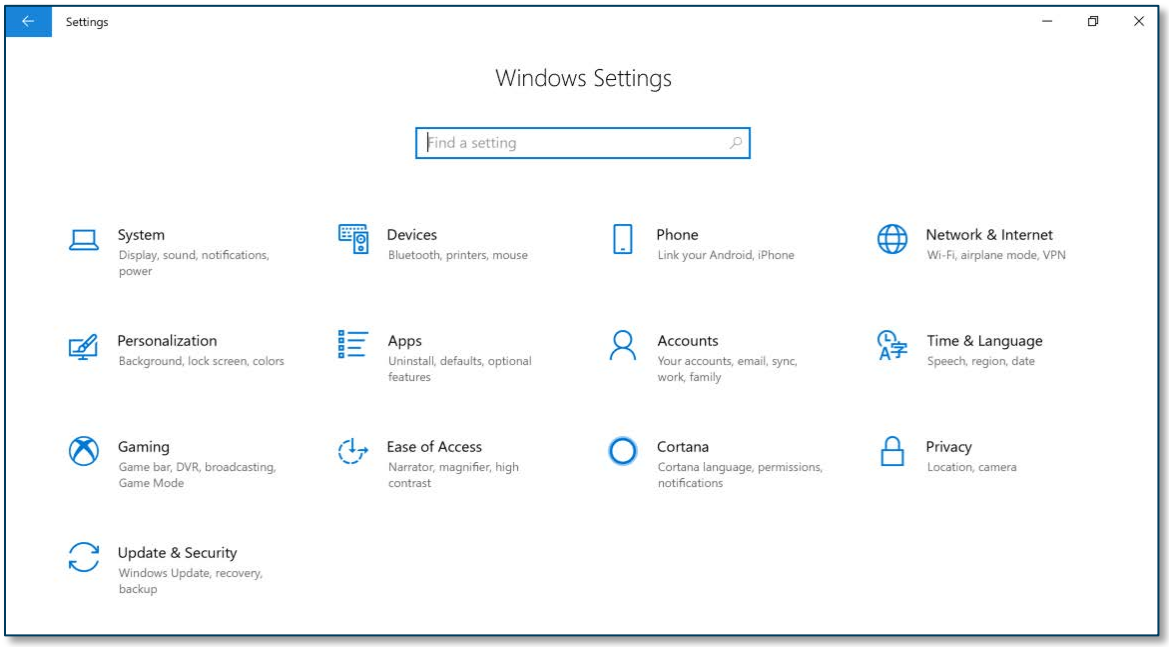


Figure 38 - Windows Settings Home Screen

6. Accounts that have administrative access will indicate “Administrator” under the username.

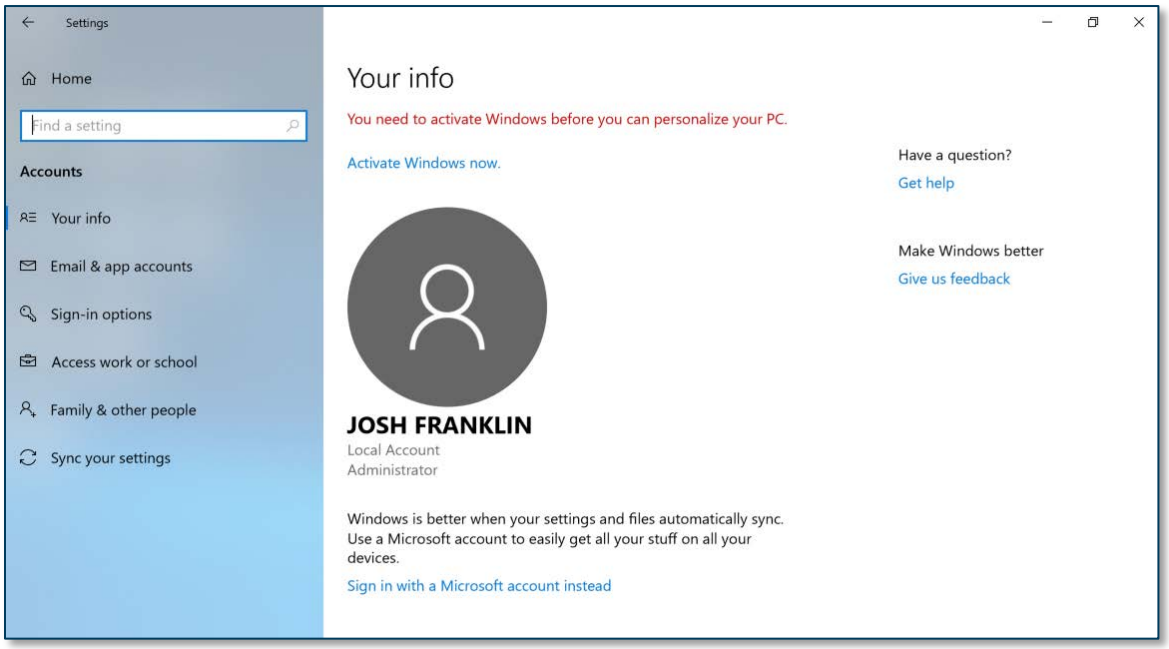


Figure 39 - Account Home Screen

Enabling the System Event Audit Log

This process applies to CIS Control 6.2: Activate Audit Logging. Use these steps to enable the System Event Audit Log.

Note: Enabling system logs on a Windows 10 system can be a complex task. There are hundreds of different types of logs that can all be enabled differently. This guide shows one of many possible methods for enabling system event audit logs. For organizations looking for a simple solution, CIS recommends organizations enable the following logs from the Microsoft Windows basic audit policy located at this link: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.

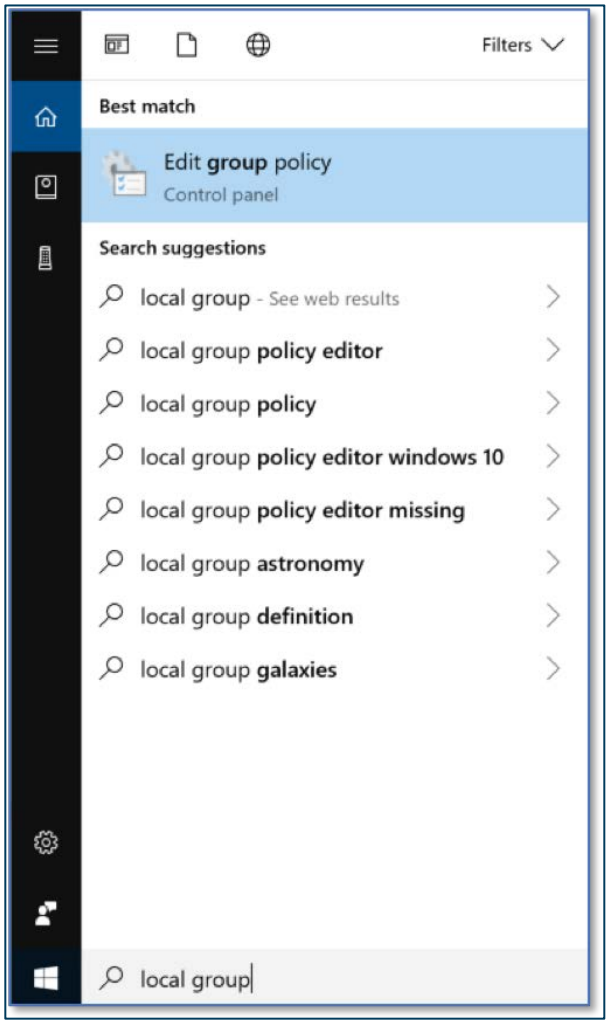


Figure 40 - Searching for LGPE

2. Enter “local group” in the Search field. The search results populate.

3. Select “Edit group policy” in the search list. The *Local Group Policy Editor Home Screen* displays.

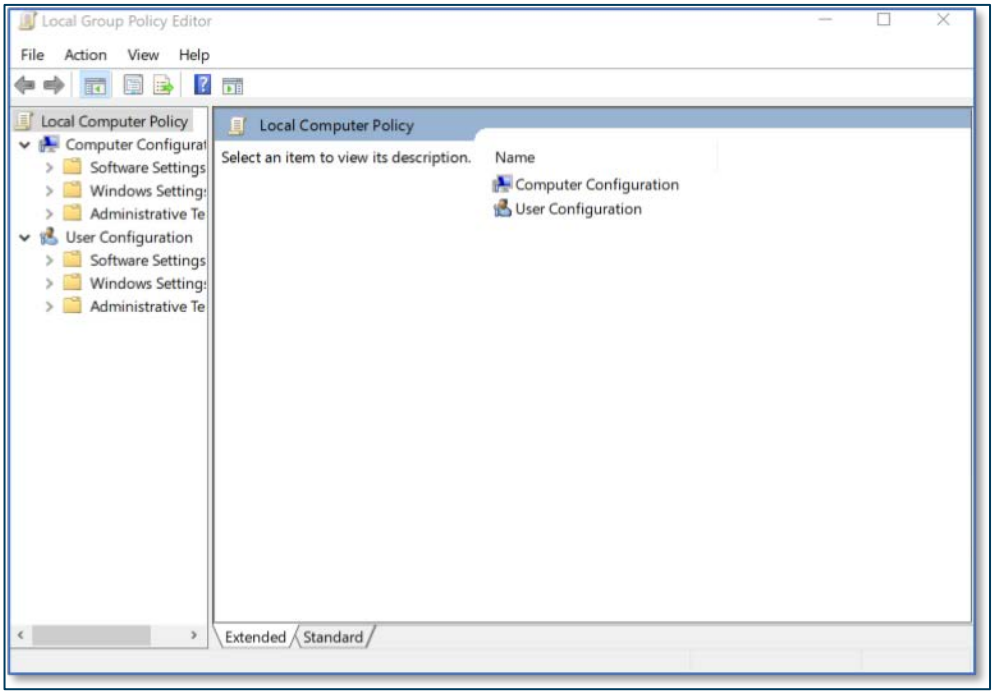


Figure 41 - LGPE Home Screen

4. Under *Computer Configurations*, select *Security Settings*, and then *Advanced Audit Policy Configuration.*

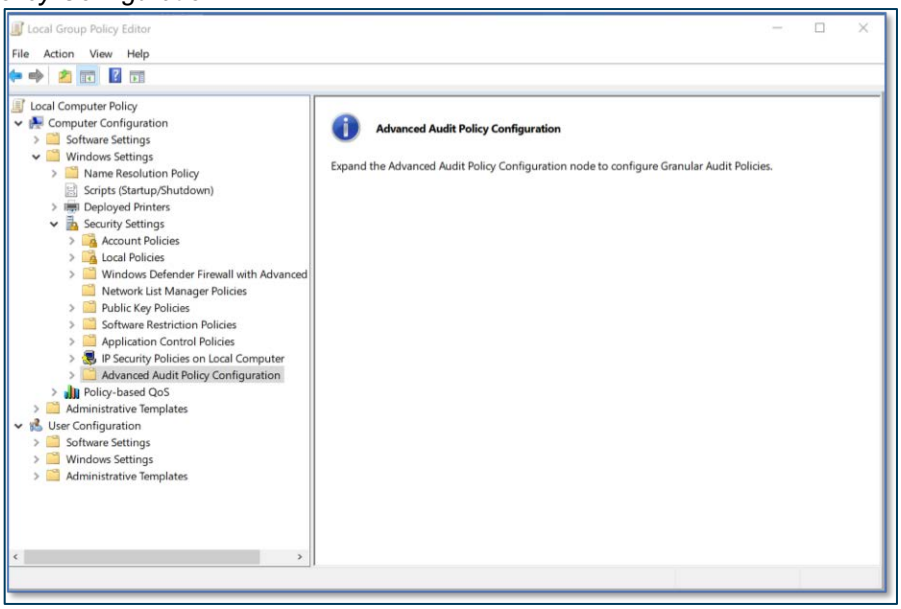


Figure 42 - Advanced Audit Policy Configuration Home Screen

5. Expand *Advanced Audit Policy Configuration* to show *System Audit Policies - Local Group Policy Object*.

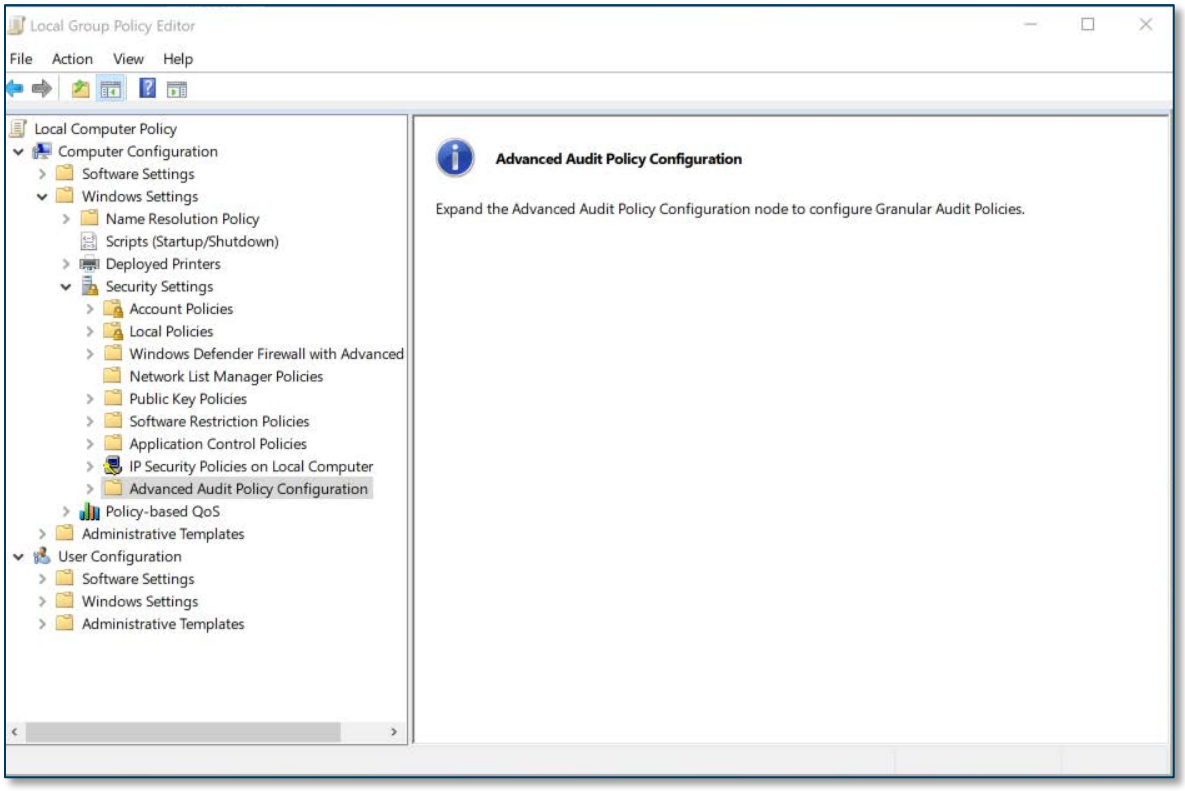


Figure 43 - Advanced Audit Policy Configuration

6. Expand *Advanced Audit Policy Configuration* once more. The system audit policies display.

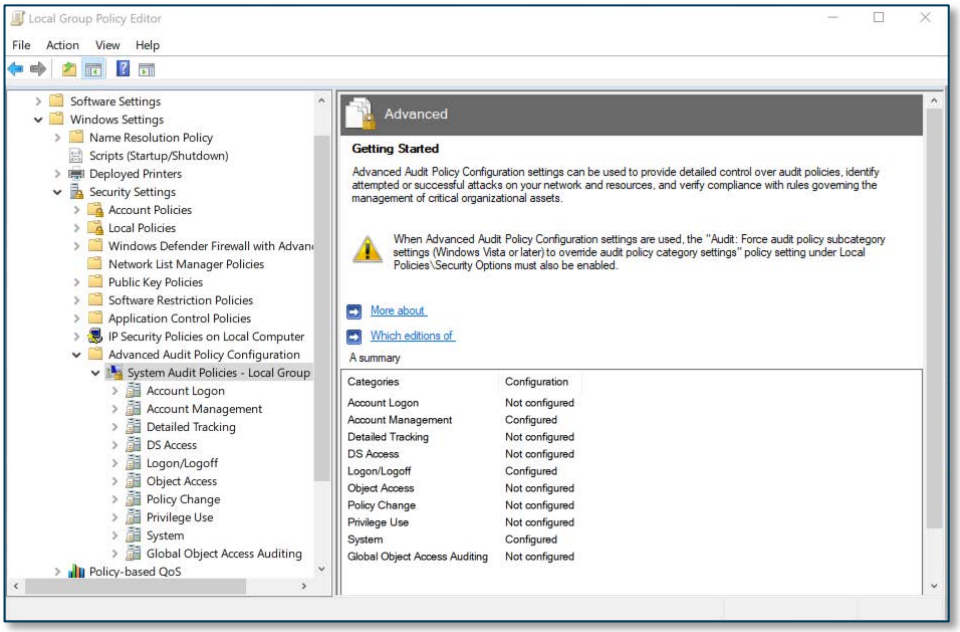


Figure 44 - System Audit Policies

7. Under *Account Logon*, select *Audit Credential Validation*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

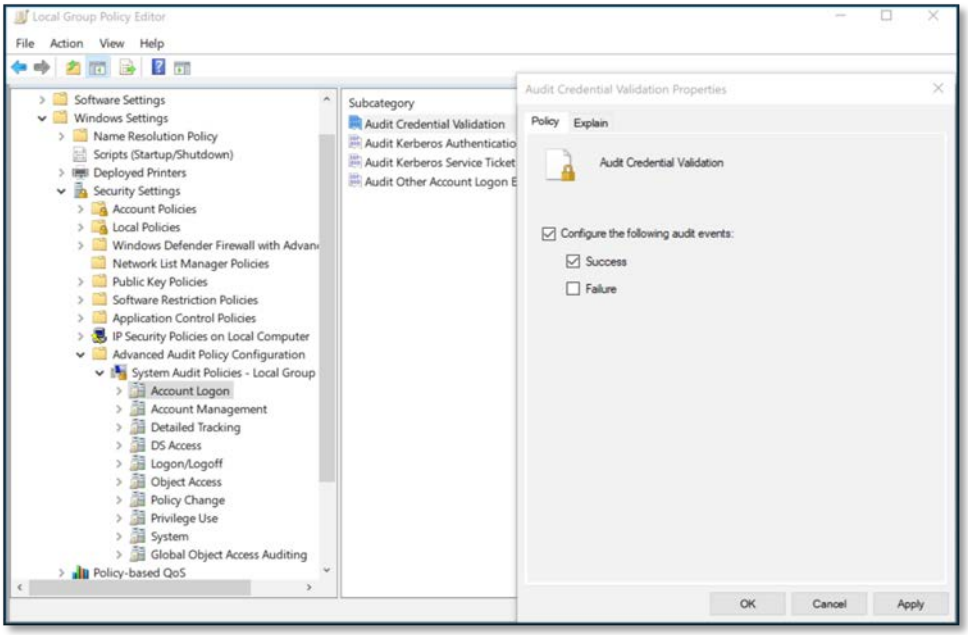


Figure 45 - Audit Credential Validation Policies

8. Under *Account Management*, select *Audit Computer Account Management*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

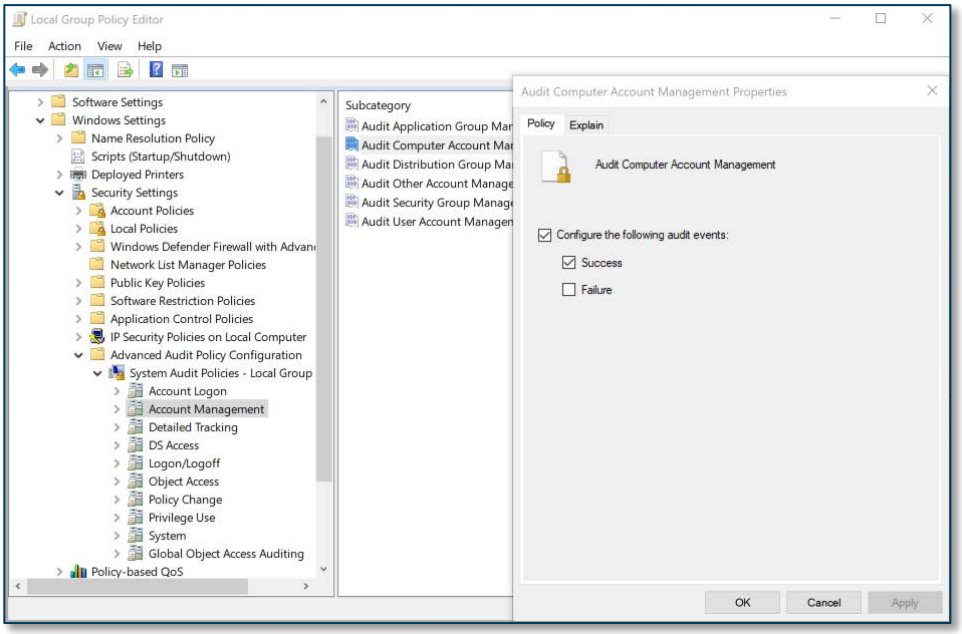


Figure 46 - Audit Computer Account Management

9. Under *Account Management*, select *Audit Other Account Management Events*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

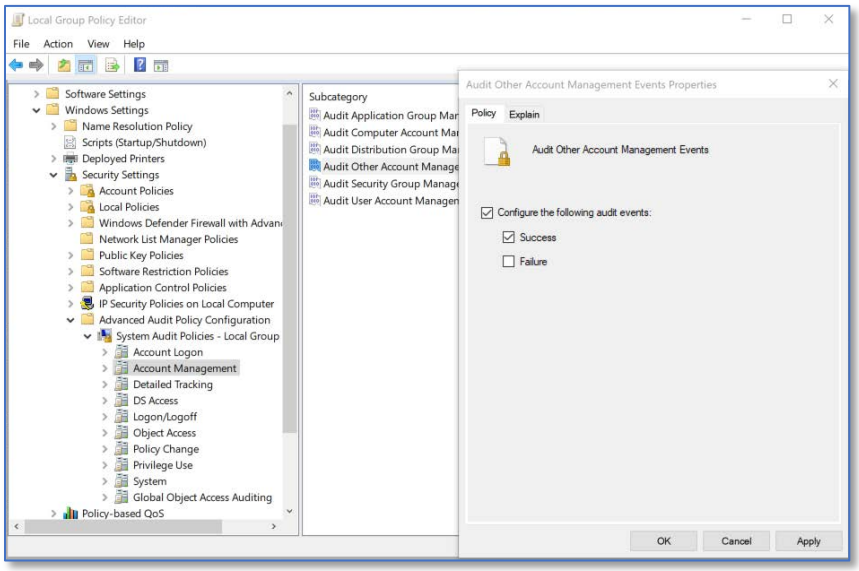


Figure 47 - Audit Other Account Management Events

10. Under *Account Management*, select *Audit Security Group Management*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

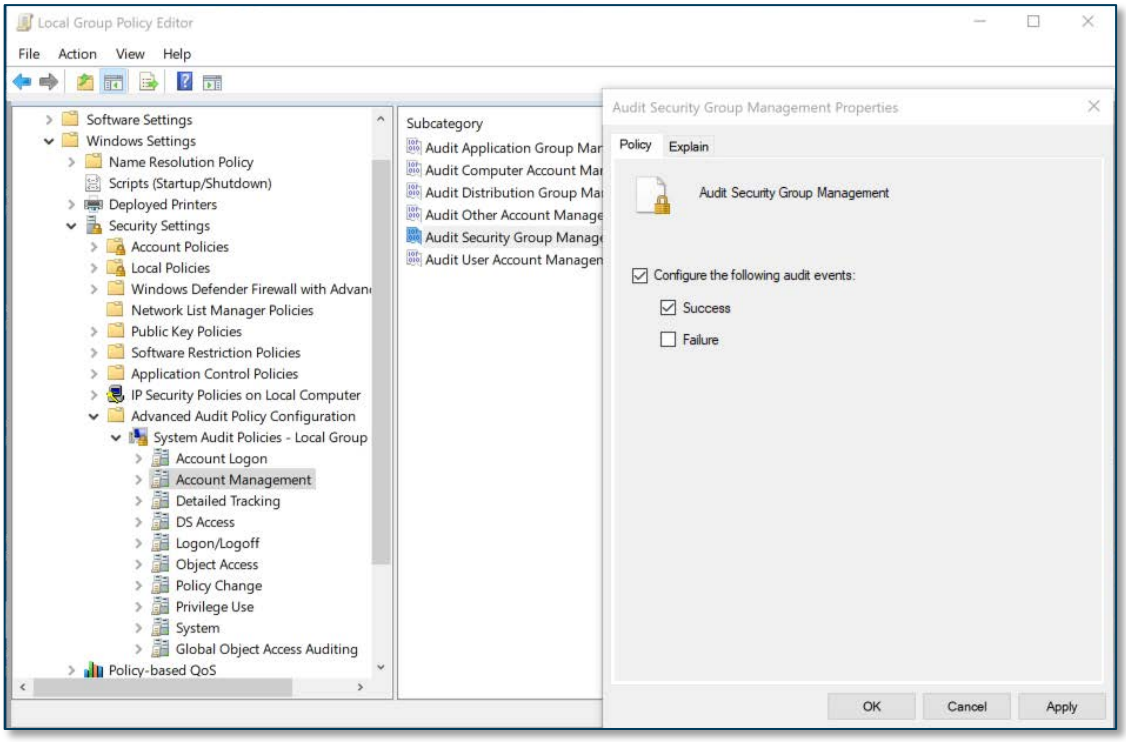


Figure 48 - Audit Security Group Management

11. Under *Account Management*, select *Audit User Account Management*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

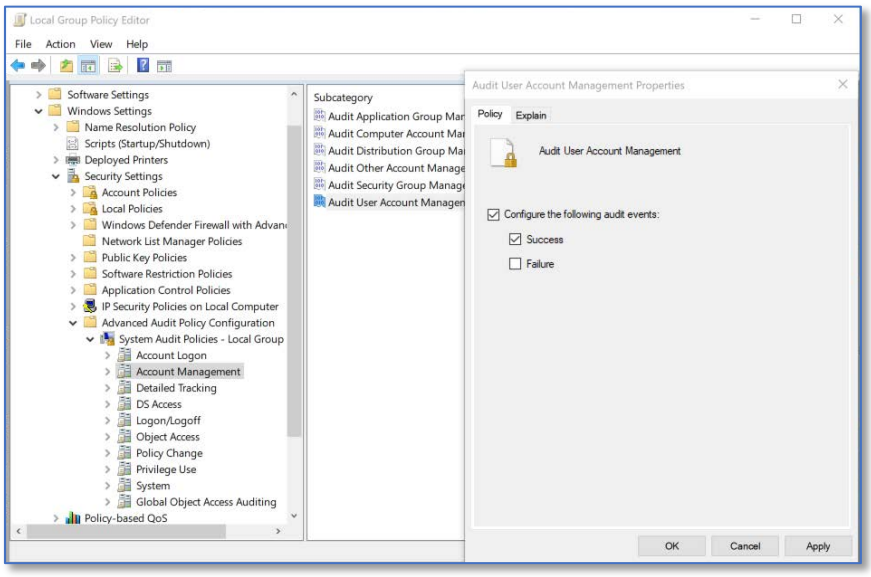


Figure 49 - Audit User Account Management

12. Under *Detailed Tracking*, select *Audit Process Creation*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

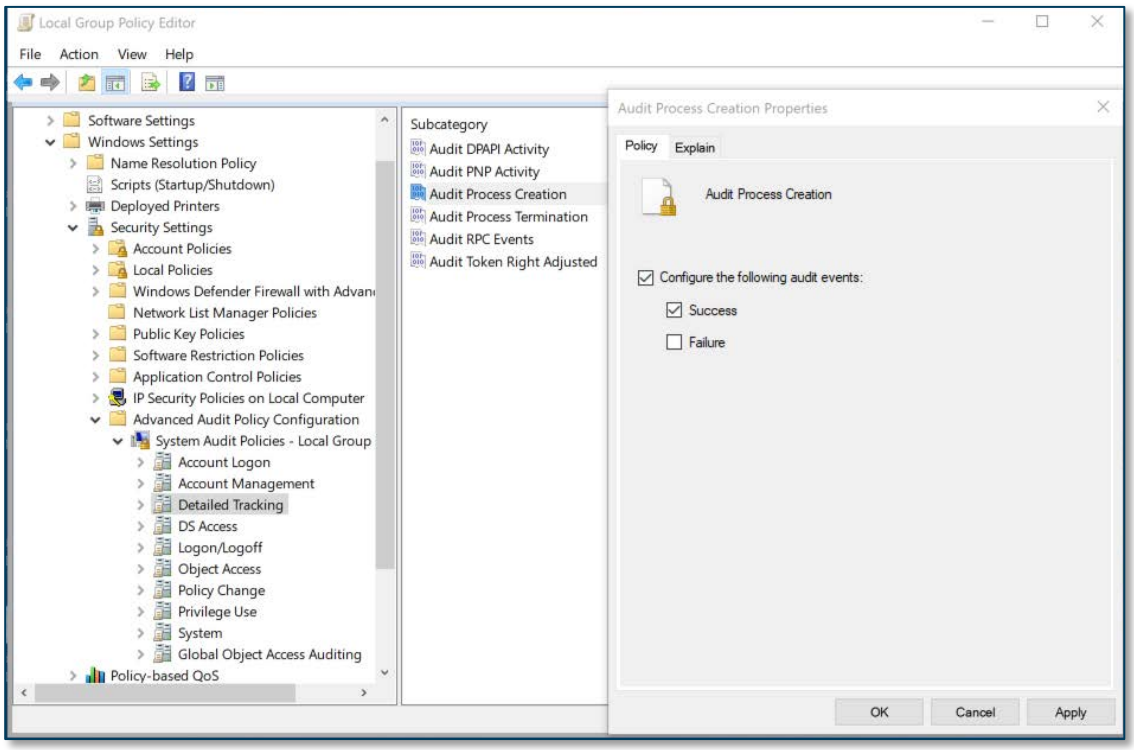


Figure 50 - Audit Process Creation

13. Under *Logon/Logoff*, select *Audit Logoff*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

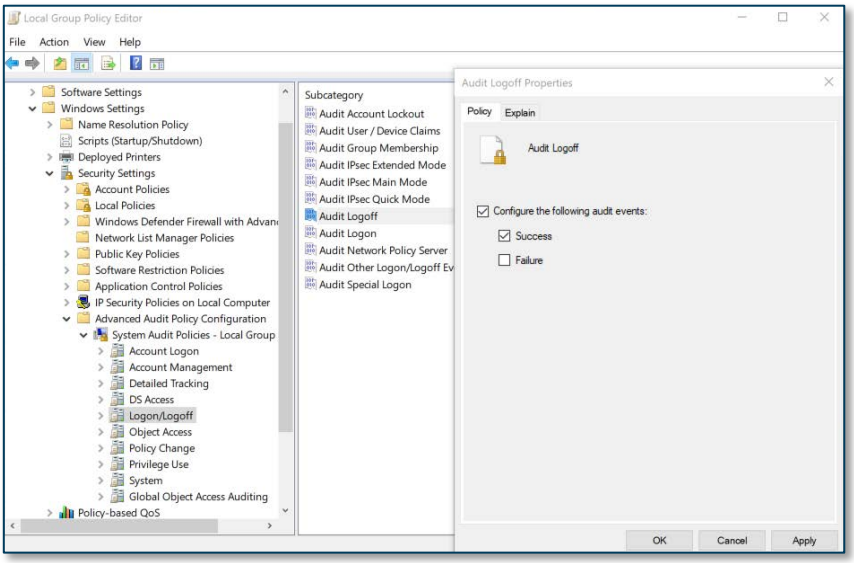


Figure 51 - Audit Logoff

14. Under *Logon/Logoff*, select *Audit Logon*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked. Also ensure that *Failure* is checked.

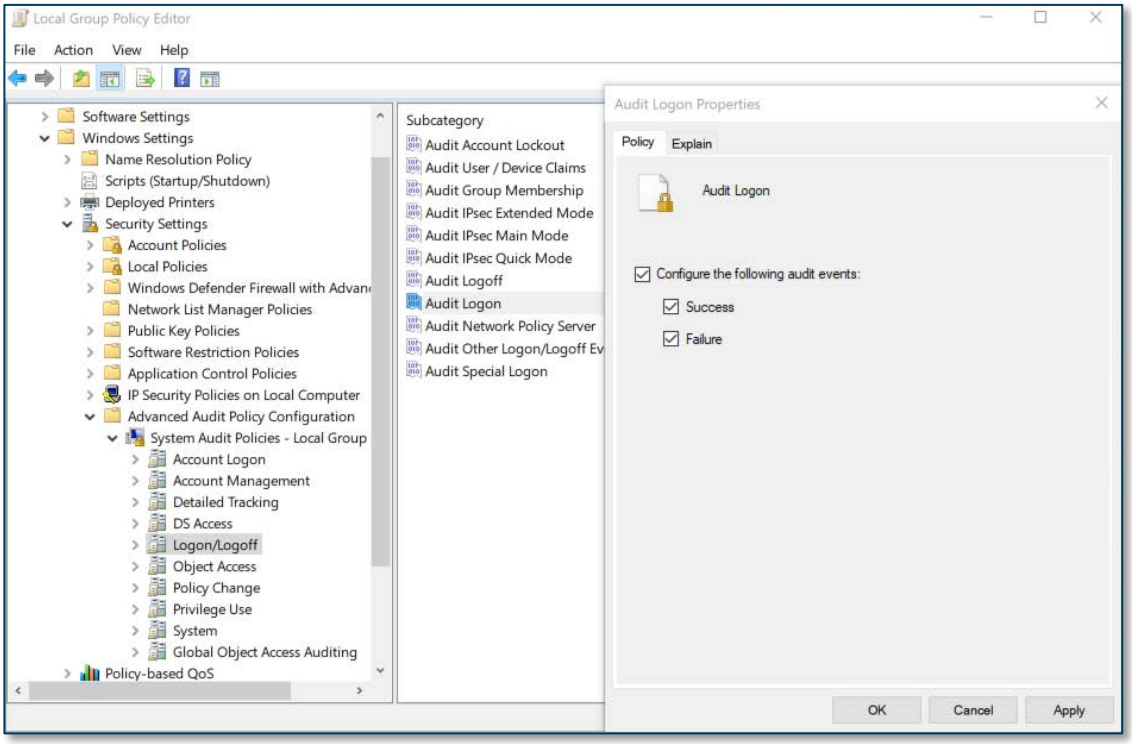


Figure 52 - Audit Logon

15. Under *Logon/Logoff*, select *Audit Special Logon*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

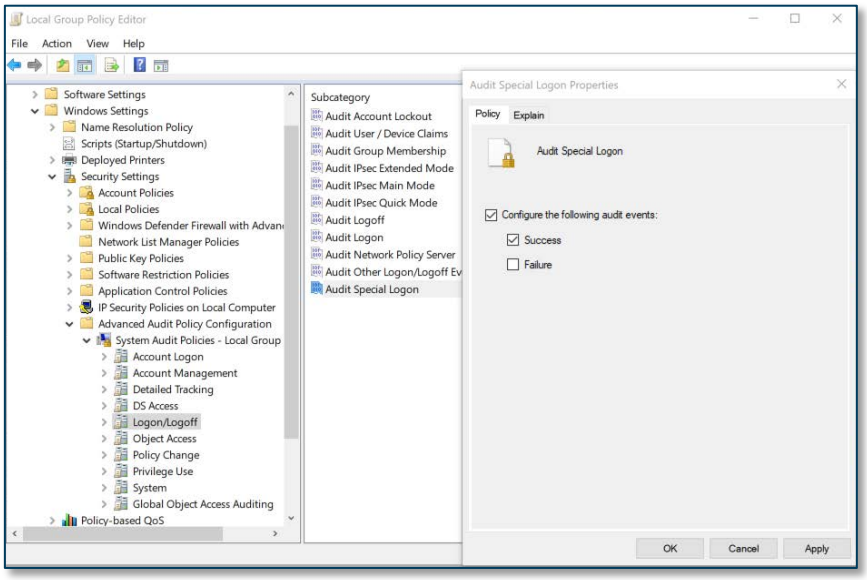


Figure 53 - Audit Special Logon

16. Under *Policy Change*, select *Audit Audit Policy Change*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked. Also ensure that *Failure* is checked.

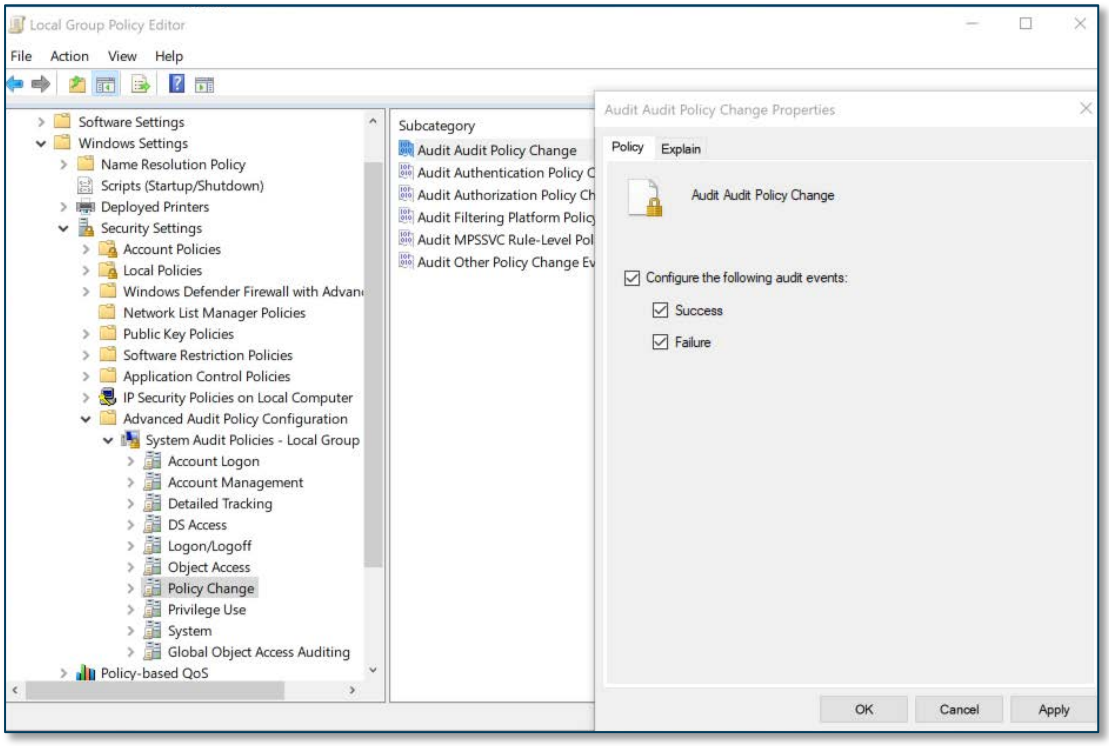


Figure 54 - Audit Audit Policy Change

17. Under *Policy Change*, select *Audit Authentication Policy Change*. Ensure that *Configure the following audit events* is checked, and that *Success* is checked.

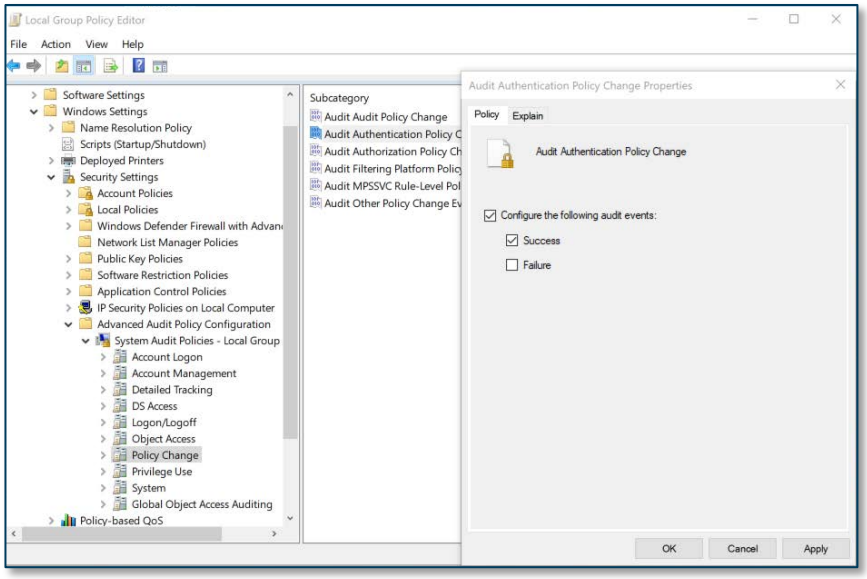


Figure 55 - Audit Authentication Policy Change

18. Under *System*, select *Audit IPsec Driver*. Ensure that *Configure the following audit events* is checked, *Success* is checked, and *Failure* is checked.

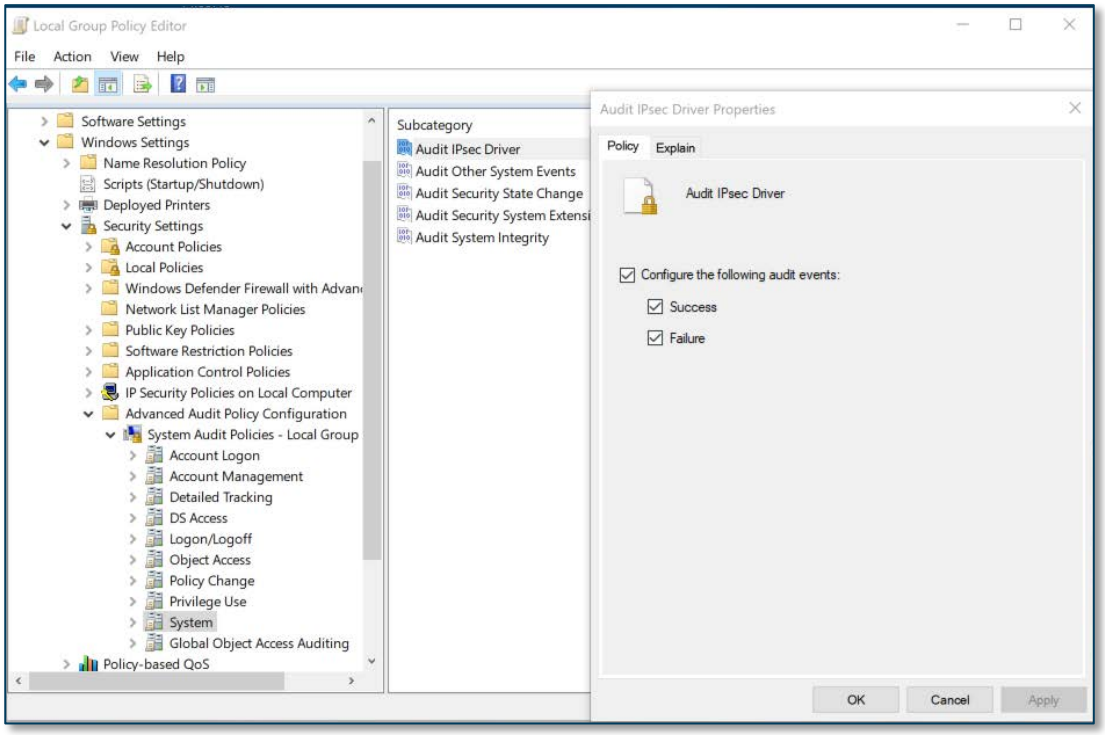


Figure 56 - Audit IPsec Driver

19. Under *System*, select *Audit Security State Change*. Ensure that *Configure the following audit events* is checked, *Success* is checked, and *Failure* is checked.

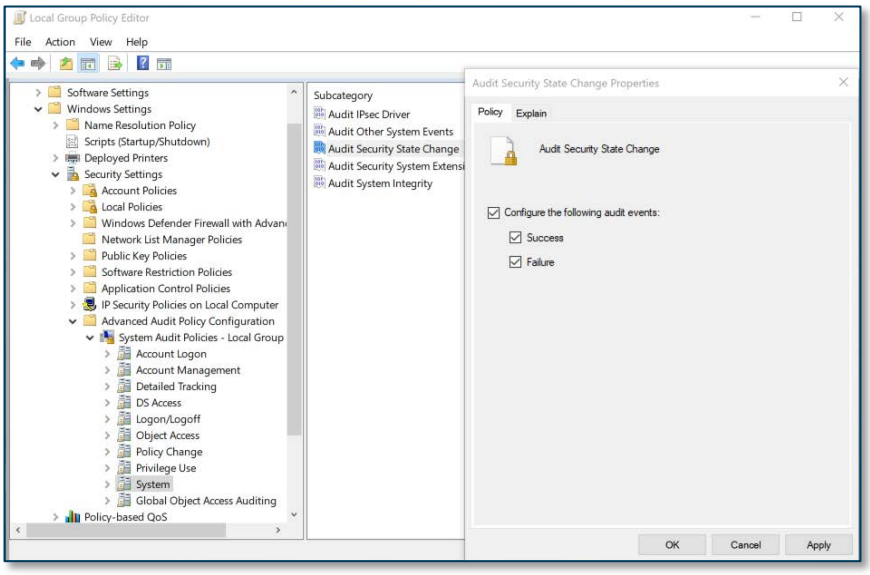


Figure 57 - Audit Security State Change

20. Under *System*, select *Audit Security System Extension*. Ensure that *Configure the following audit events* is checked, *Success* is checked, and *Failure* is checked.

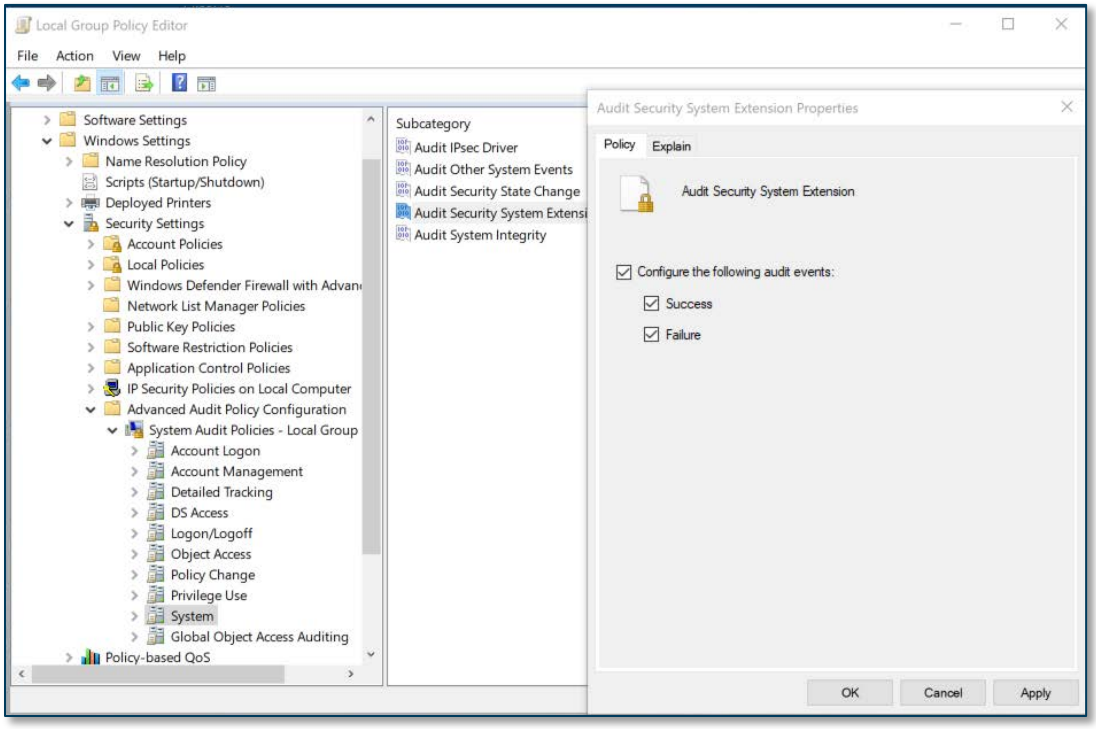


Figure 58 - Audit Security System Extension

21. Under *System*, select *Audit System Integrity*. Ensure that *Configure the following audit events* is checked, *Success* is checked, and *Failure* is checked.

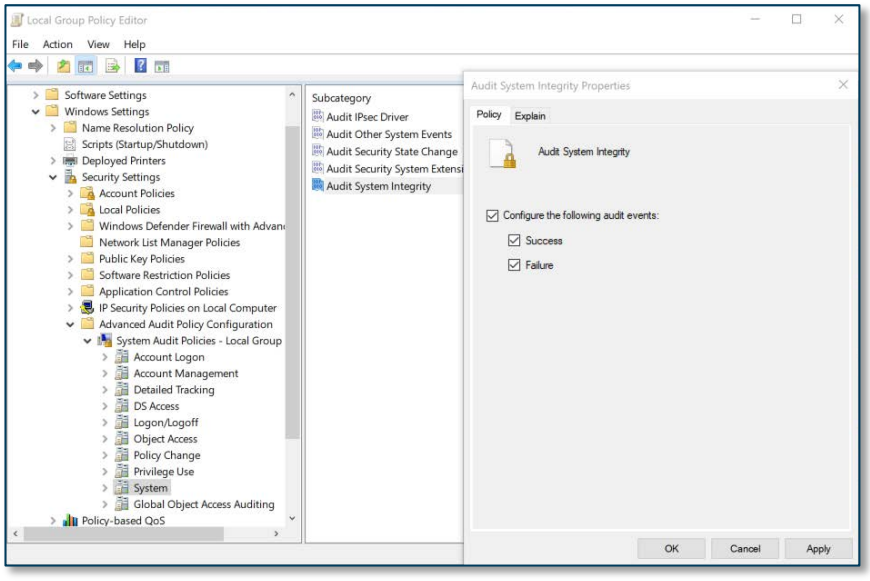


Figure 59 - Audit System Integrity

For those interested in implementing all of the logging requirements required for larger organizations, that information is available within the CIS Windows 10 Benchmark.

In the Windows search bar with the magnifying glass icon, type *local group* to open the Local Group Policy Editor.

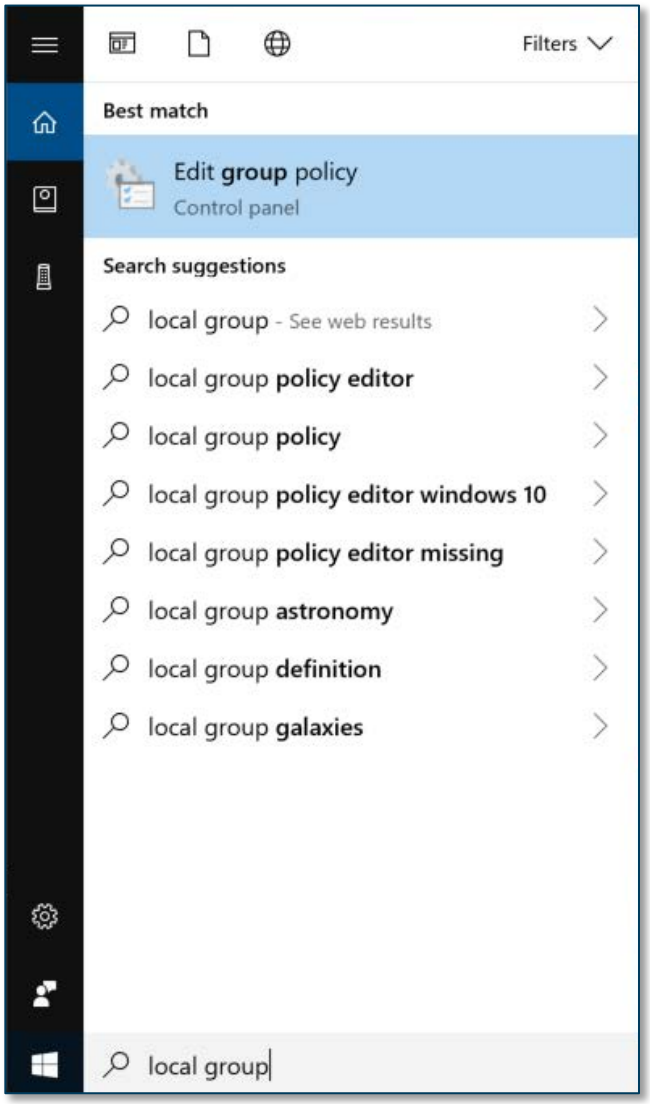


Figure 60 - Searching for the LGPE

Checking Windows Defender Security Center

This process applies to CIS Control 8.2: Ensure Anti-Malware Software and Signatures Are Updated

Note: Windows Defender is enabled in Windows 10 by default. The following steps help to ensure that Windows Defender is properly enabled and the defaults have not been changed. This is not a substitute for configuring Windows Defender via the Windows LGPE. This is shown on the next page of this document.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “windows defender” in the search field. Windows displays search results.
3. Select the Windows Defender App. The “Security at a Glance” window opens with status for monitored areas.

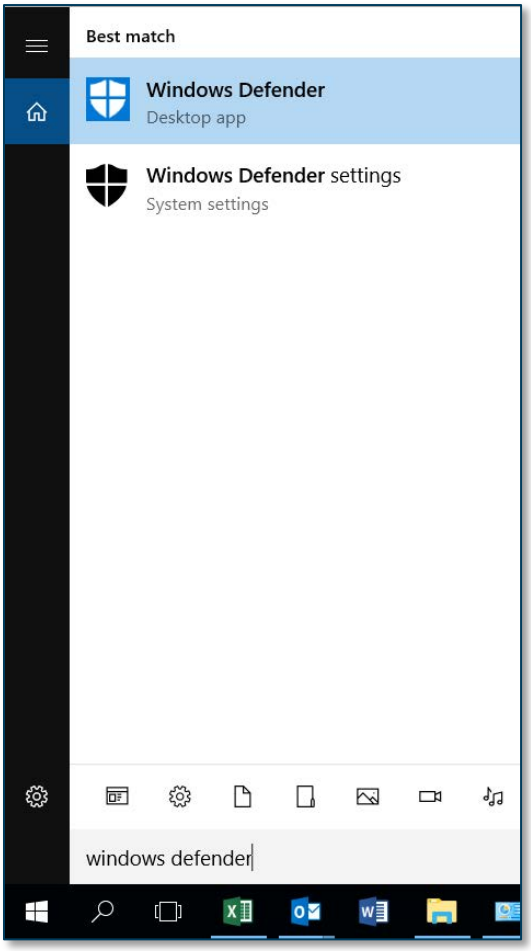


Figure 61 - Searching for Windows Defender

4. Any items that need to be reviewed will have an exclamation point within a triangle under the icon.

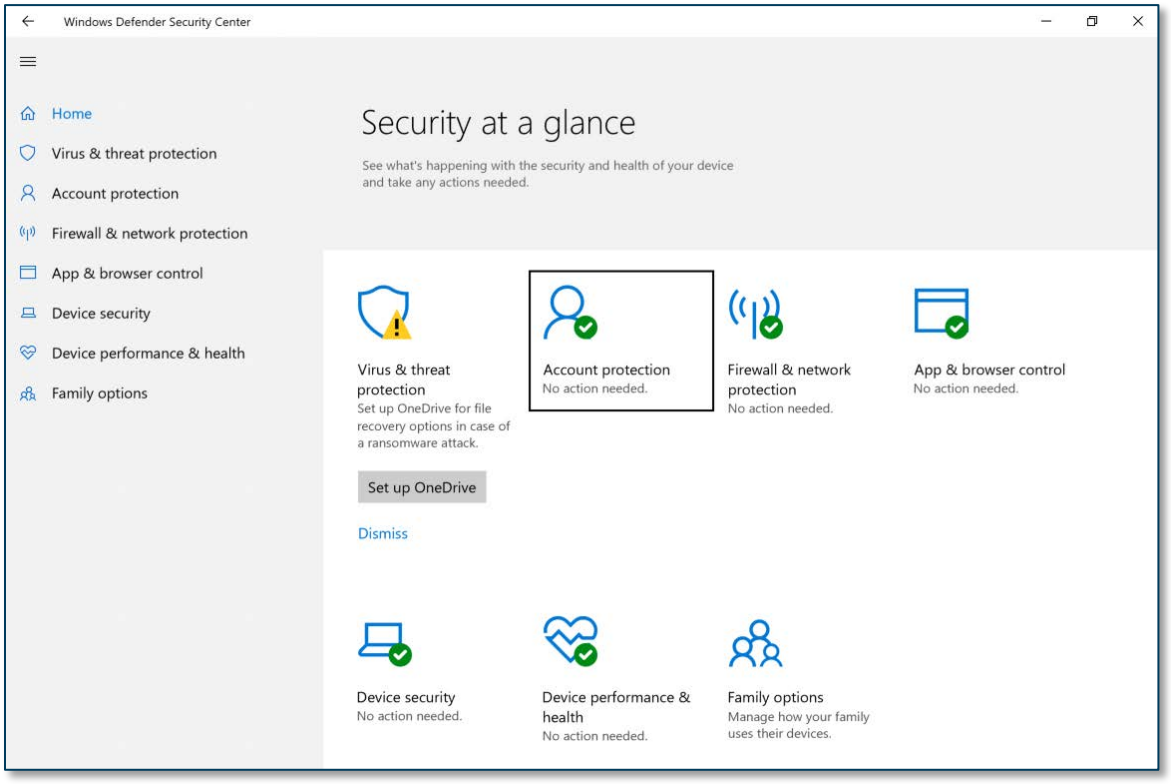


Figure 62 - Windows Defender Security Center Home Screen

Enabling Windows Defender Security Center via LGPE

This control applies to CIS Control 8.2: Ensure Anti-Malware Software and Signatures Are Updated

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter ‘local group” in the search field. Search options populate for “local group”.

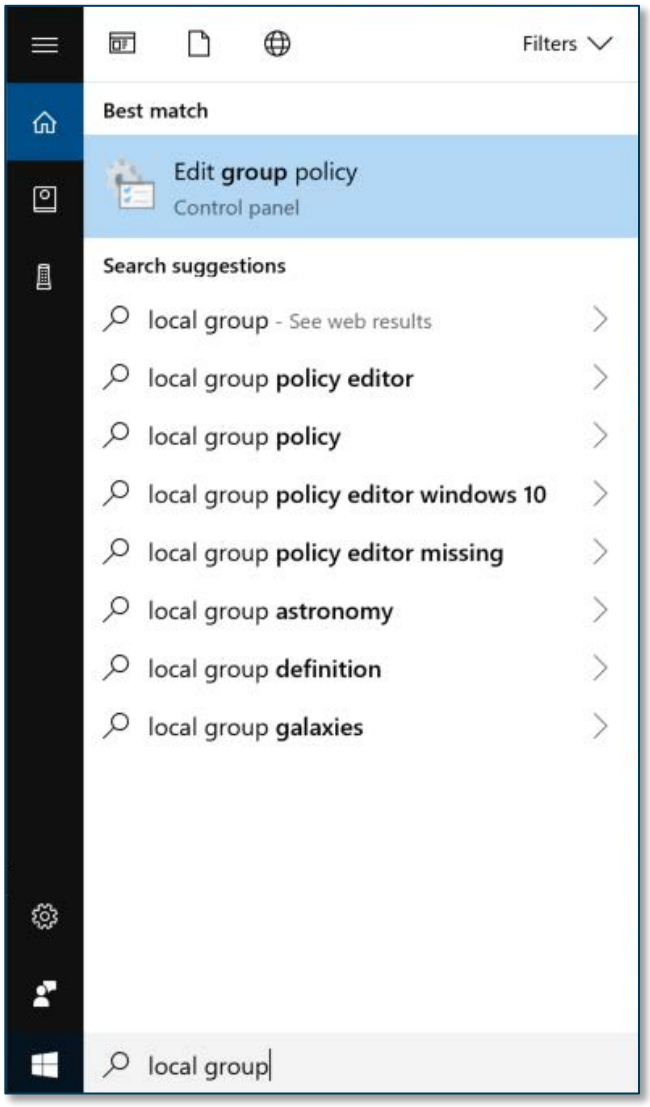


Figure 63 - Searching for the LGPE

3. Select “Edit group policy” in the search list. The *Local Group Policy Editor Home Screen* displays.

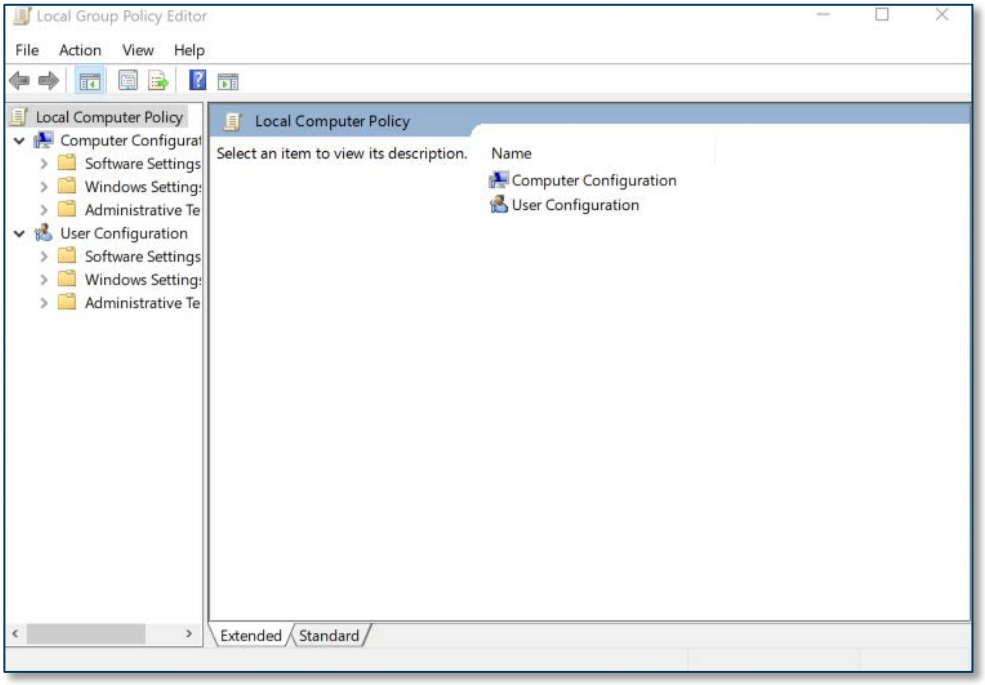


Figure 64 - LGPE Home Screen

4. Select *Computer Configuration* and expand *Administrative Templates*. The *Administrative Templates* subfolders display.

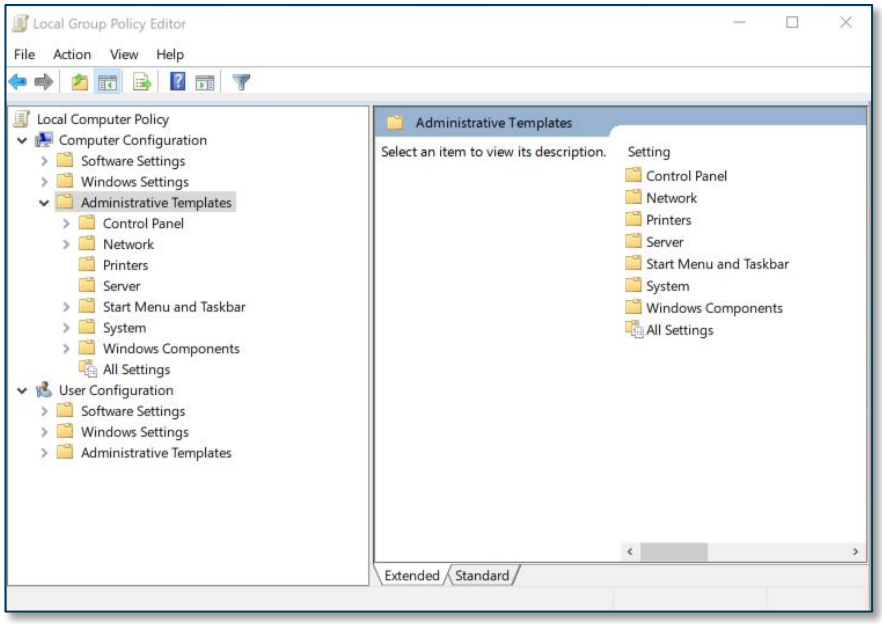


Figure 65 - LGPE Administrative Templates

5. Expand *Windows Components* and then *Windows Defender Antivirus*.

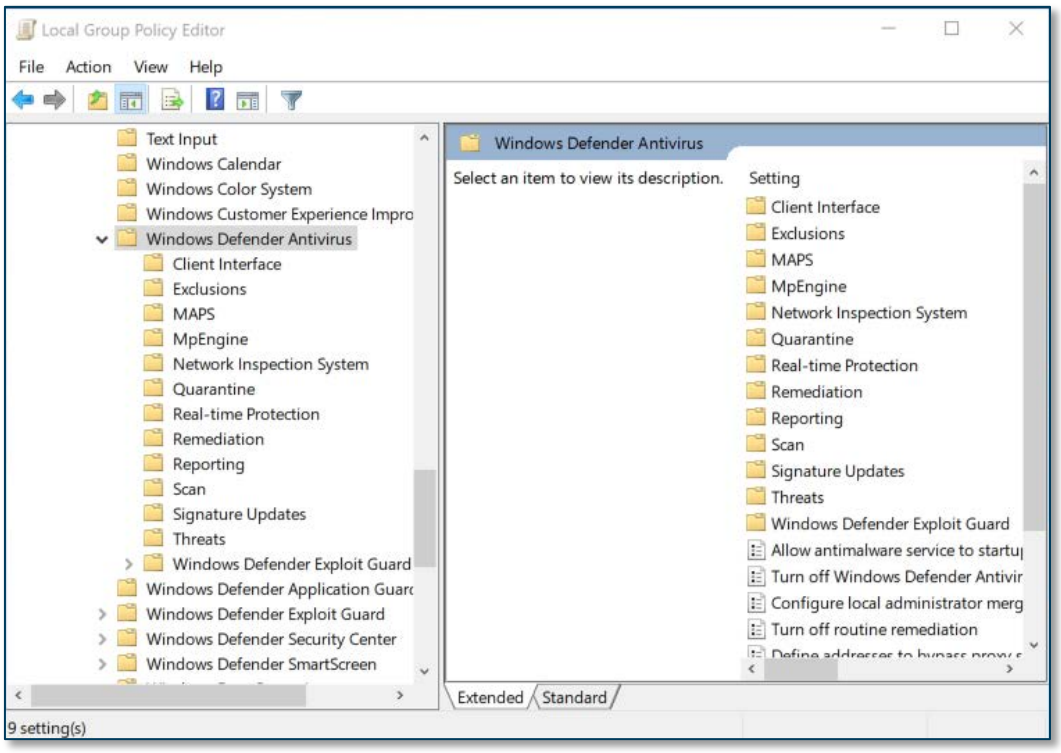


Figure 66 - LGPE Windows Defender Antivirus

6. Double click *Turn off Windows Defender Antivirus* and ensure *Disabled* is selected. Windows Defender Antivirus is enabled by default. This prevents it from being disabled by a user.

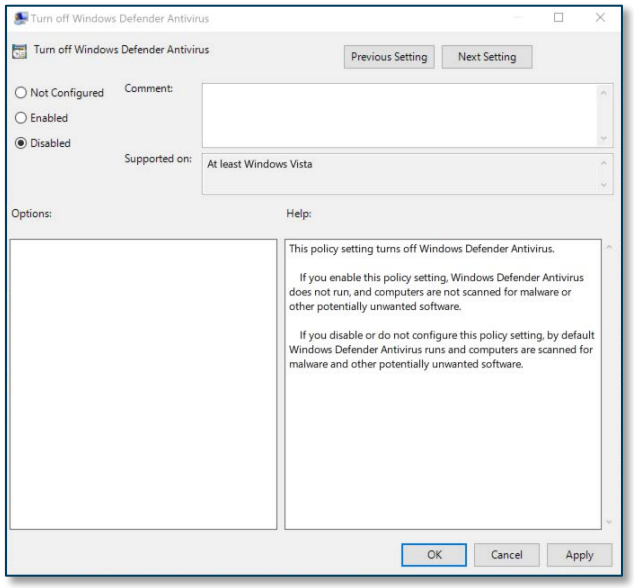


Figure 67 - Windows Defender Antivirus Settings

Note: Additional actions are required.

7. Click the blue back arrow in the top left of the *Local Group Policy Editor* and select *Real-time Protection*, followed by *Turn off real-time protection.*

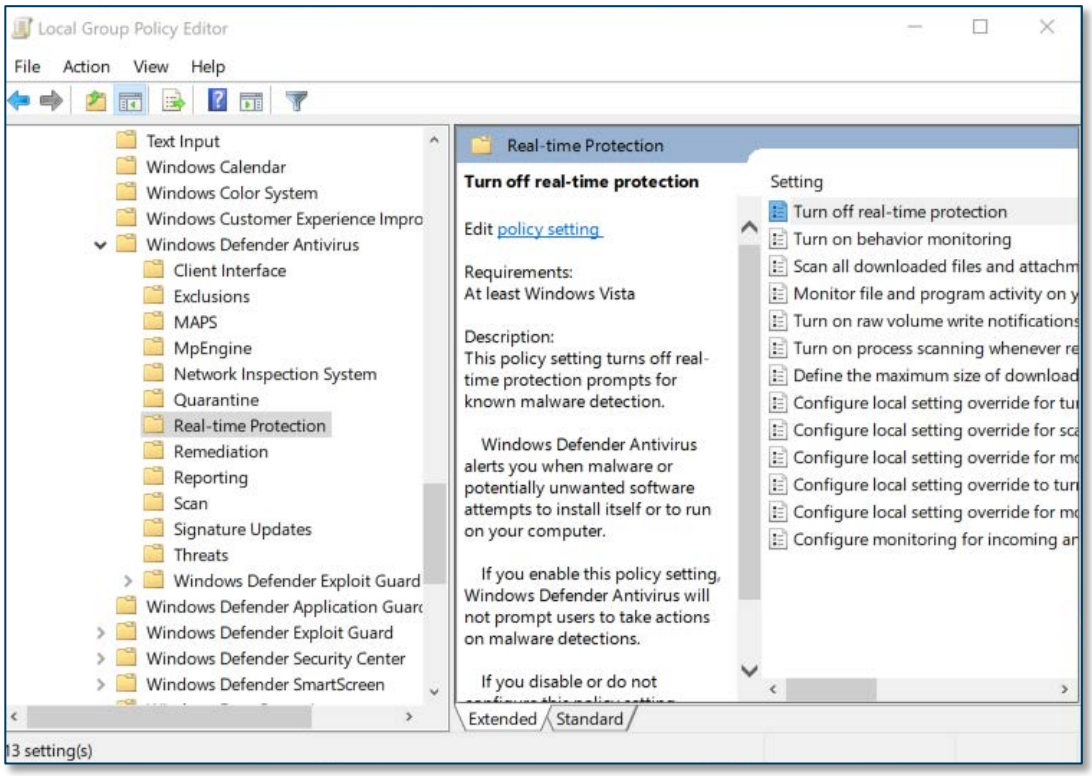


Figure 68 – LGPE Real-time Protection

8. Ensure that *Turn off real-time protection* is *Disabled*. This prevents the application from being disabled.

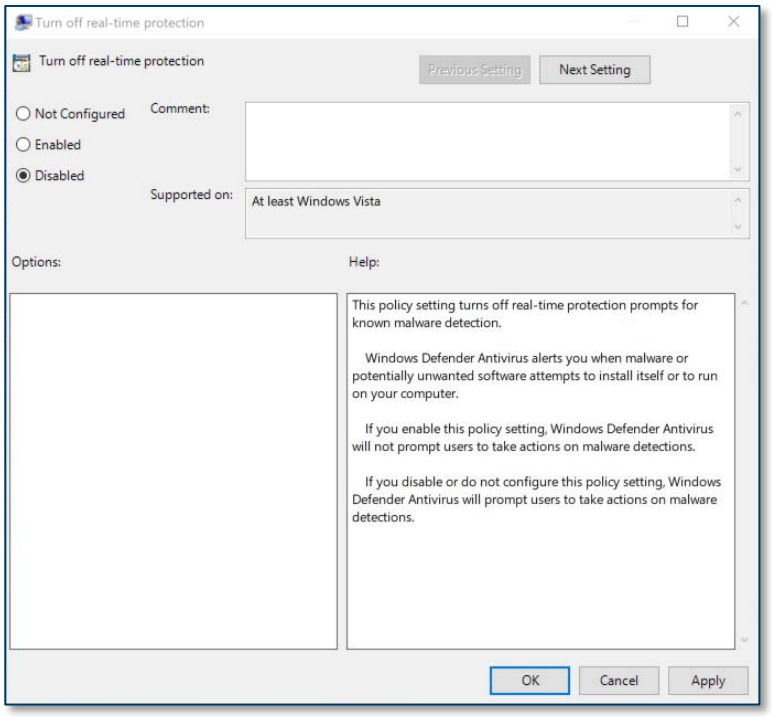


Figure 69 - Real-time Protection Settings

Scanning Removable Devices via LGPE

This process applies to CIS Control 8.4: Configure Anti-Malware Scanning of Removable Media. Use these steps to scan removable devices using LGPE.

1. Click the Windows *Start* button. The Windows Start menu displays with search bar.
2. Enter “local group” in the search bar. Search options populate for “local group”.

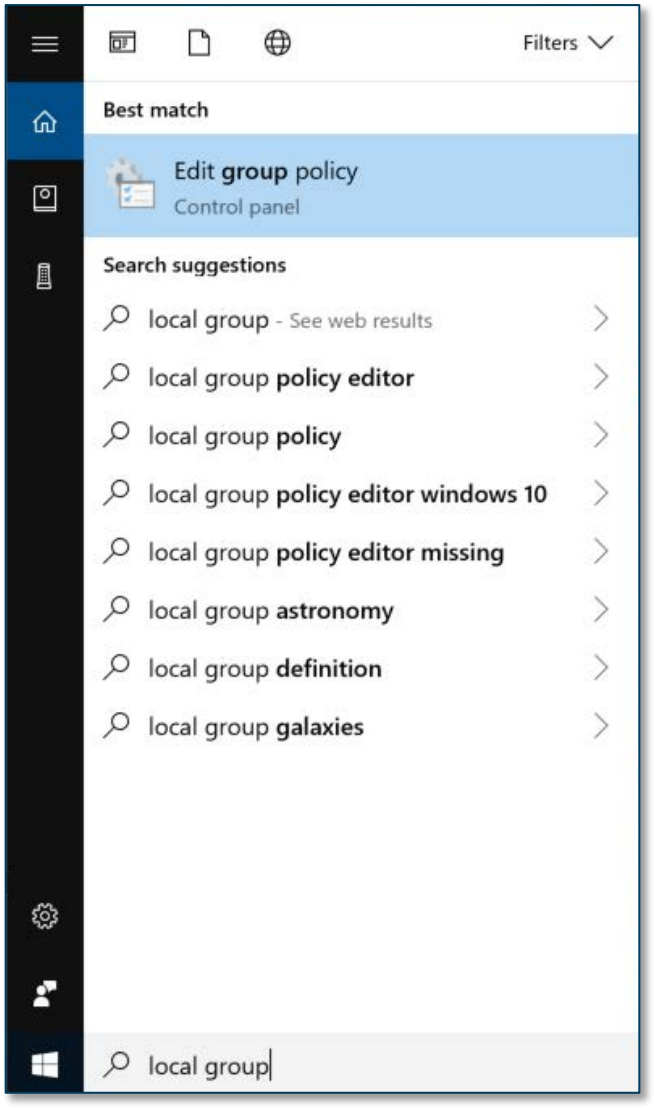


Figure 70 - Searching for the LGPE

3. Select “Edit group policy” in the search list. The *LGPE Home Screen* displays.

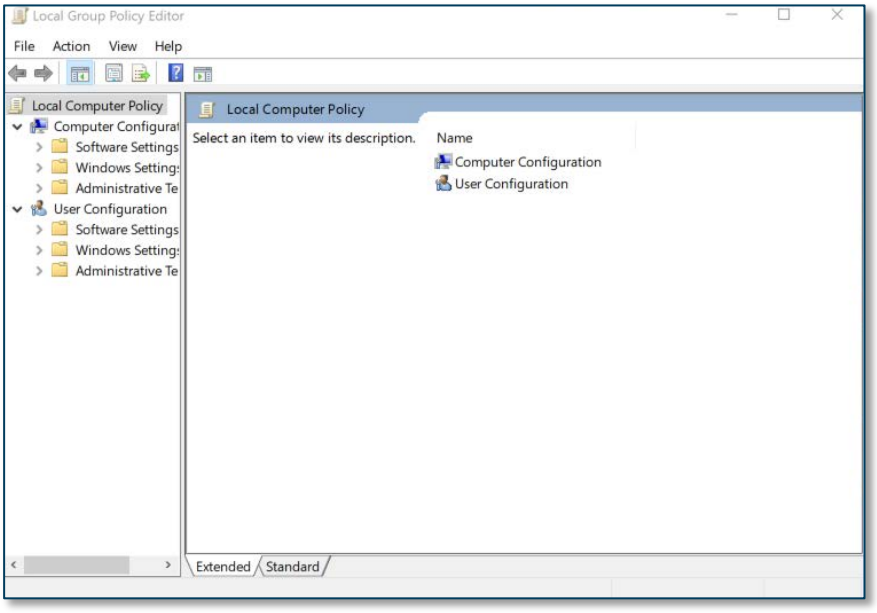


Figure 71 - LGPE Home Screen

4. Select *Computer Configuration* and expand *Administrative Templates*. The *Administrative Templates* subfolders display.

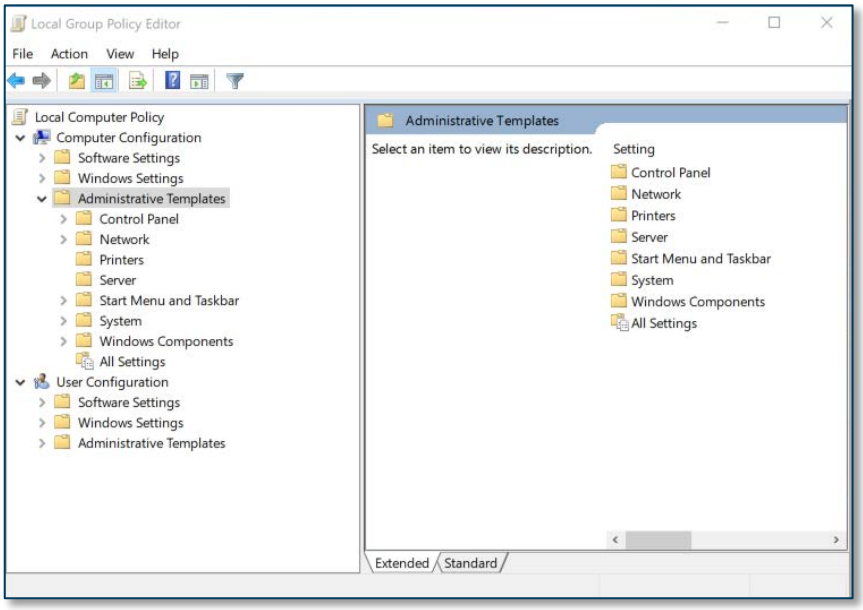


Figure 72 - LGPE Administrative Templates

5. Expand *Windows Components* and then select *Windows Defender Antivirus*.

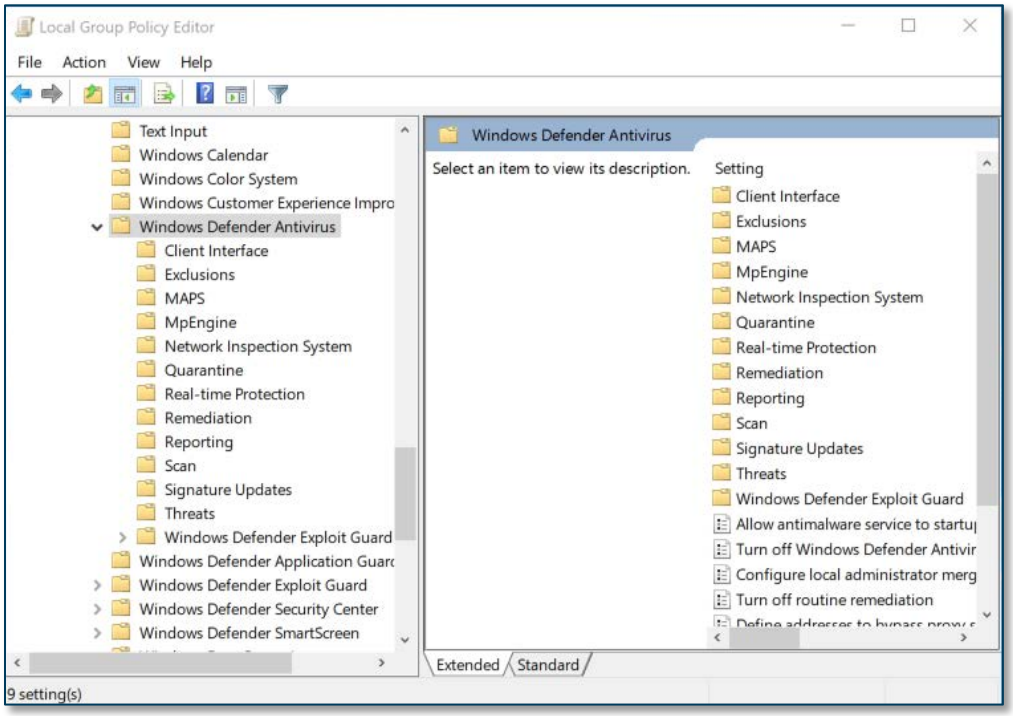


Figure 73 - LGPE Windows Defender Antivirus

6. Select *Scan* and double click *Scan removable drives*. The *Scan Removable Drives* folder opens.

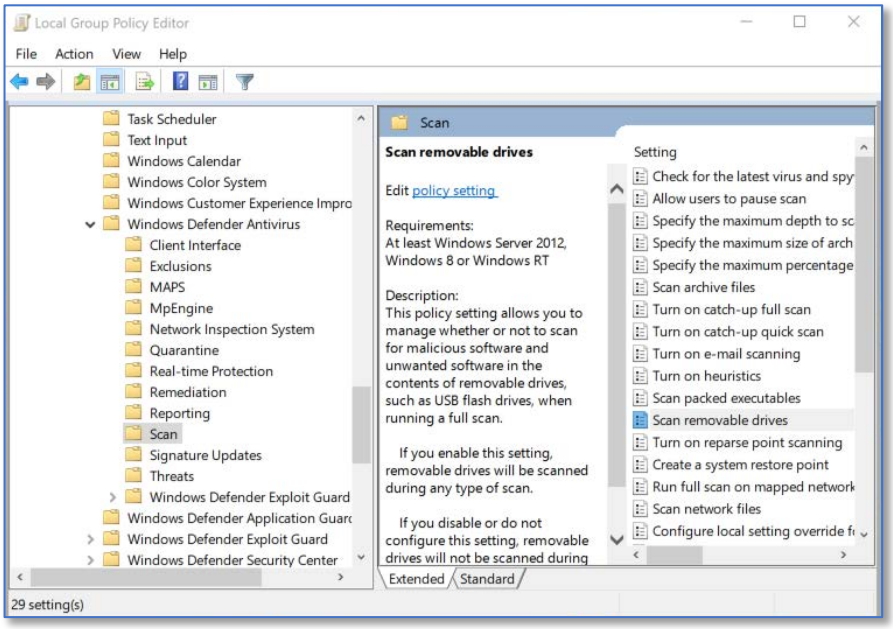


Figure 74 - LGPE Windows Defender Antivirus Scan

7. Ensure the scan removable drives setting is set to *Enabled*. Note that this will not automatically scan any inserted device. Instead, if a Windows Defender Antivirus scan is run while a removable drive is inserted, that drive will also be within scope of the scan.

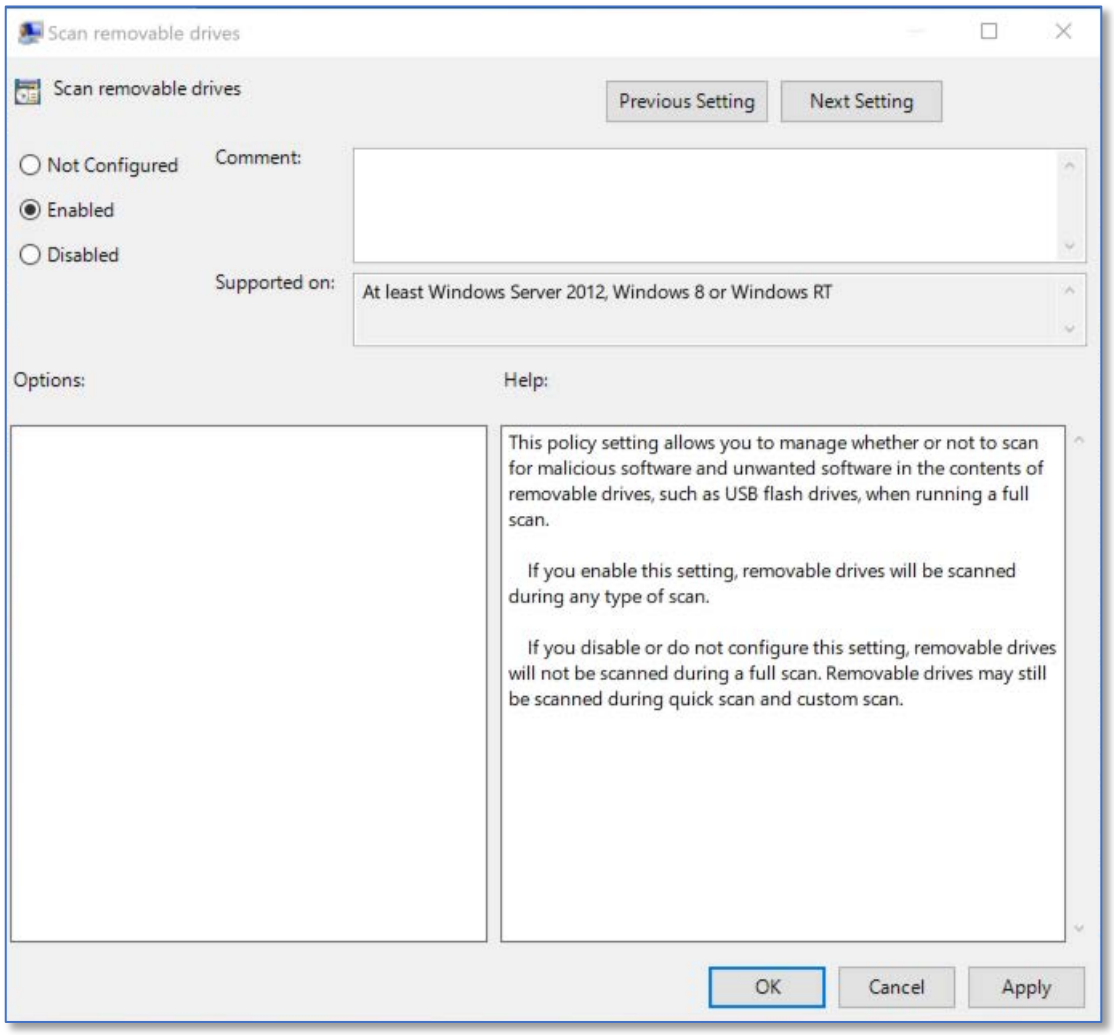


Figure 75 - Windows Antivirus Scan Settings

Configuring AutoPlay via Windows Control Panel

This process applies to CIS Control 8.5: Configure Devices to Not Auto-Run Content.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “settings” in the search field.
3. Click the search icon. Windows search options for “settings”.

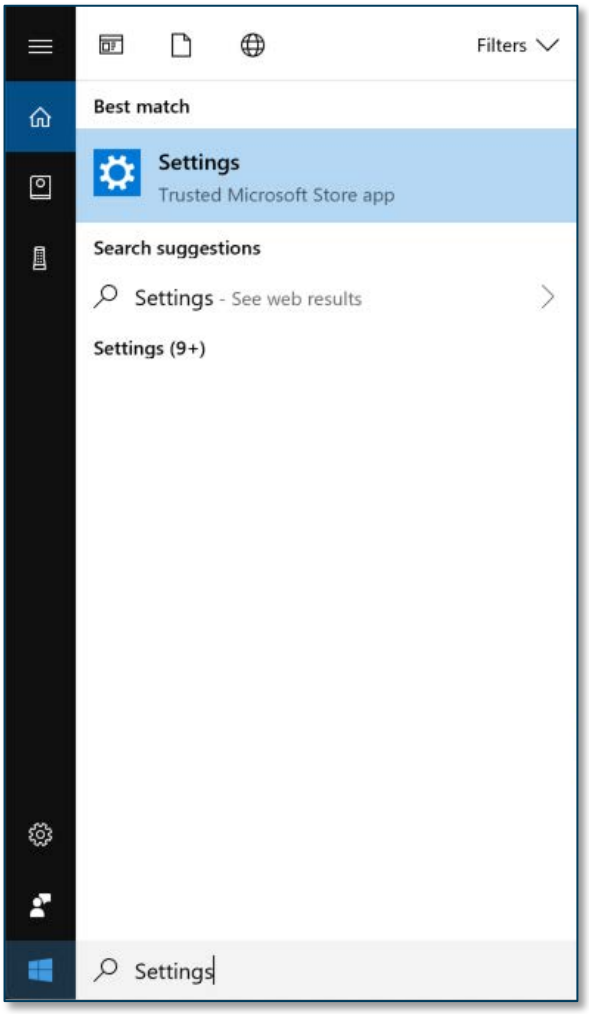


Figure 76 - Searching for Windows Settings

4. Select the *Settings* app. The Windows Settings window opens.

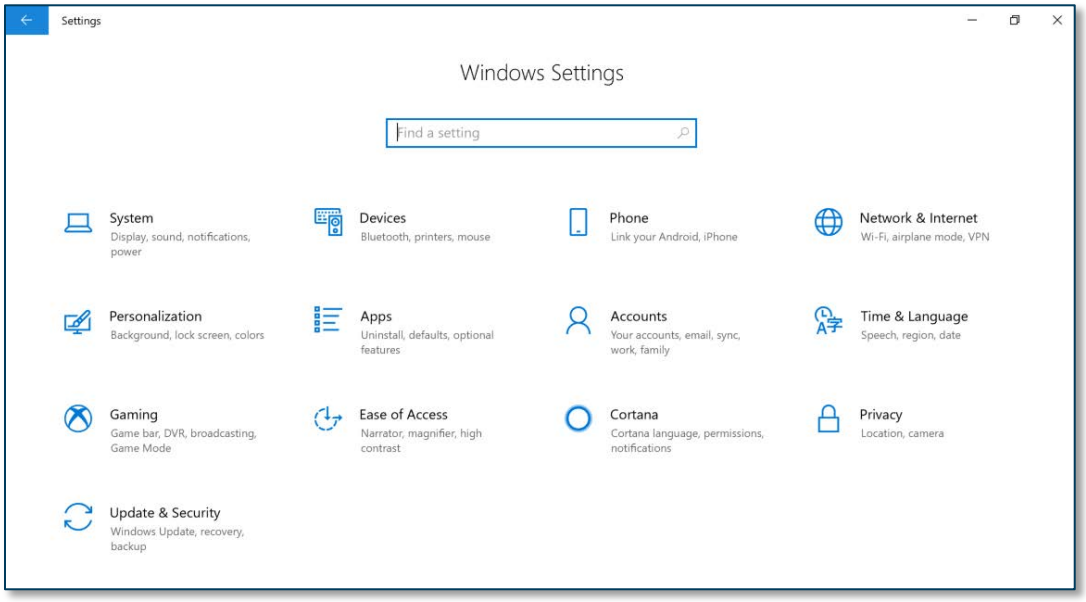


Figure 77 - Windows Settings Home Screen

5. Select *Devices*. The *Bluetooth and Other Devices* screen opens.

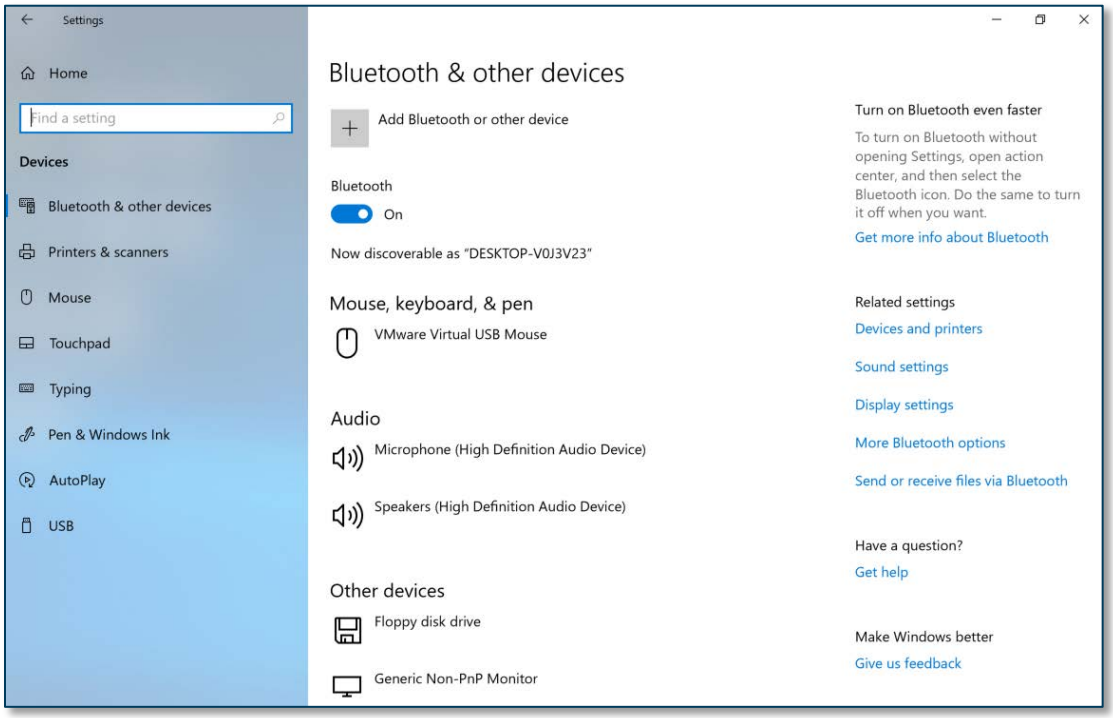


Figure 78 - Bluetooth and Other Devices Settings

6. Select *AutoPlay*. The AutoPlay screen opens.

7. Ensure that AutoPlay is turned *off.*

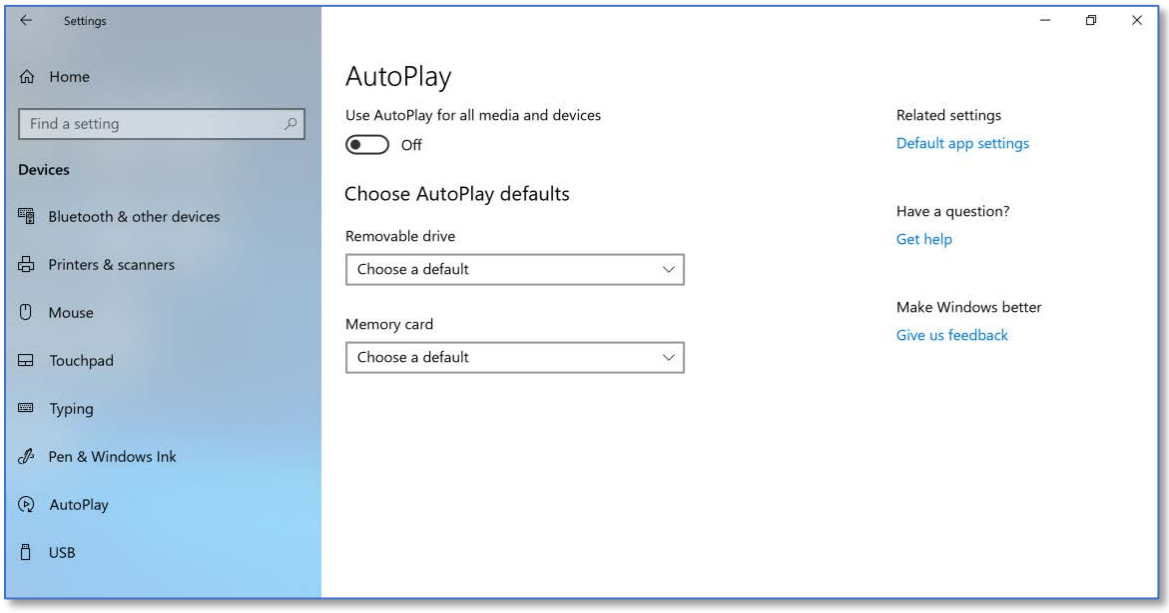


Figure 79 - AutoPlay Settings

Configuring AutoPlay via LGPE

This process applies to CIS Control 8.5: Configure Devices to Not Auto-Run Content. Use these steps to configure AutoPlay via LGPE.

Note: Alternatively, the *Local Group Policy Editor* can be used to configure the Windows 10 AutoPlay setting.

1. Click the Windows *Start* button. The Windows Search menu displays.
2. Enter “local group” in the search field. Search options populate for “local group”.

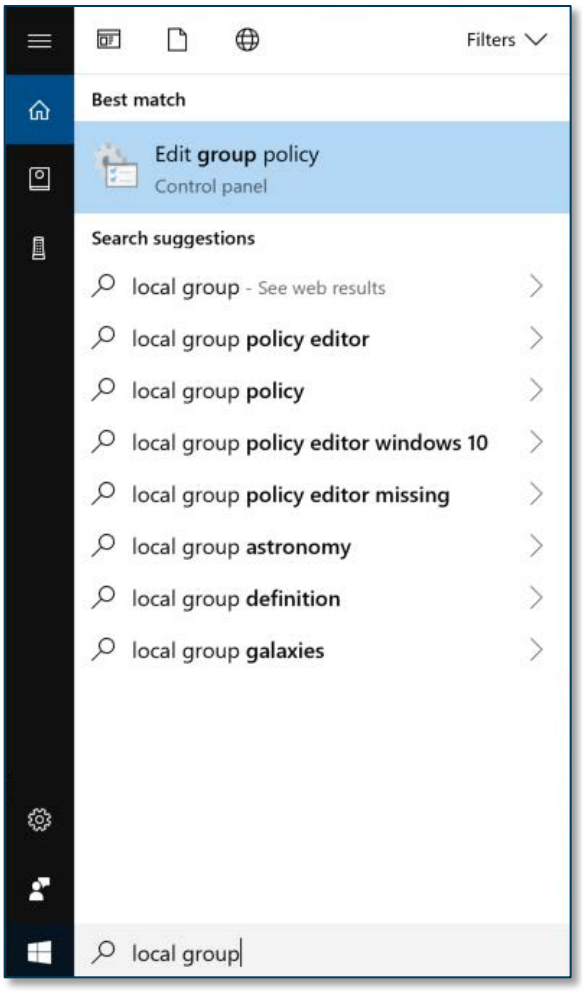


Figure 80 - Searching for LGPE

3. Select “Edit group policy” in the search list. The *Local Group Policy Editor Home Screen* displays.

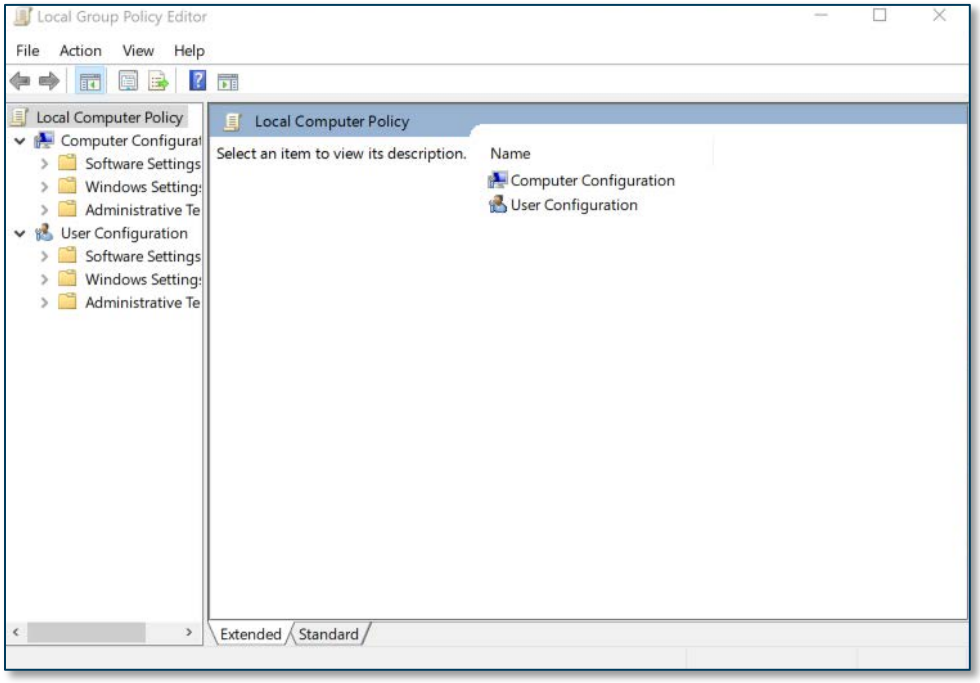


Figure 81 – LGPE Home Screen

4. Select *Computer Configuration* and expand *Administrative Templates*. The *Administrative Templates* subfolders display.

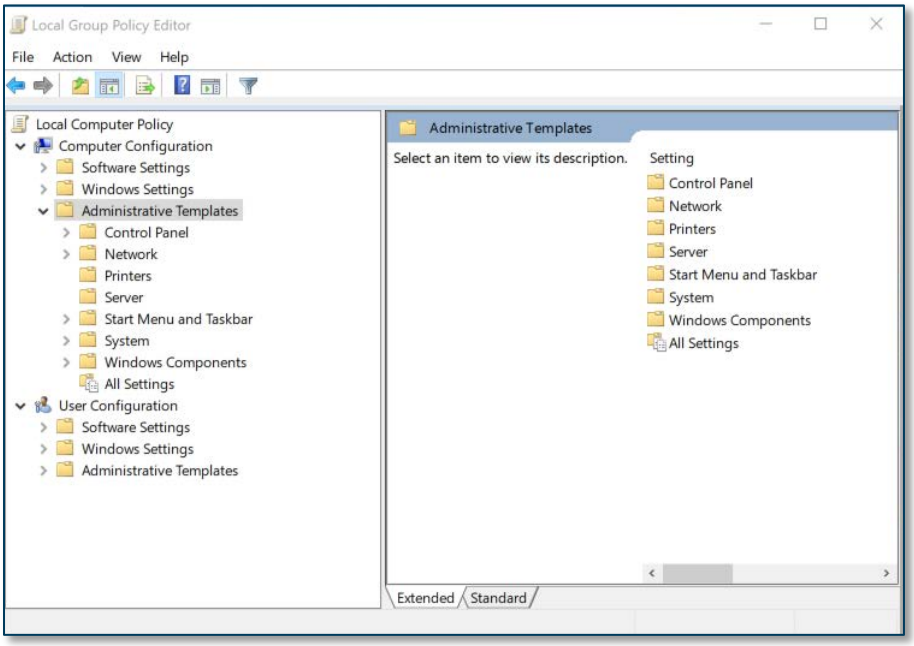


Figure 82 - LGPE Administrative Templates

5. Select *Windows Components* and *AutoPlay Policies*. The *AutoPlay* settings display.

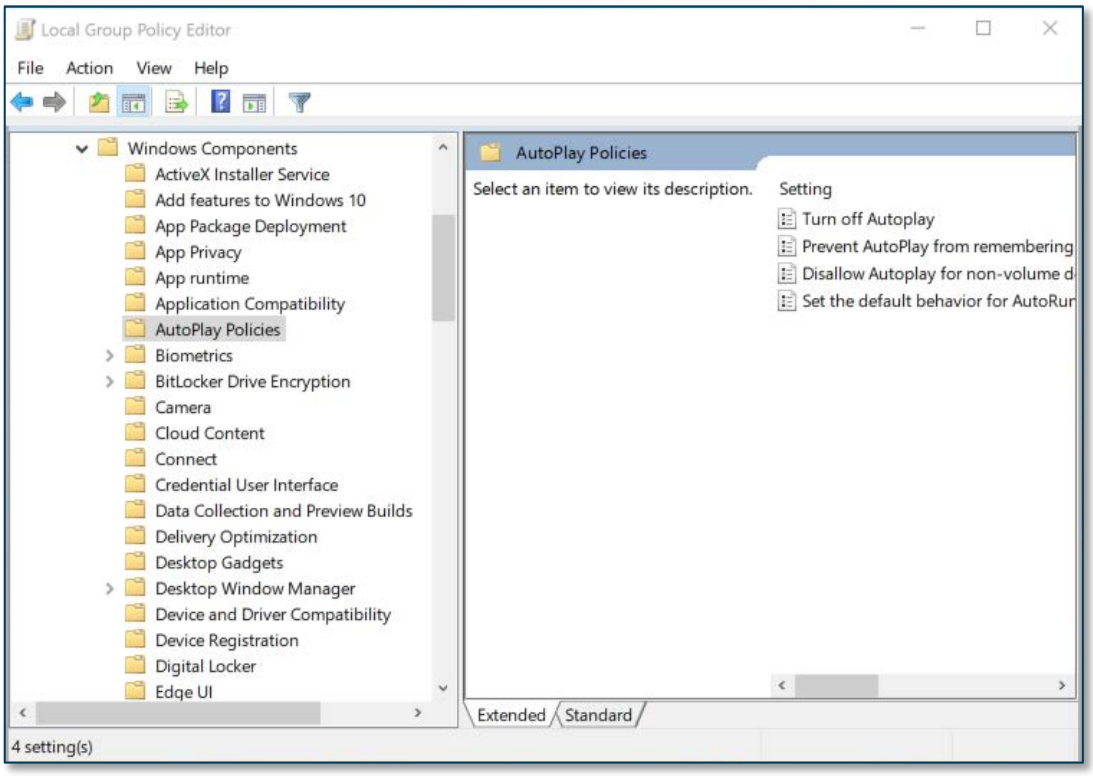


Figure 83 - LGPE AutoPlay Policies

6. Select *Set the default behavior for AutoRun* and set the value to *Disabled*.

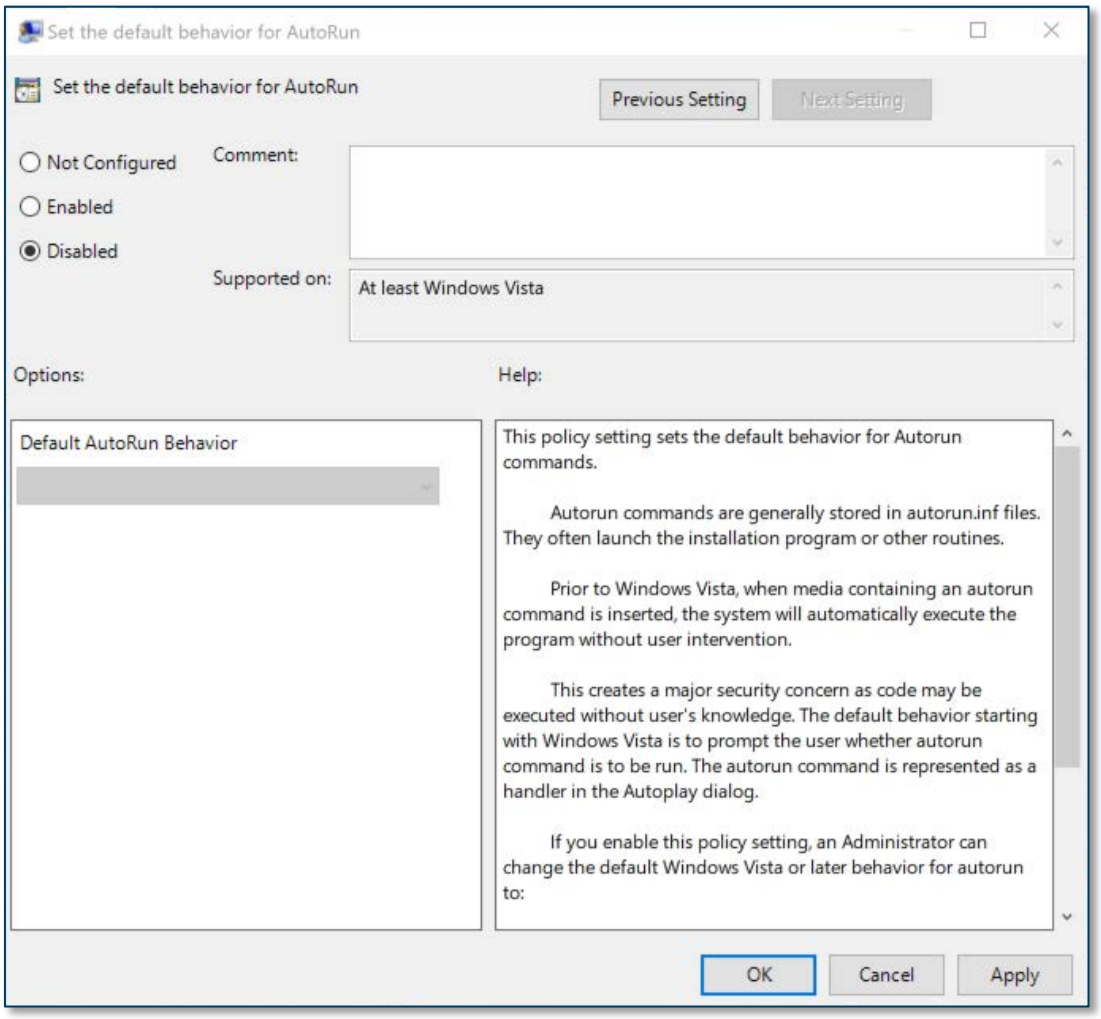


Figure 84 - LGPE AutoRun Settings

7. Under *AutoPlay Policies*, Select *Turn off Autoplay*. The *Turn off AutoPlay* screen opens.

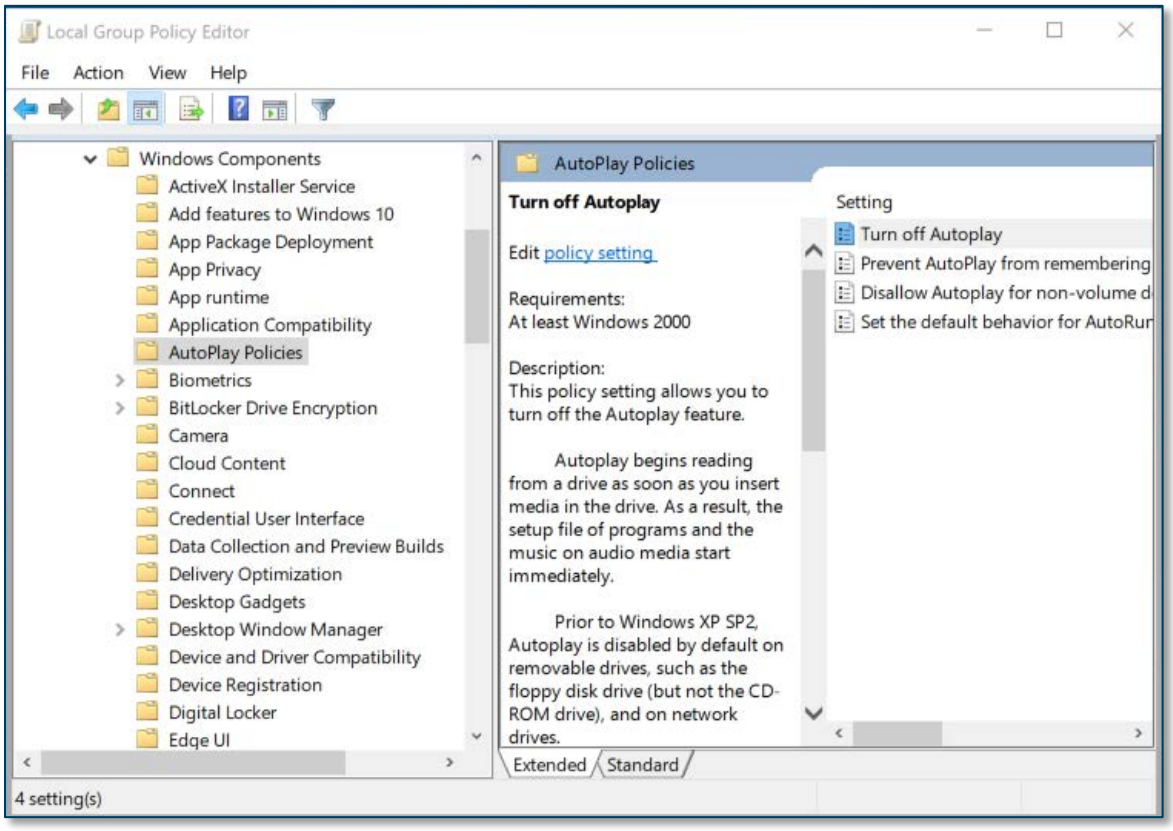


Figure 85 - Turn off AutoPlay Settings

8. Set the value to *Enabled*.

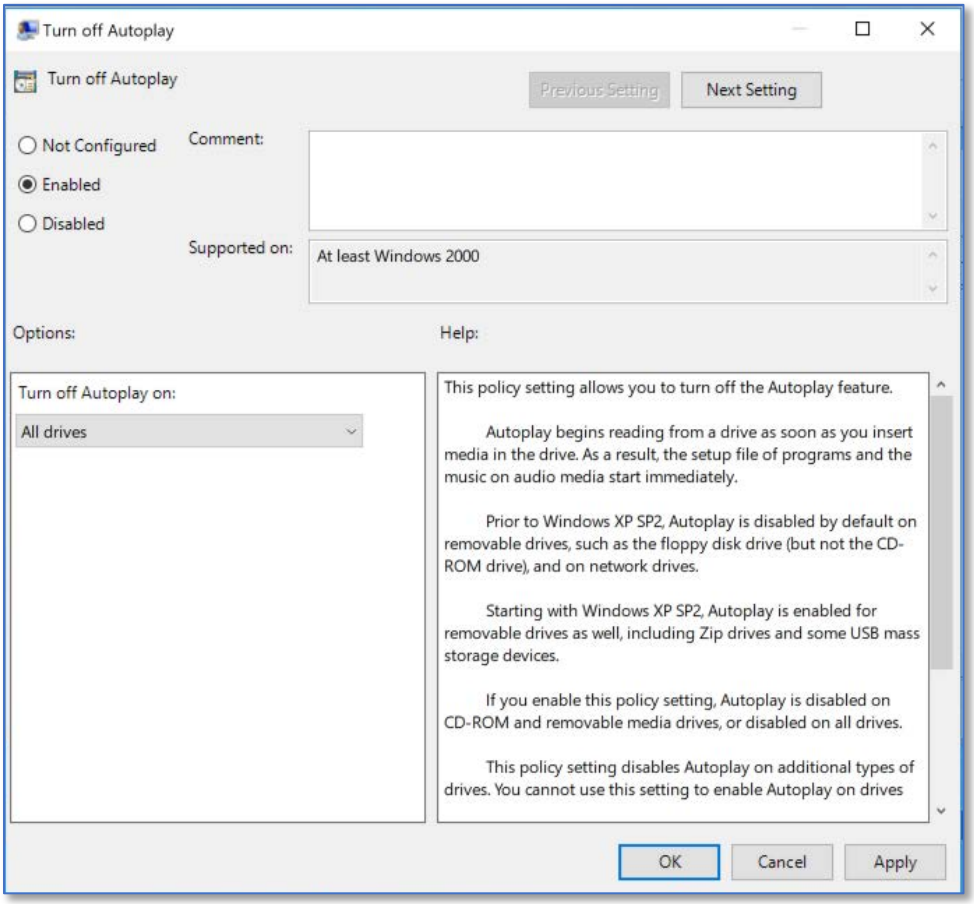


Figure 86 - Proper AutoPlay Configuration

Enabling Windows Defender Firewall

This process applies to CIS Control 9.4: Apply Host-Based Firewalls or Port-Filtering.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “windows defender” in the search bar. Search results for “windows defender” display.

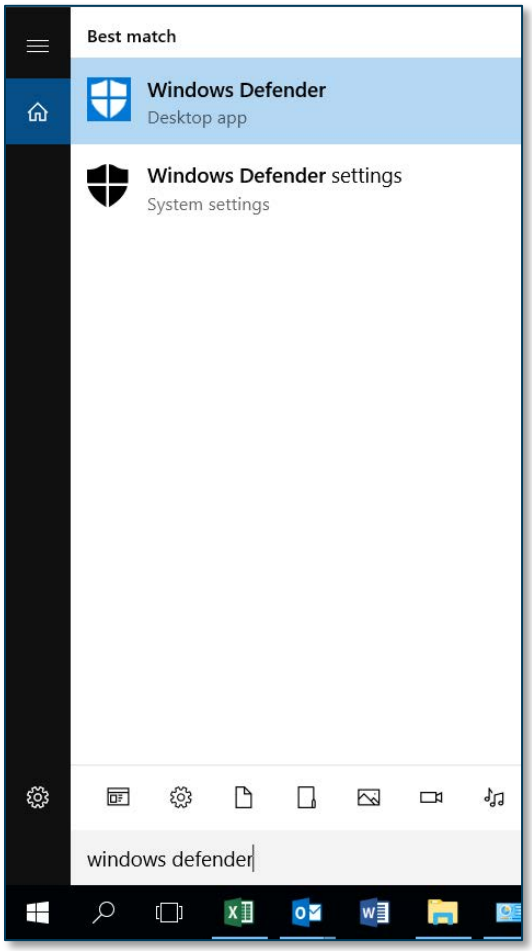


Figure 87 - Searching for Windows Defender

3. Select the Windows Defender App. The *Security at a Glance* window opens with status for monitored areas.

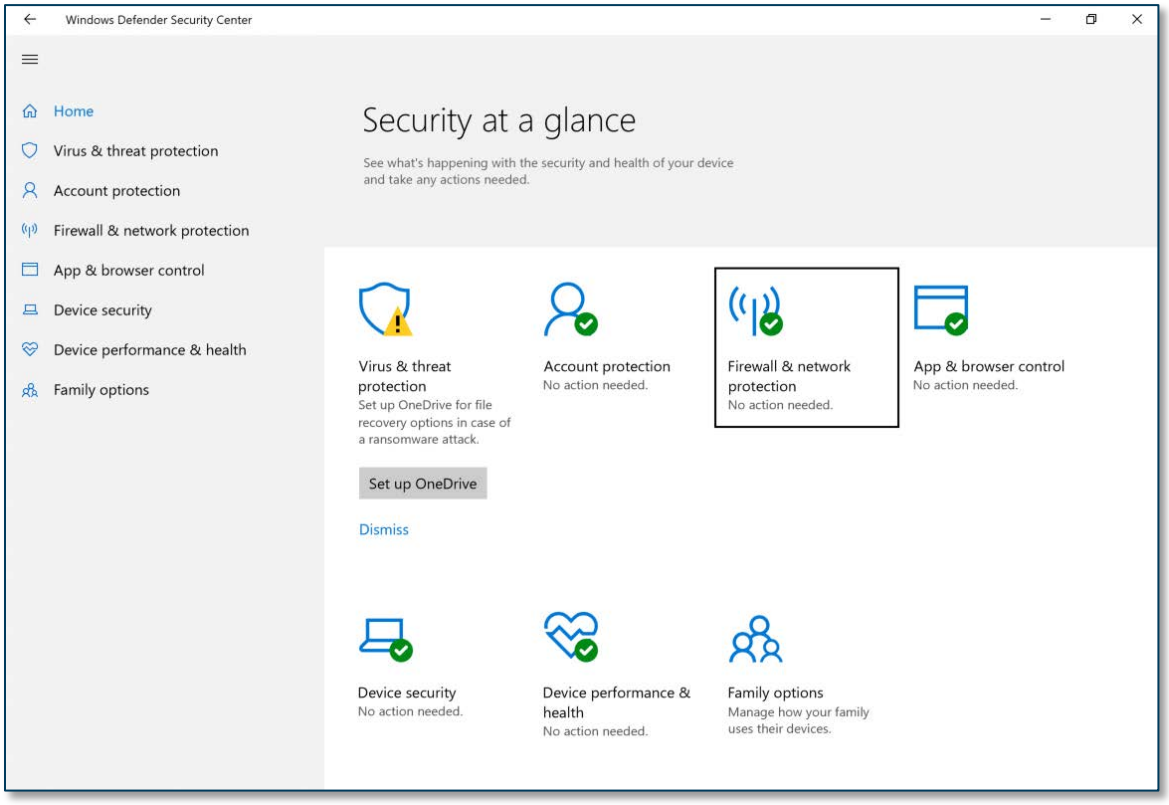


Figure 88 - Windows Defender Security Center Home Screen

4. Select *Firewall & network protection*. The *Fire and network protection* view opens.

5. Ensure that the Domain network, Private network, and Public network firewalls are set to *on*.

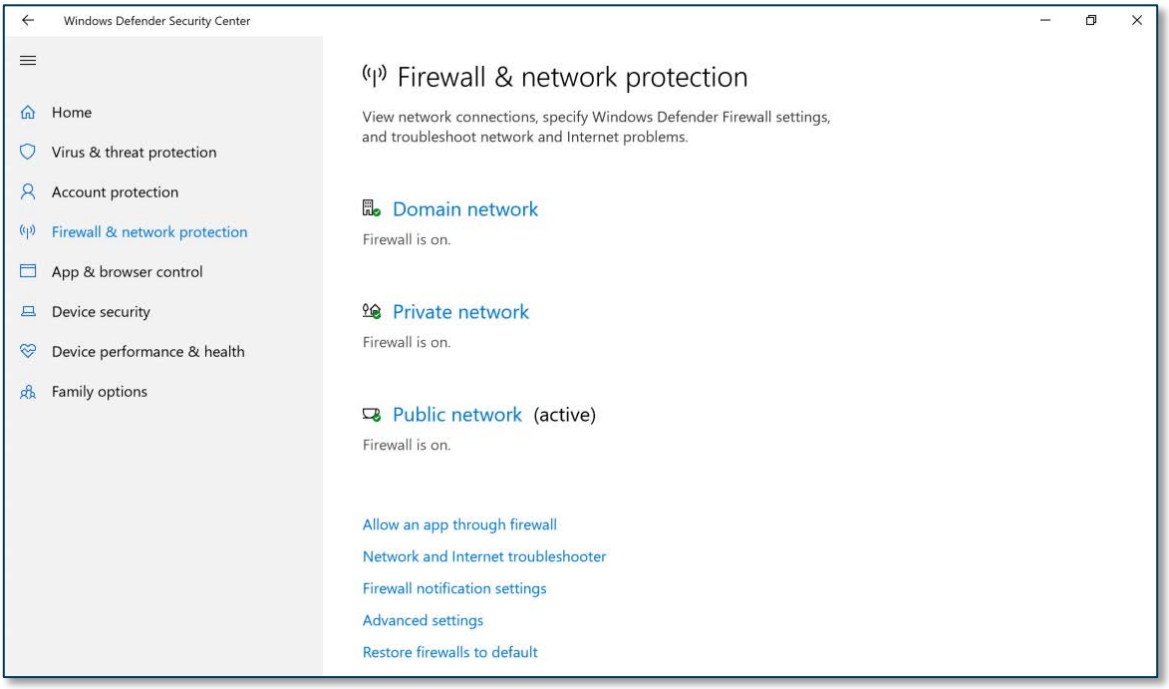


Figure 89 - Firewall and Network Protection Settings

6. If any of the three firewalls are not set to *on*, select that firewall to enable it.

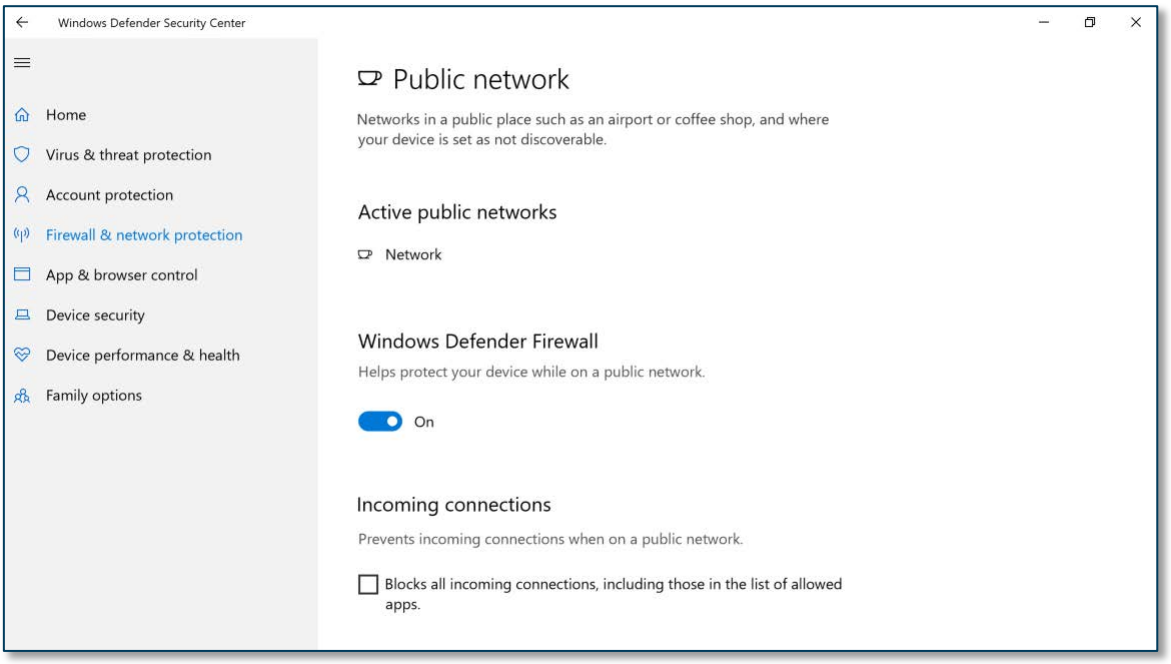


Figure 90 - Windows Firewall Public Network Settings

Configuring Microsoft File History

This process applies to CIS Control 10.1: Ensure Regular Automated Backups.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “backup” in the Windows search bar. Search results display for “backup”.

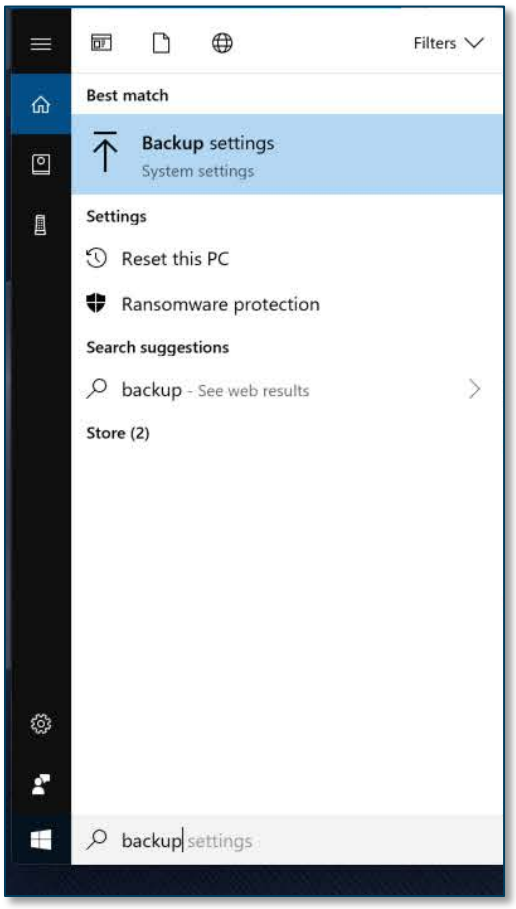


Figure 91 - Searching for Windows Backup Settings

3. Select “Backup settings”. The *Backup* screen displays.

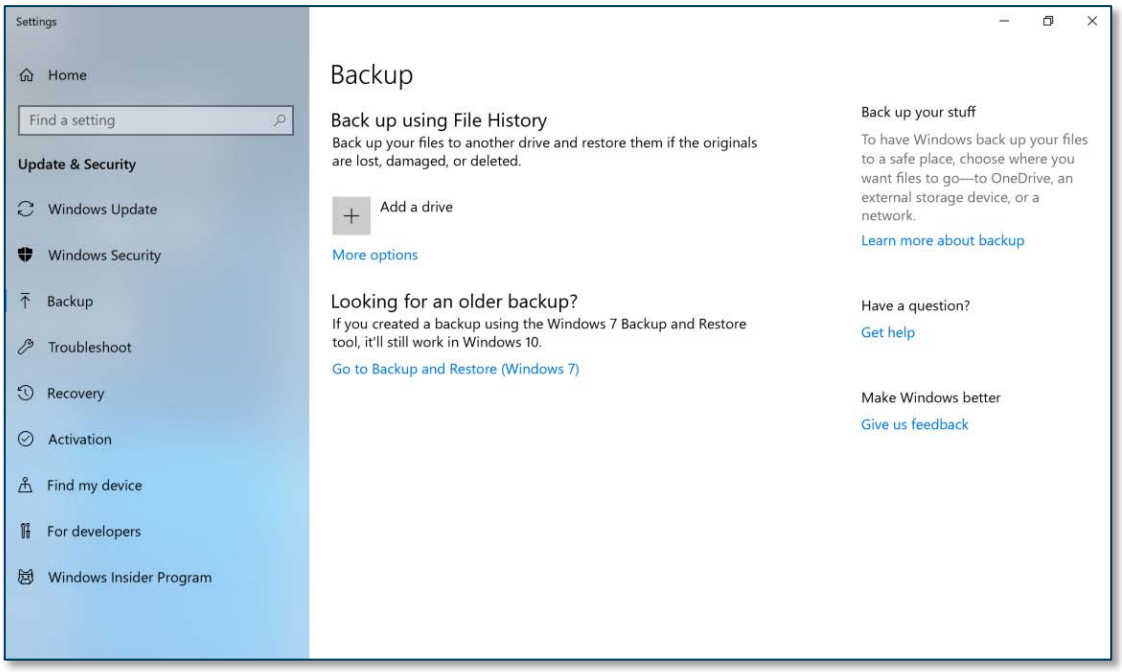


Figure 92 - Windows 10 Backup Settings

4. Select *Add a drive* under *Back up using File History*. The *Backup options home screen* displays.

Note: An external hard drive or removable media (e.g., USB drive, thumb drive) must be connected to the computer to backup information onto.

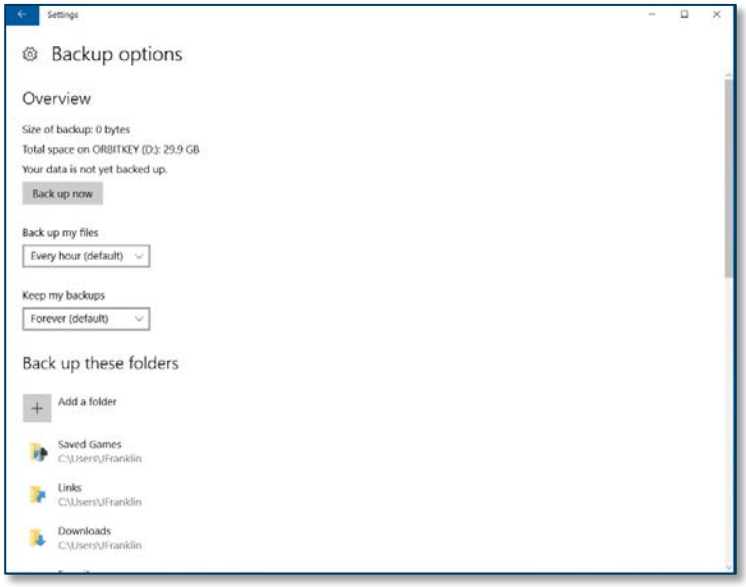


Figure 93 - File History Backup Options

5. Scroll down and select *See advanced settings*.

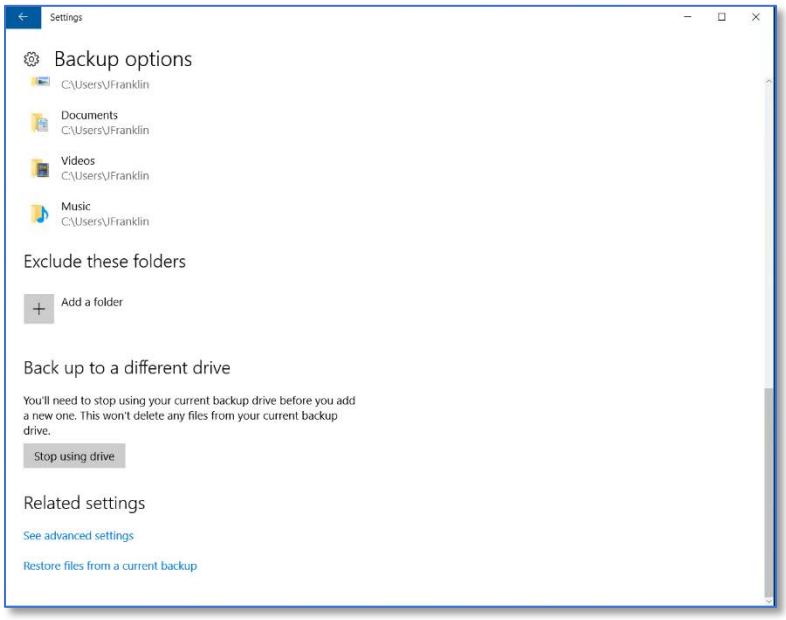


Figure 94 - Advanced File History Options

6. Ensure file history is turned *on*.

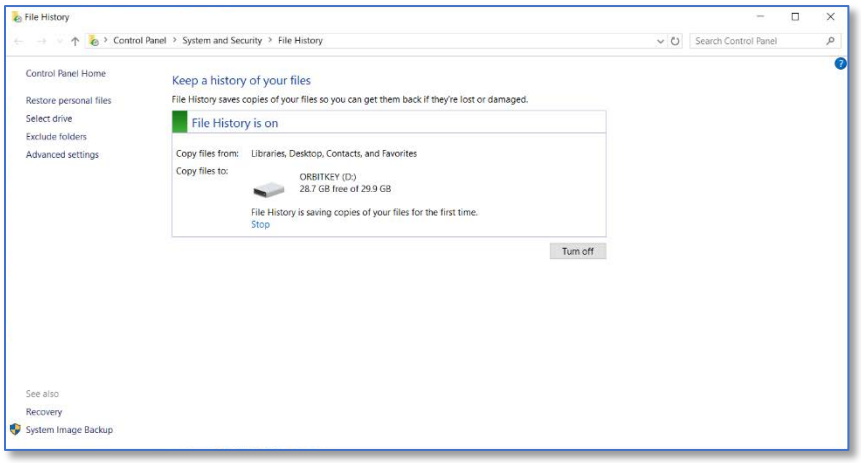


Figure 95 - Final File History Screen

Creating System Images with Windows 10 Pro

This process applies to CIS Control 10.2: Perform Complete System Backups. Use these steps to create system images with Windows 10 Pro.

1. Select the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “backup settings” in the search bar. Search results for “backup settings” display.

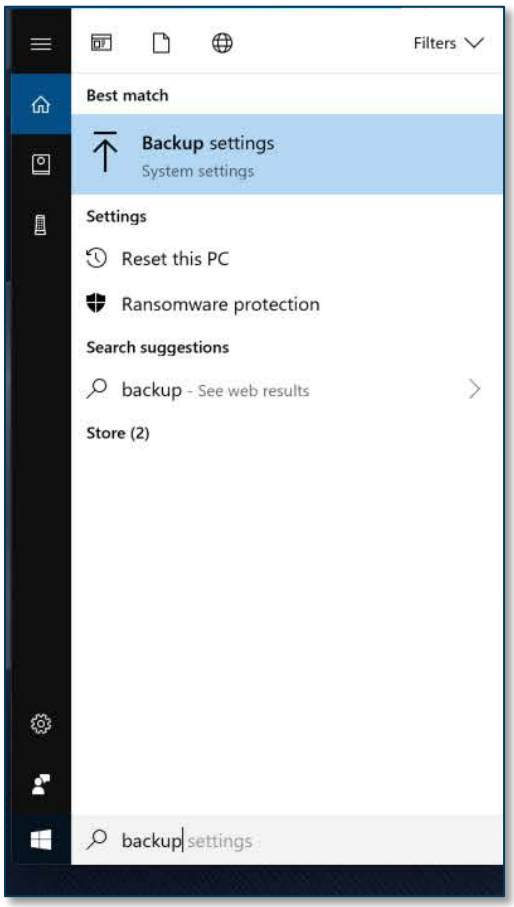


Figure 96 - Searching for Windows Backup Settings

3. Select “Backup settings”. The *Backup* screen displays.

4. Select *Go to Backup and Restore (Windows 7)*. The *Backup and Restore (Windows 7)* screen displays.

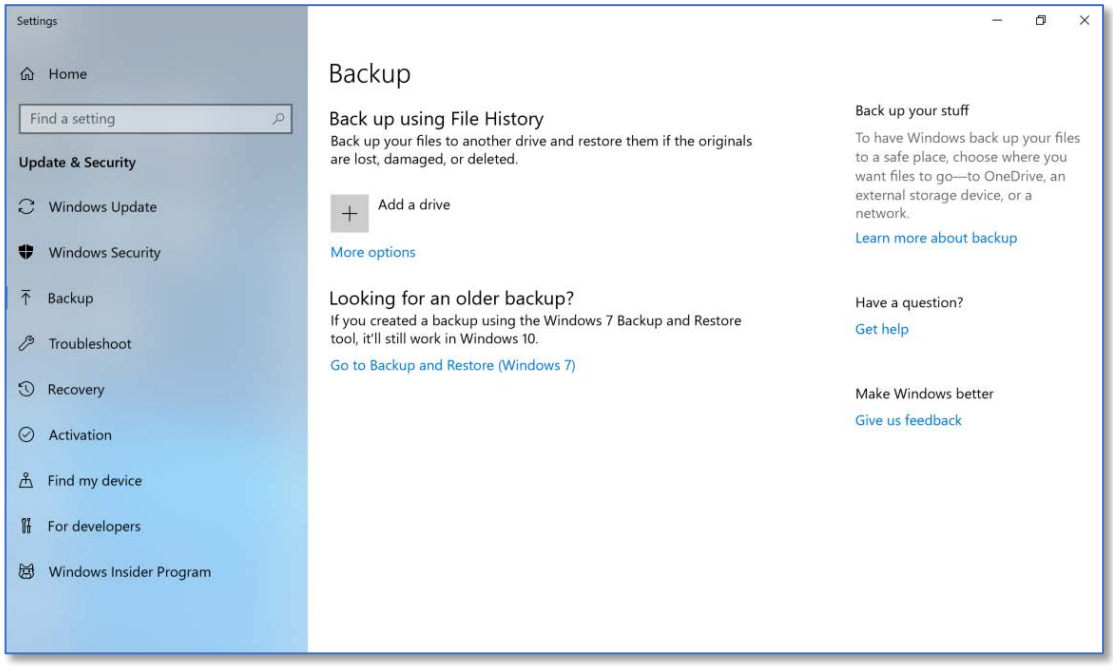


Figure 97 - Windows 10 Backup Settings

5. Select *Set up backup*. The *Set up backup* window displays.

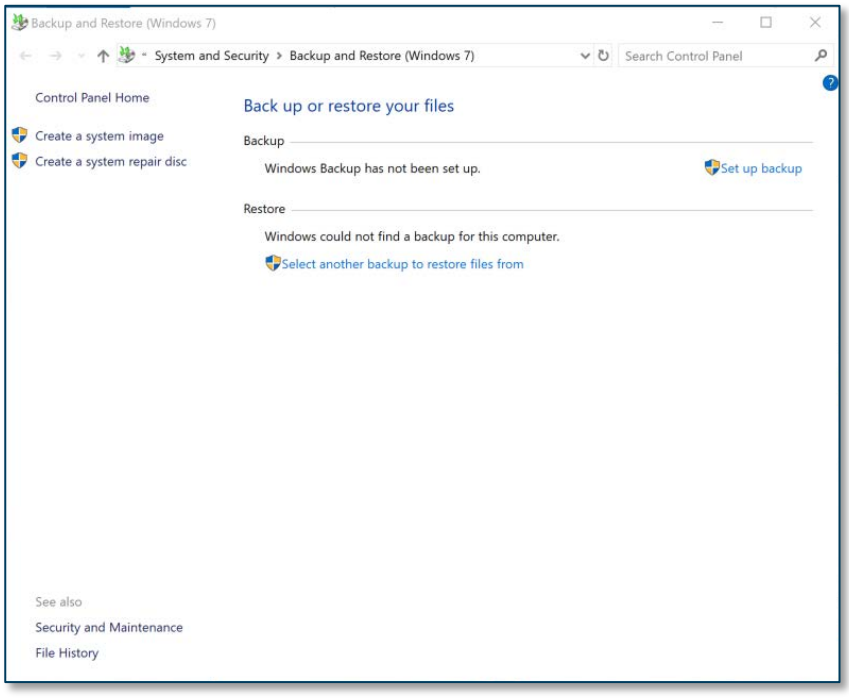


Figure 98 - Backup and Restore Home Screen

6. Select the local or network drive where backups should be stored. Click *Next*.
7. The *Select where you want to save your backup* view opens. Determine whether Windows will select which files need to be backed up, or if this is a decision that needs to be made on a file by file basis. This example lets Windows select the files to be saved.

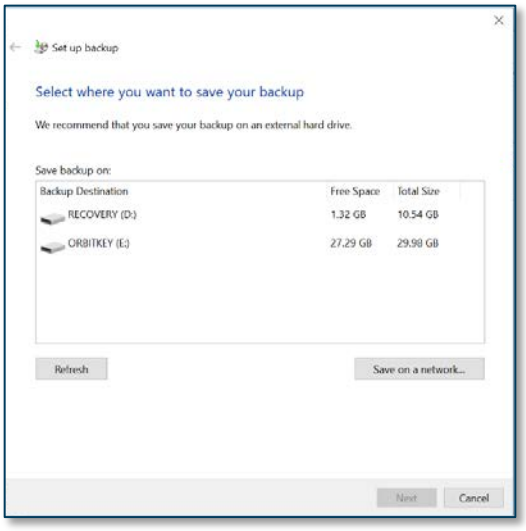


Figure 99 - Selecting the Storage Location for Backups

8. Click *Next.* The *What do you want to back up?* view opens.
9. Select *Let windows choose (recommended)* to have Windows determine what files to backup.
10. Click *Next.* The *Review your backup settings* view opens.

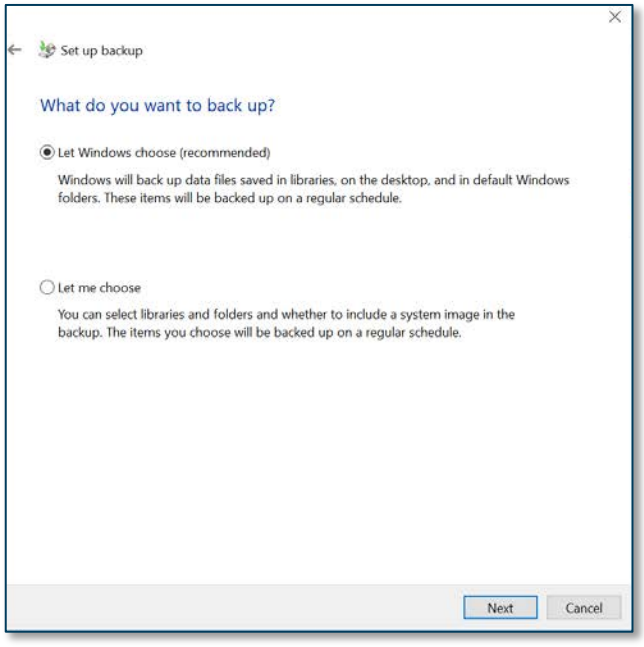


Figure 100 - Choosing the Storage Location

11. Review the selected backup options. If you are satisfied the settings are appropriate, click *Save settings and run backup*. Otherwise, click *Cancel.*

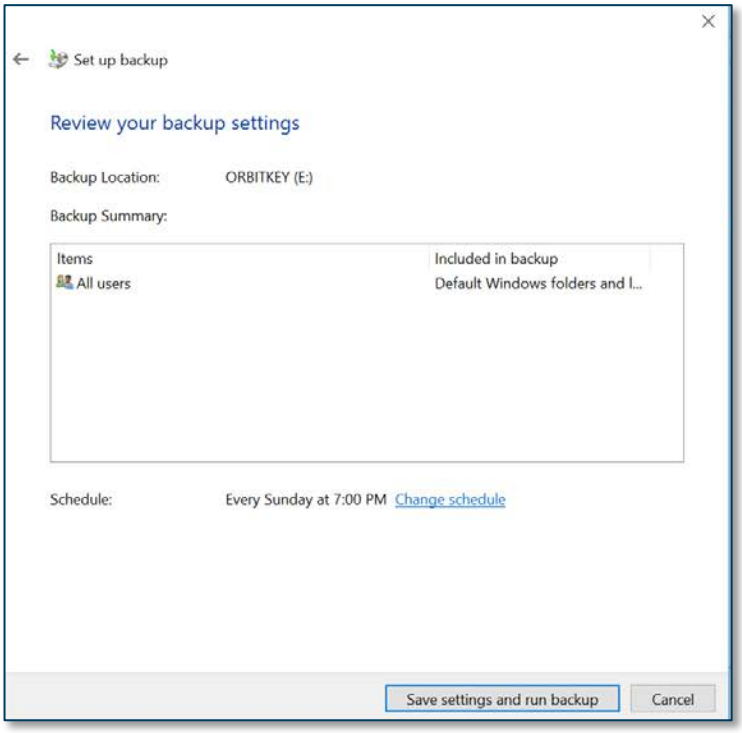


Figure 101 - Selecting the Accounts that will be Backed Up

12. The backup begins. It may take a long time to successfully complete. While the backup is in progress, a backup in progress bar displays.

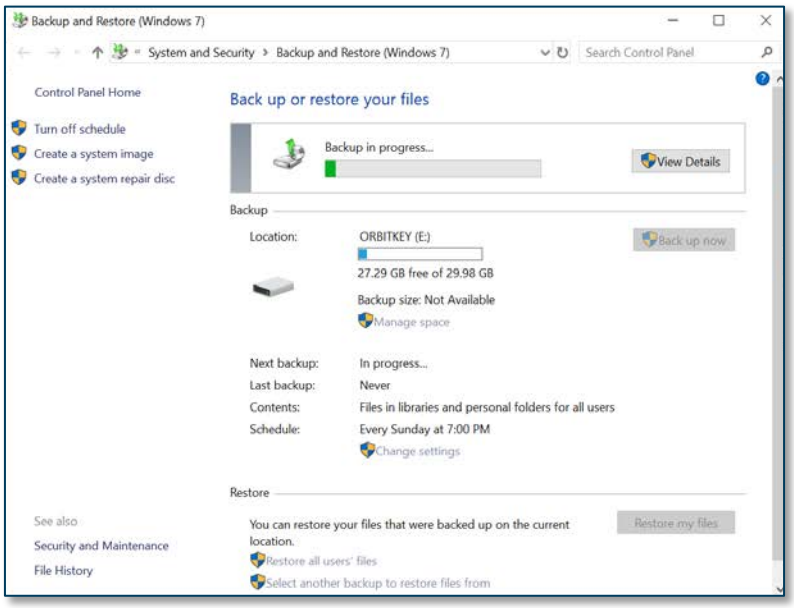


Figure 102 - Back Up in Progress

Configuring Windows BitLocker

Note: BitLocker can be complicated to enable. In addition to this guidance, it may be useful to consult the Microsoft documentation (https://support.microsoft.com/en-us/help/4502379/windows-10-device-encryption).

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “bitlocker” in the search bar. Search results related to “bitlocker” display.

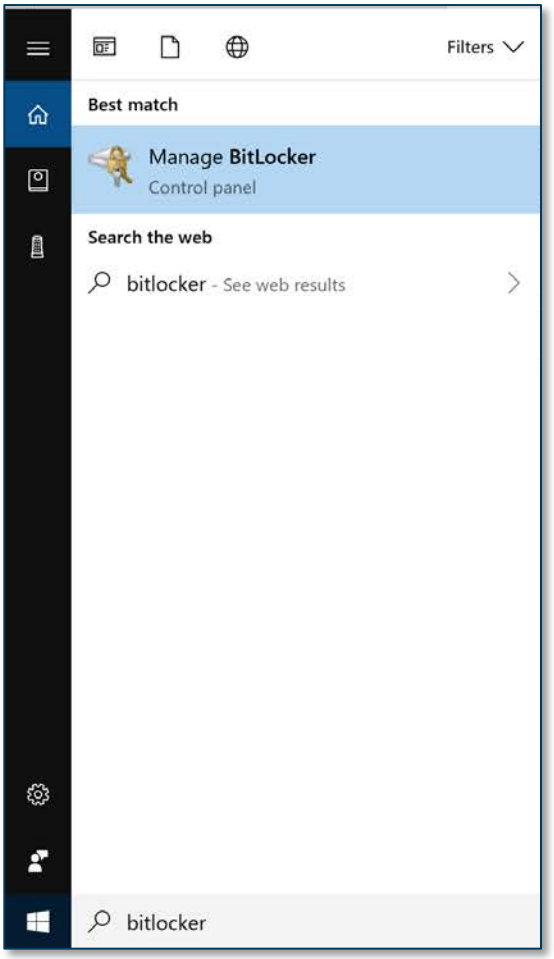


Figure 103 - Searching for BitLocker

3. Select “Manage Bitlocker” in the search results. The *BitLocker Drive Encryption* screen displays.

4. Select *Turn on BitLocker*.

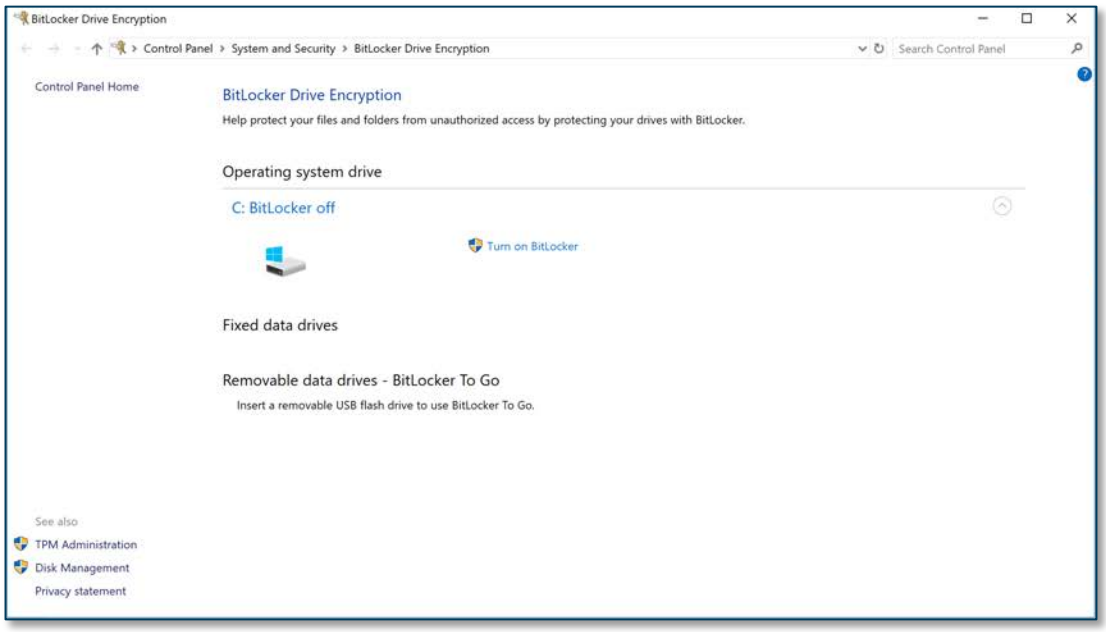


Figure 1044 - Turn on BitLocker Setting

Note: An error may be displayed if the computer in question lacks a hardware encryption module (e.g., Trusted Platform Module). TPMs are the preferred method to enable encryption on Windows 10 but encryption can be used without it. The following error message may be presented.

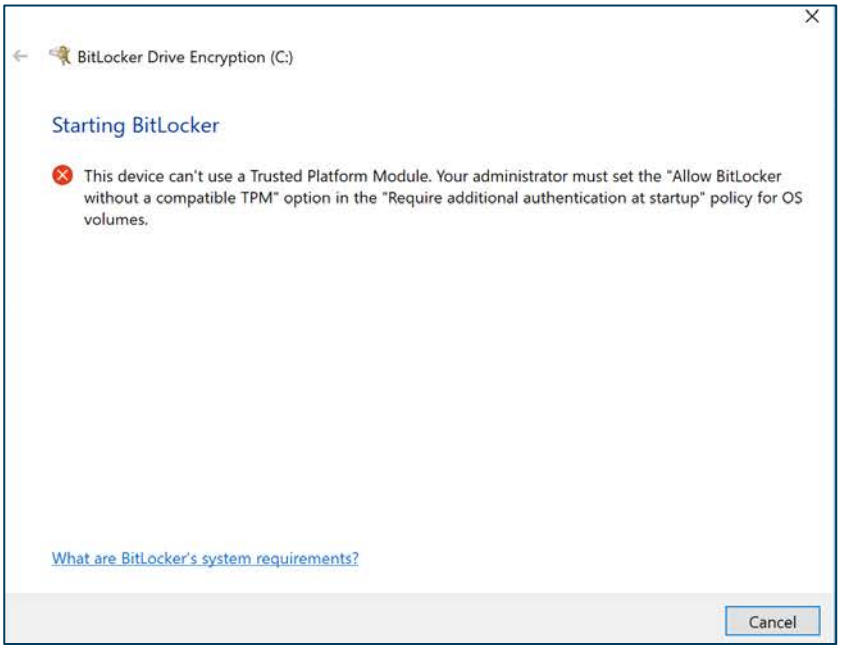


Figure 1055 - Starting BitLocker Error Screen

Set up a Trusted Platform Module

In order to solve this issue, the Windows Local Group Policy Editor can be used. Follow this path to navigate to the correct LGPE settings:

1. Select *Computer Configuration* and navigate the following path:

   Administrative Templates, *Windows Components*, *BitLocker Drive Encryption*, *Fixed System Drives*, *Configure use of hardware-based encryption for fixed data drives*.

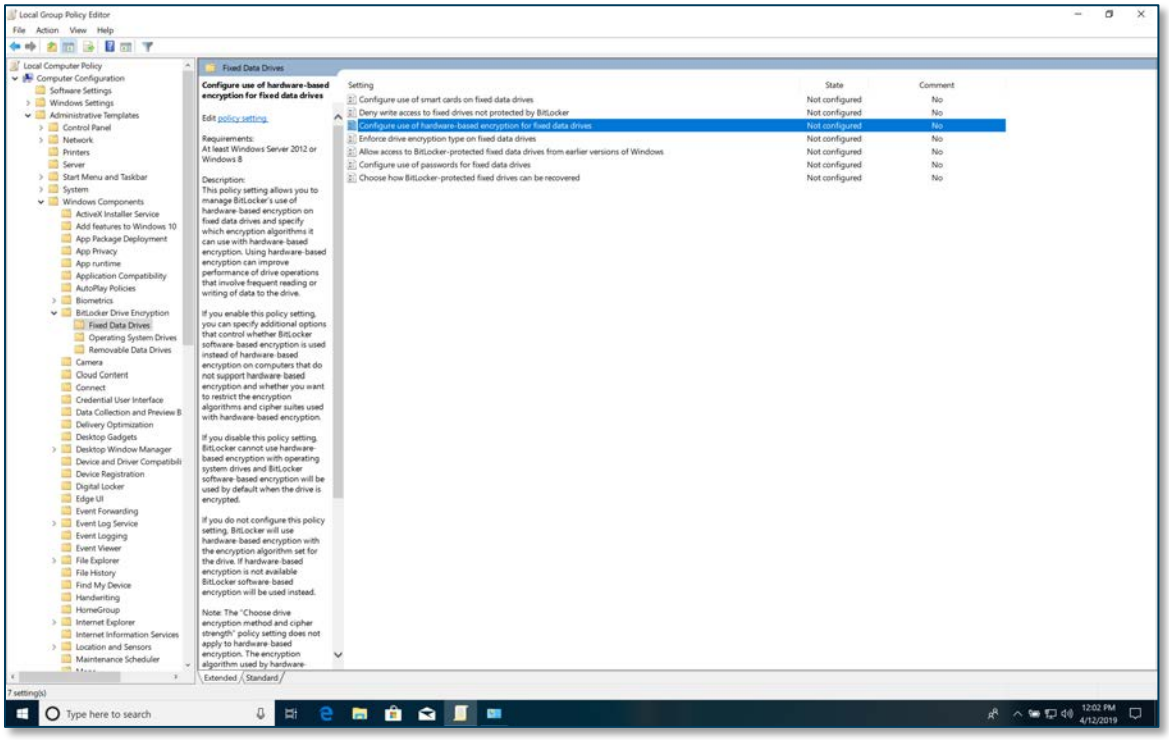


Figure 1066 - Configure Hardware-Based Encryption

2. Enable *Configure use of hardware-based encryption for fixed data drives.* Then select *Use BitLocker software-based encryption when hardware encryption is not available*.

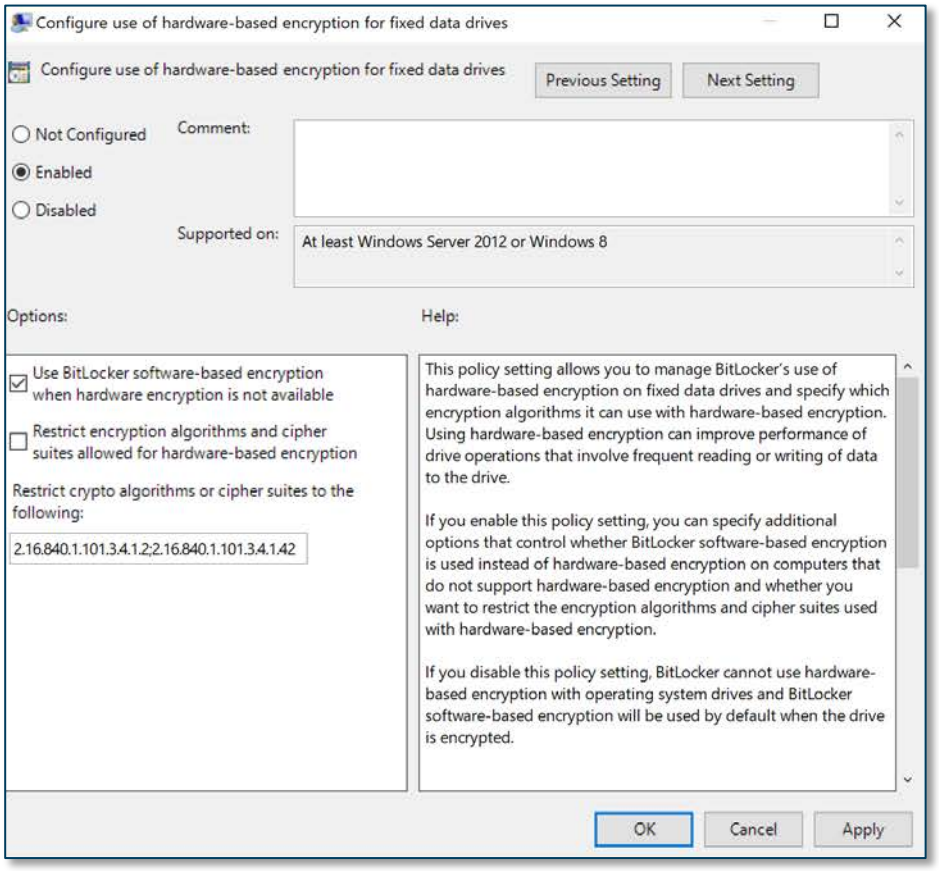


Figure 1077 – Enabling Software-Based Encryption

Another setting must also be configured to resolve this error.

3. Under *Computer Configuration*, select *Administrative Templates* and then *Windows Components*. The *Windows Components* subfolders display.

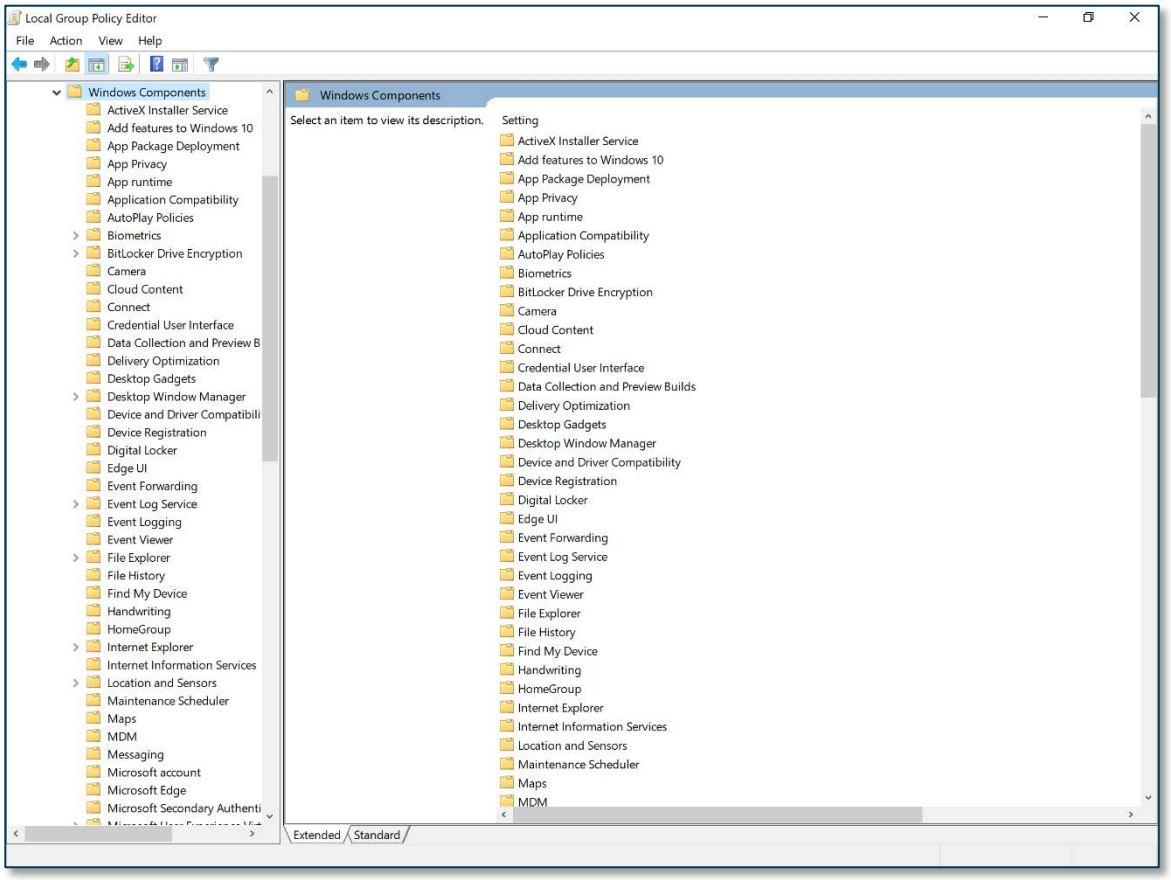


Figure 1088 - Identifying Additional BitLocker Settings

4. Select *BitLocker Drive Encryption*, followed by *Operating System Drives*, and then select *Require additional authentication at startup*.

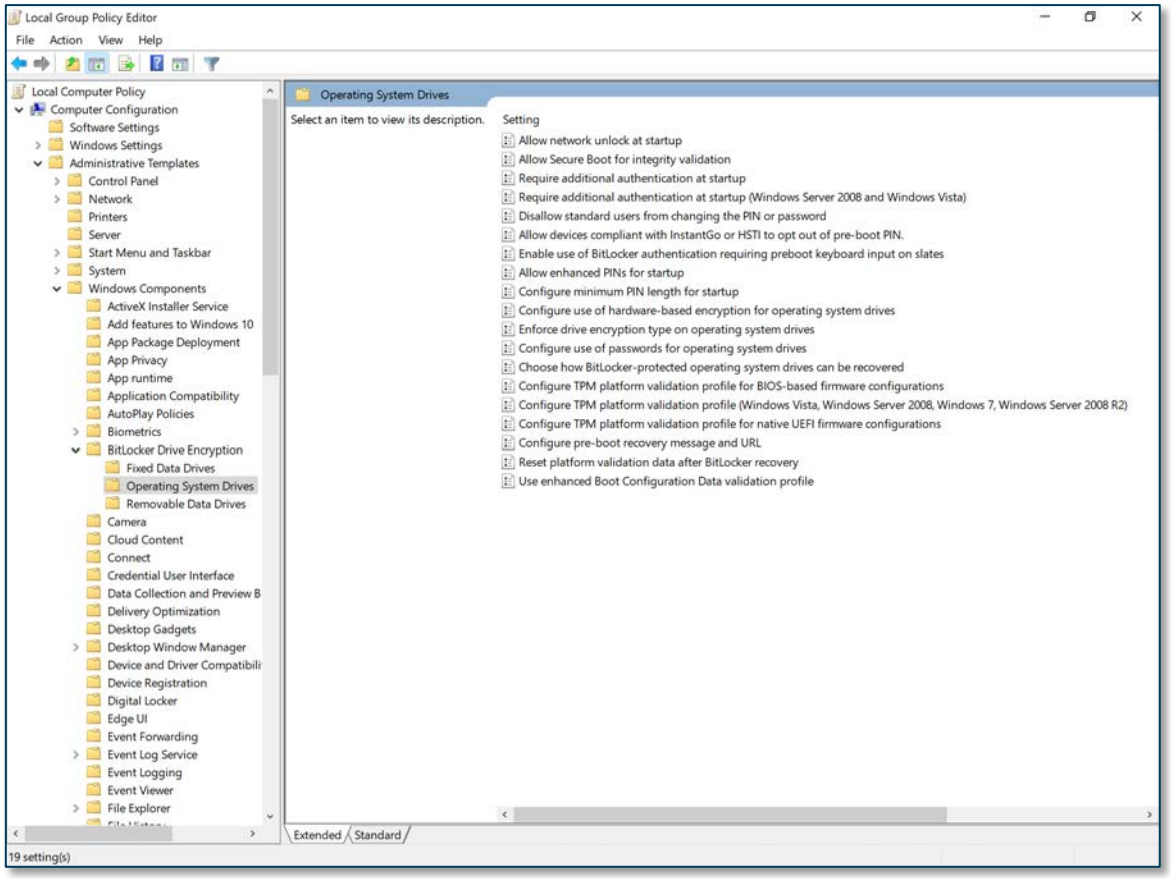


Figure 1099– Searching for BitLocker Startup Authentication Settings

5. Enable *Require additional authentication at startup* and select *Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)*. This should solve the error. If not, restart the steps in this section.

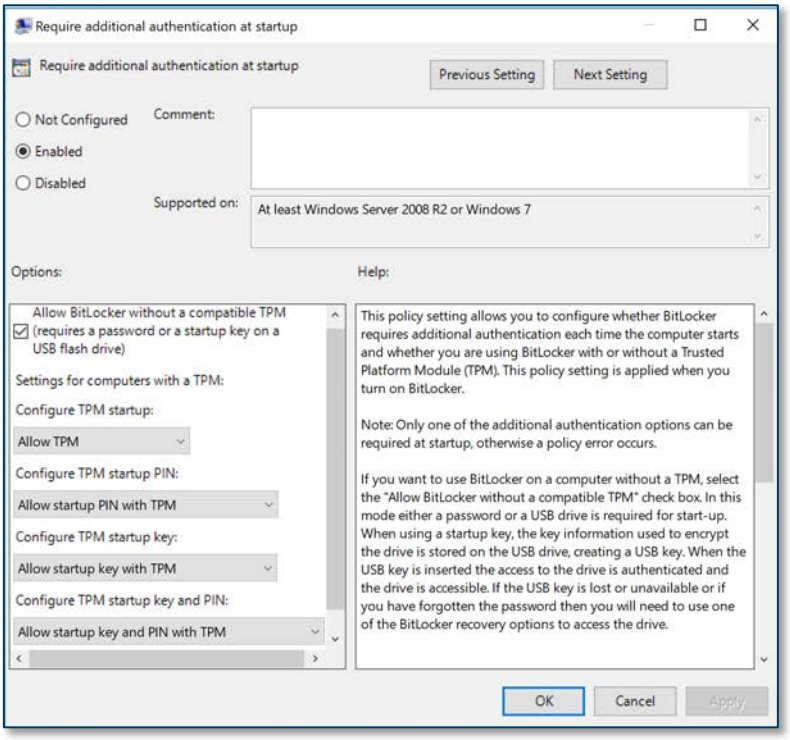


Figure 110 - Requiring Additional Authentication at Startup Policy

6. The system will check additional settings before enabling BitLocker. The *Checking your PC's configuration* screen opens.

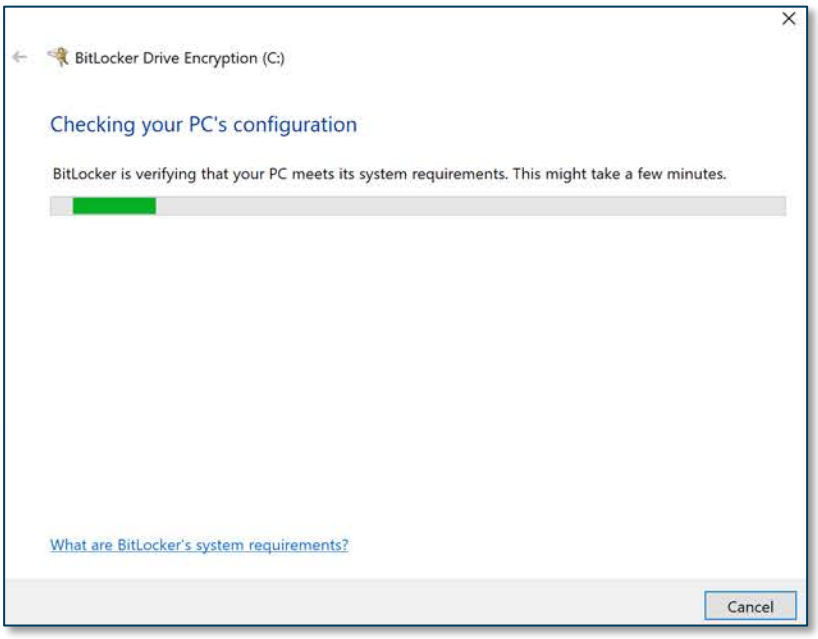


Figure 1101 - Checking the System for BitLocker Support

7. The *Bitlocker Drive Encryption setup screen* displays. Select *Next*. The *Preparing your drive for Bitlocker* screen displays.

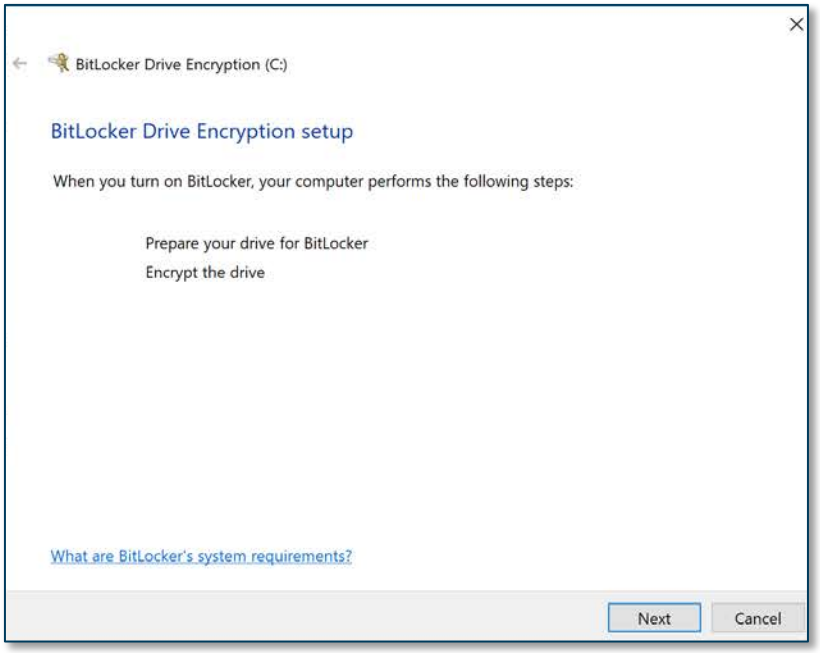


Figure 1112- BitLocker Setup

8. Select *Next* after reviewing the warnings from Windows. The *Preparing your drive for BitLocker* displays with a status of tasks.

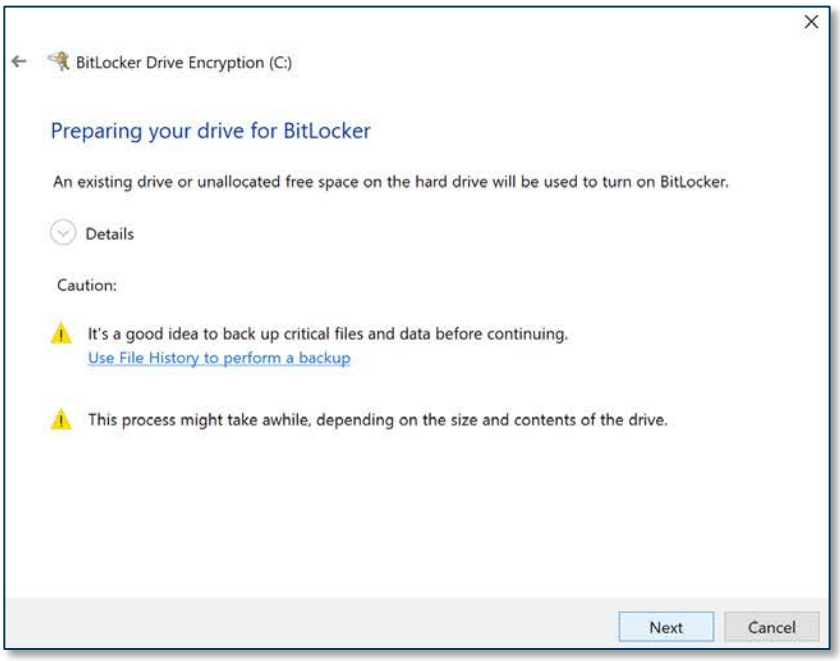


Figure 1123 - BitLocker Preparation Screen

9. Additional preparation for BitLocker. Wait until this process completes.

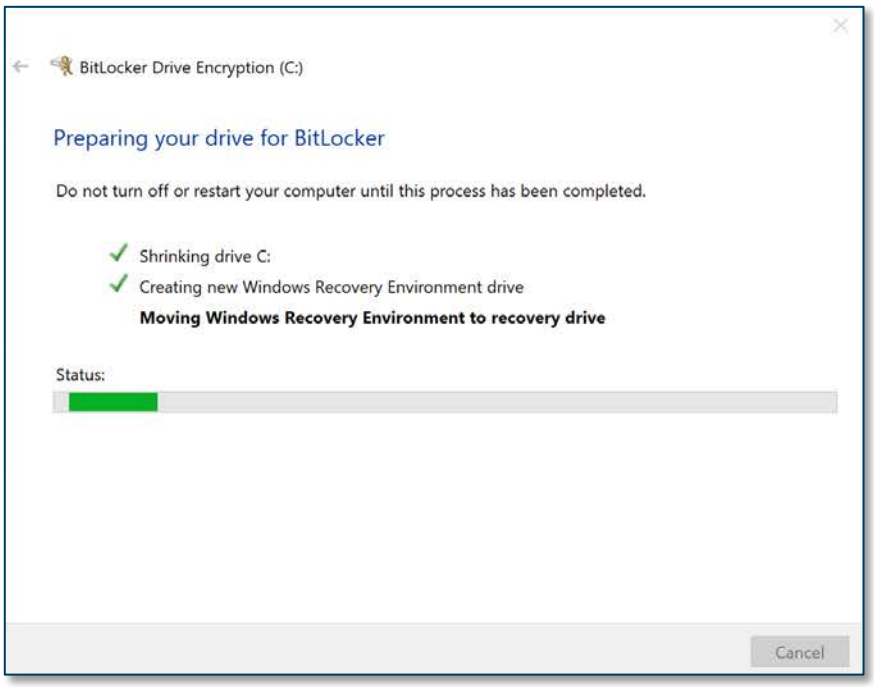


Figure 114 - Additional BitLocker Preparation Screen

10. The BitLocker Drive Encryption Setup screen with a Windows Recovery Warning displays.

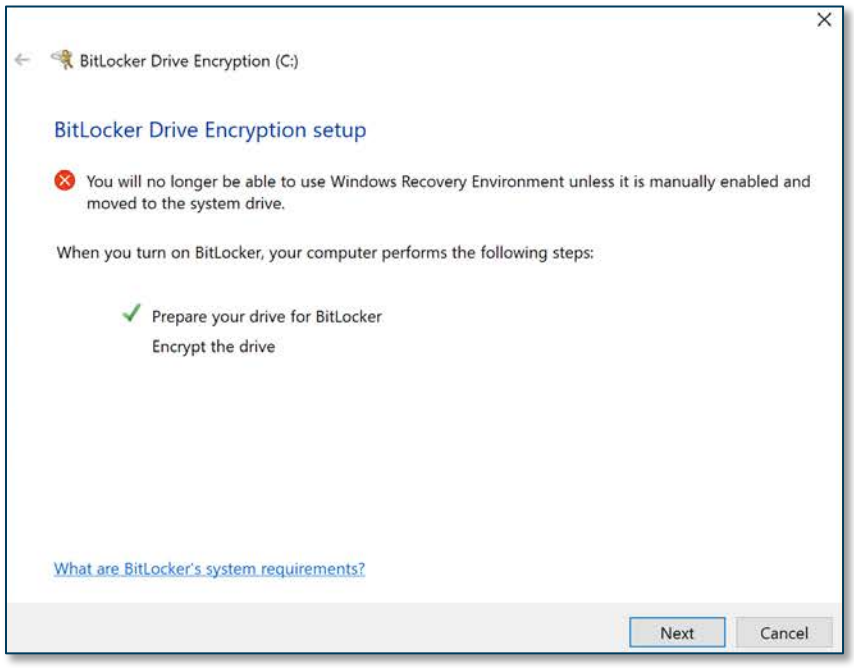


Figure 1135 - Windows Recovery Warning

11. Select *Next*. The *Choose how to unlock your drive at startup* screen displays. This screen allows the user the option for how to unlock the encrypted drive at startup. This guide will use the “Enter a password” method.

12. Select *Enter a password.* The *Create a Password to unlock this drive* screen displays.
    Note: A password is necessary to unlock BitLocker.

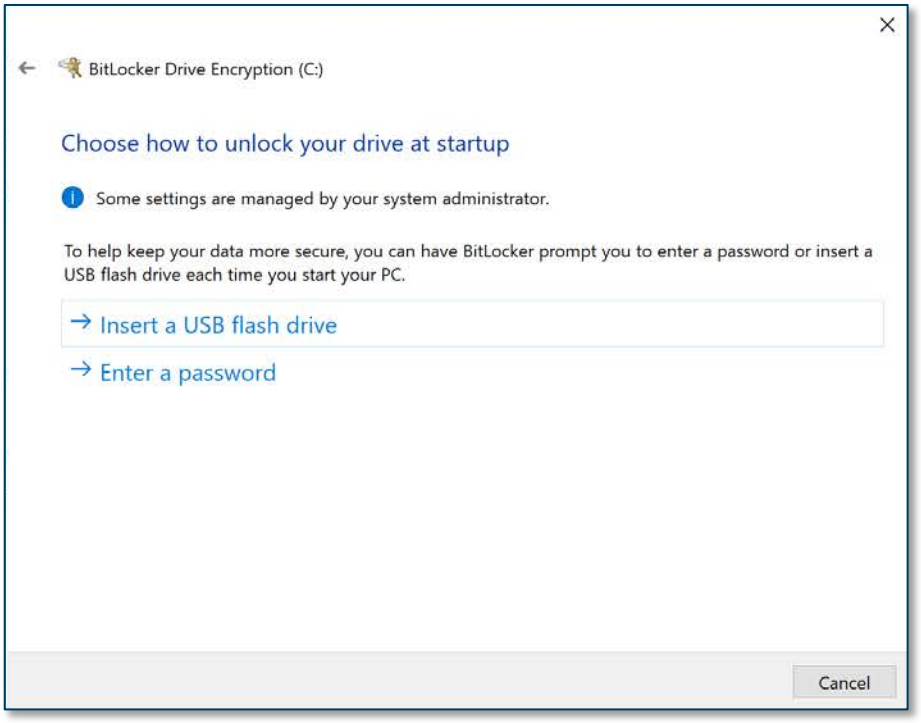


Figure 1146 – Select Unlock Method

13. Enter the password in the *Enter your password* text field.
14. Enter the password again in the *Reenter your password* text field.

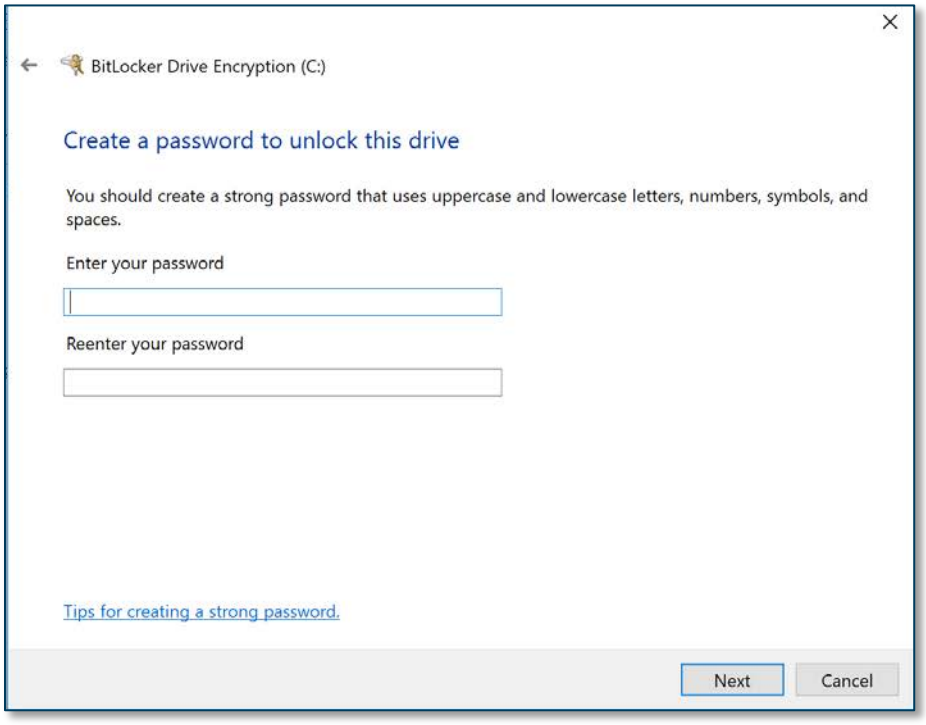


Figure 1157 - BitLocker Password Creation

15. Click *Next.* The *How do you want to back up your recovery key?* screen displays. **Note:** A recovery key should be stored elsewhere in case the BitLocker password is lost. Without the recovery key, if the password is forgotten then the system will be completely inaccessible.

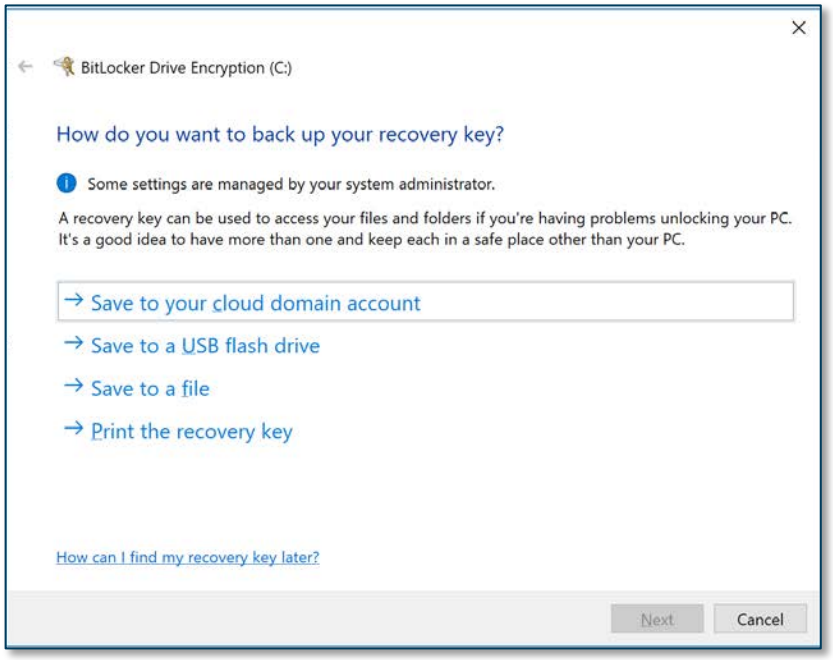


Figure 1168 - Recovery Key Selection

16. Select how the recovery key will be saved. The *Choose how much of your drive to encrypt* screen displays. This guide encourages average users to select the faster option but for systems storing sensitive data, users are encouraged to encrypt the entire drive (the second option).

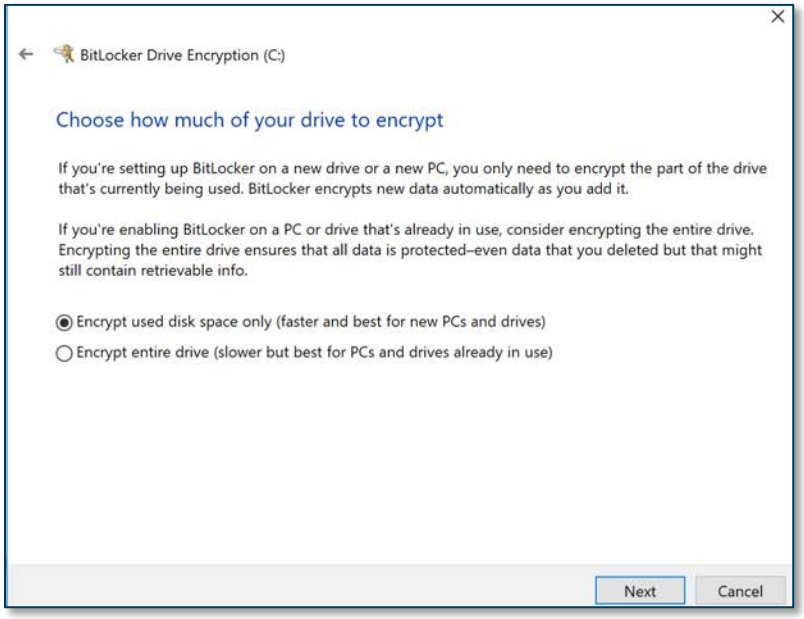


Figure 1179 - Encryption Type Selection

17. Click *Next.* The *Are you ready to encrypt this drive?* screen displays.
18. Ensure *Run BitLocker system check* is selected.
19. Click Continue. The *Choose which encryption mode to use* screen displays.

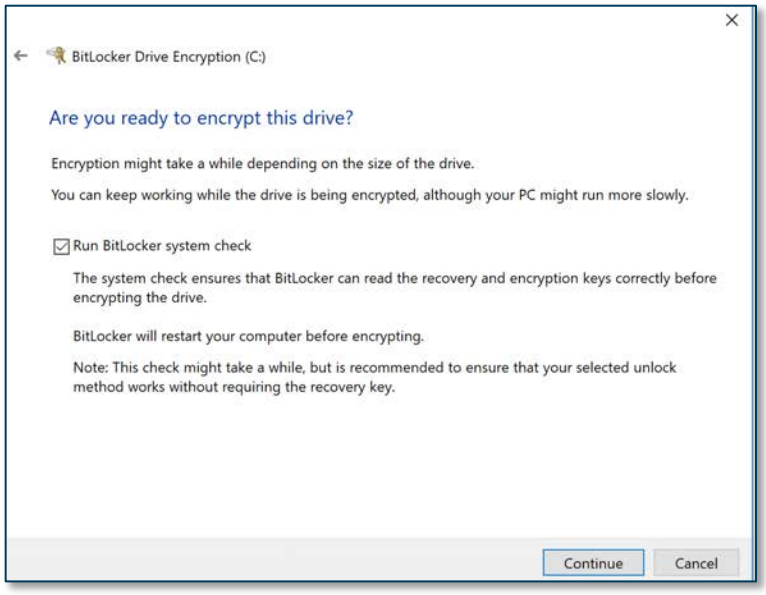


Figure 11820 - Run BitLocker System Check

20. Select *New encryption mode* (best for fixed drives on this device).

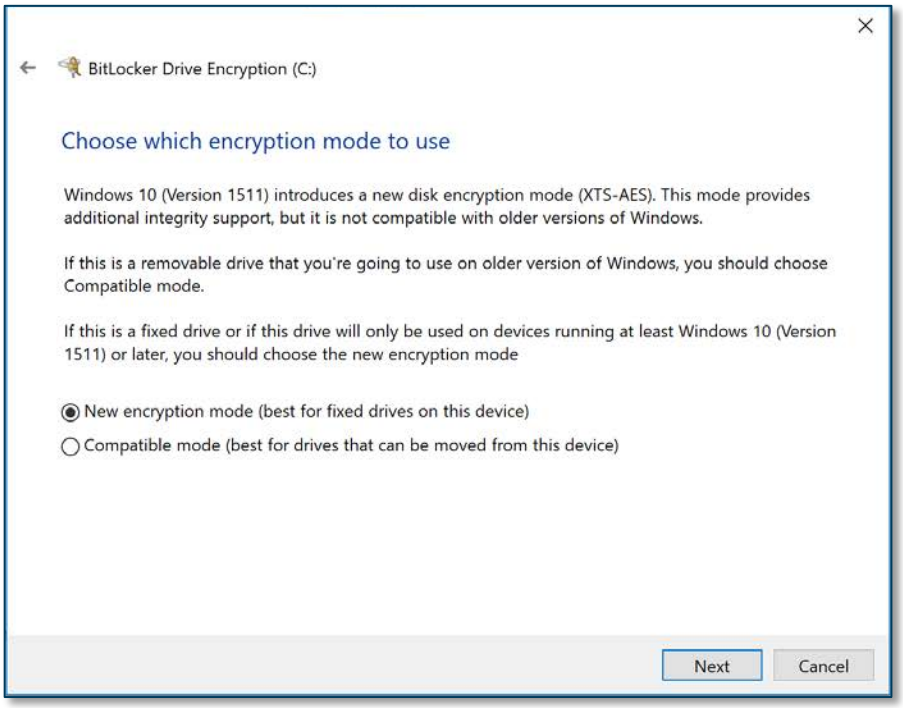


Figure 121 - Choosing the Encryption Mode

21. Click Next.

Identifying if a WiFi Connection is Using AES

This process applies to Sub-Control 15.7. Use these steps to identify if a Wifi connection is using AES.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “network” in the search bar. Search results related to “network” display.

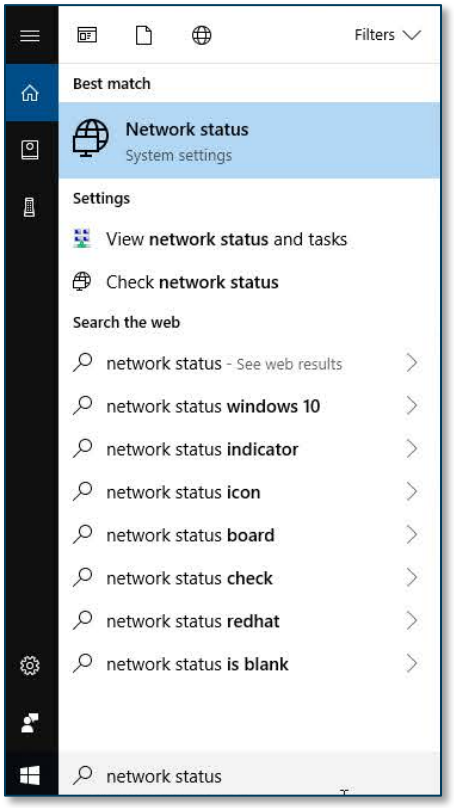


Figure 1192 - Searching for Windows Network Status

3. Select “Network status” from the search options. The *Status* screen displays.

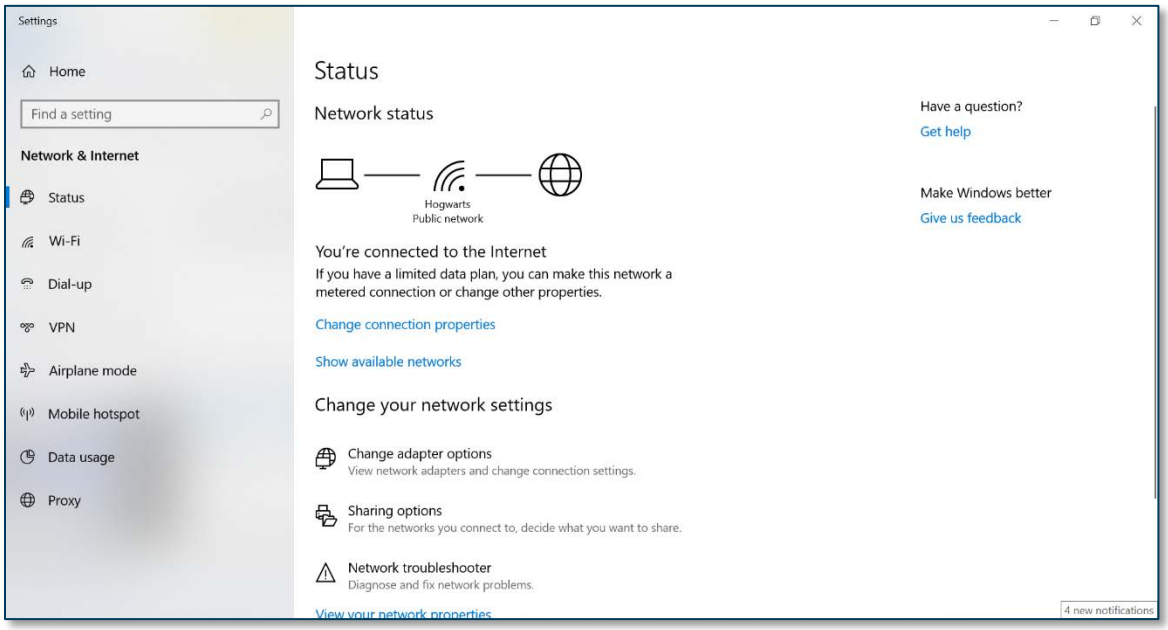


Figure 123 - Windows Network Status

4. Select *Change connection properties*. The network connection screen for the current network displays.

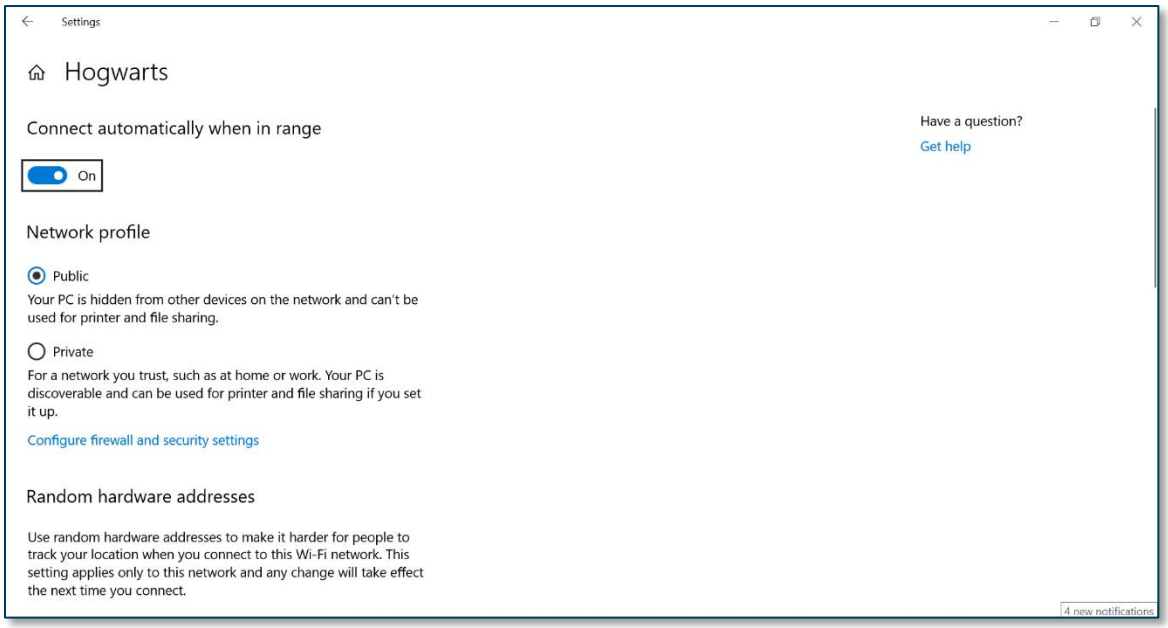


Figure 124 - Information About a Specific Network

5. If *WPA2* is listed under *Security type,* then AES is being used to secure this wireless connection.

Figure 125 - Identifying AES on Local WiFi

Viewing Accounts on a Windows 10 System

This process applies to CIS Control 16.8: Disable Any Unassociated Accounts.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “settings” in the search bar.
3. Click the search icon. Search results related to “settings” display.

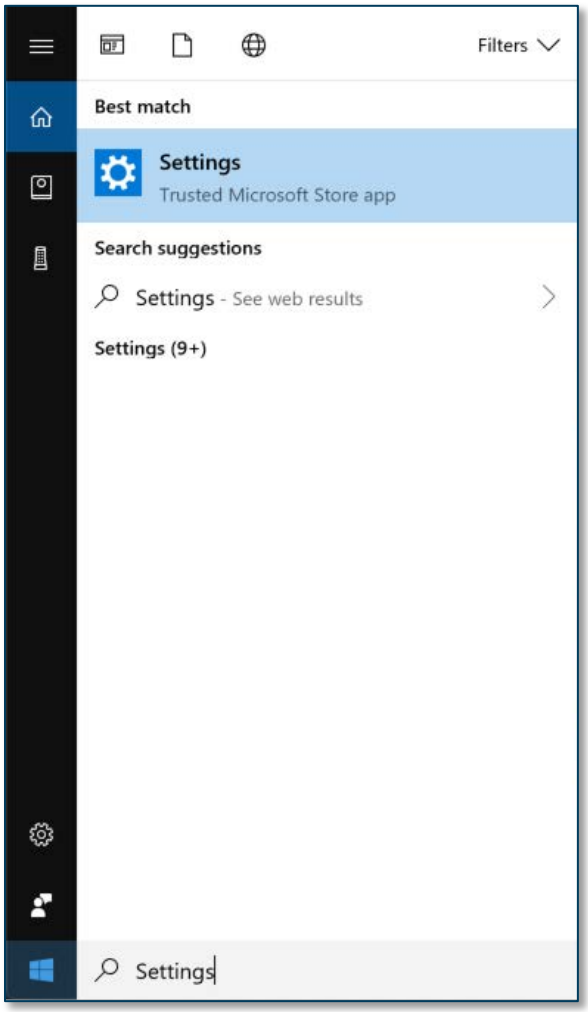


Figure 126 - Searching for Windows Settings

4. Select the Settings app. The *Windows Settings* window displays.

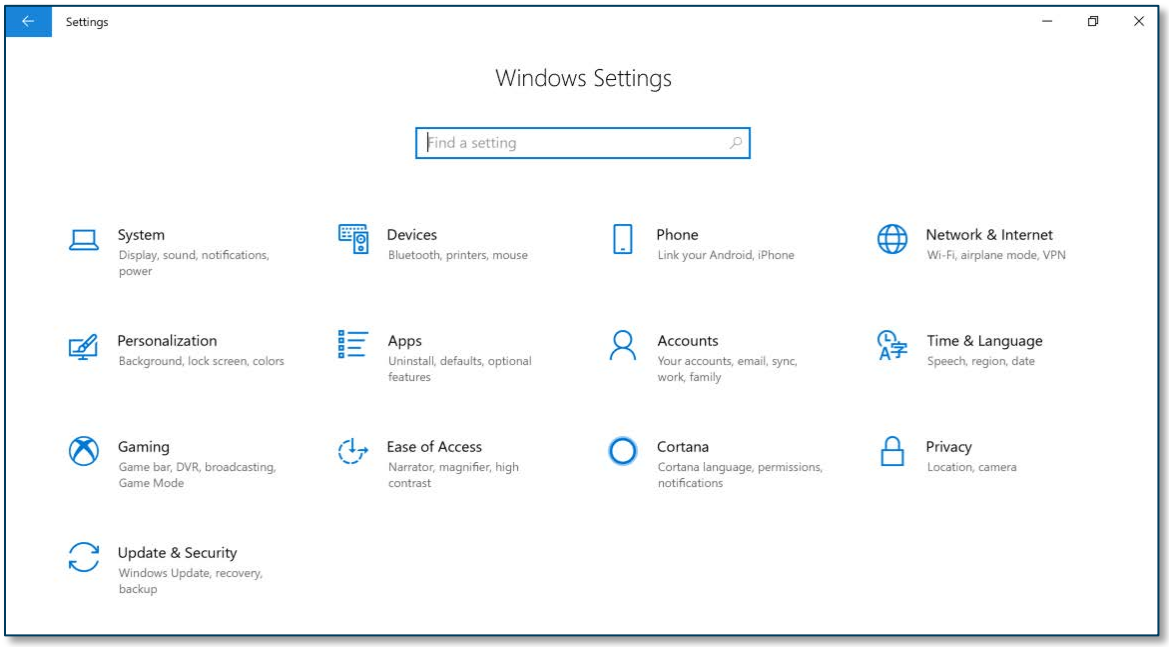


Figure 1207 - Windows Settings Home Screen

5. Select *Accounts*. The *Your info* screen opens.

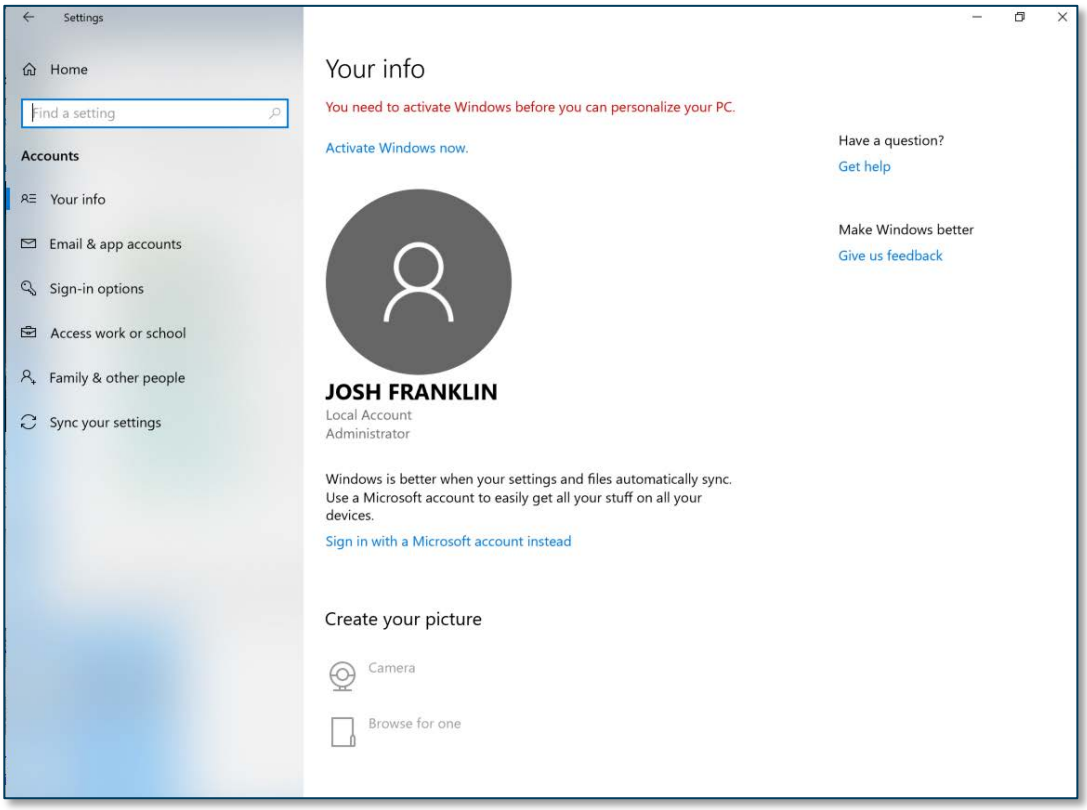


Figure 1218 - Individual Account Home Screen

6. Select *Family & other people*. The *Family & other people* screen opens. Other accounts on the computer are sometimes viewable on this screen. If the user viewing this display is not an administrator, they may not be able to see all the accounts on the system.

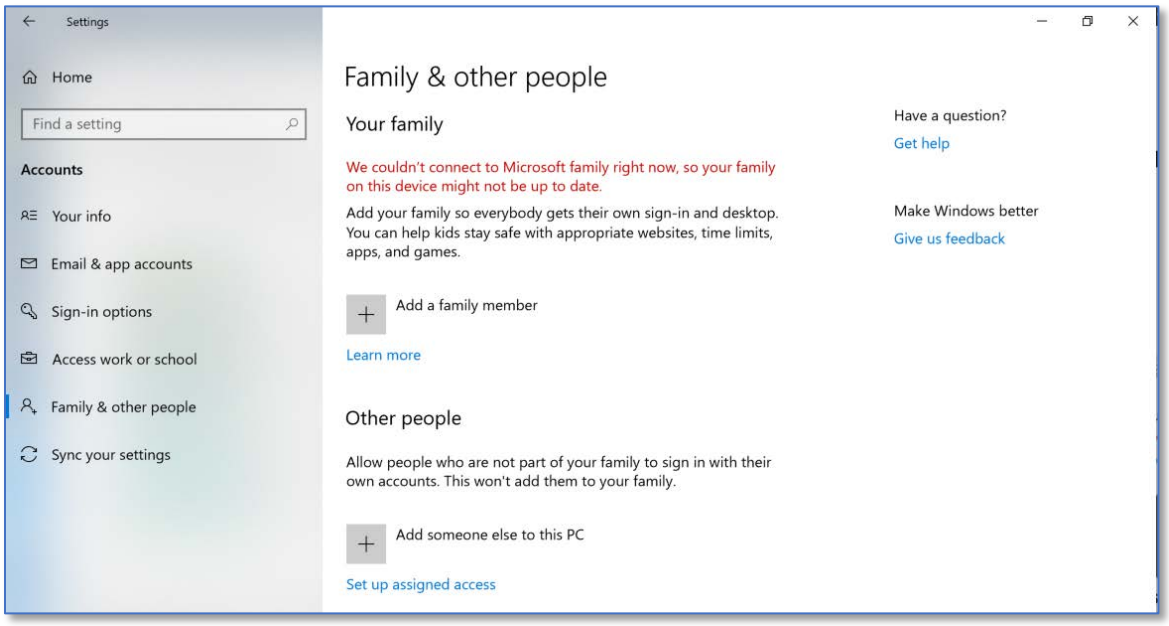


Figure 1228 - Identifying Other Accounts on Windows

Automatically Locking a Workstation

This process applies to CIS Control 16.11: Lock Workstation Sessions After Inactivity. Use these steps to automatically lock a workstation following a set period of inactivity.

1. Click the Windows *Start* button. The Windows Start menu displays with the search bar.
2. Enter “local group” in the search bar. Search results for “local group” display.

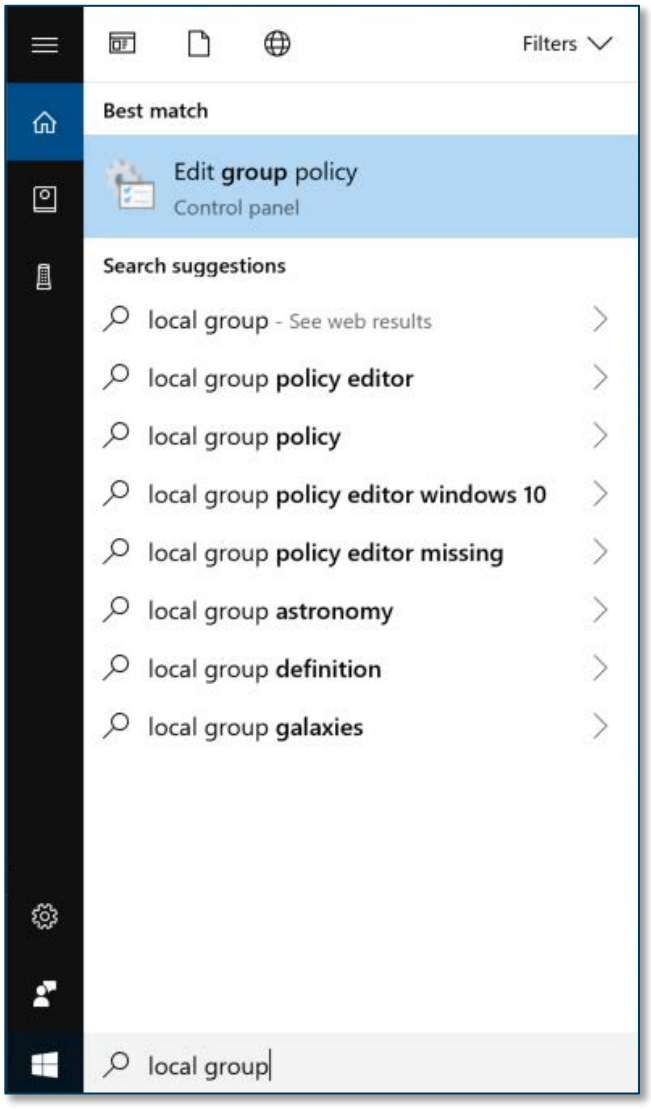


Figure 12330 - Searching for LGPE

3. Select “Edit group policy: in the search list. The *Local Group Policy Editor Home Screen* displays.

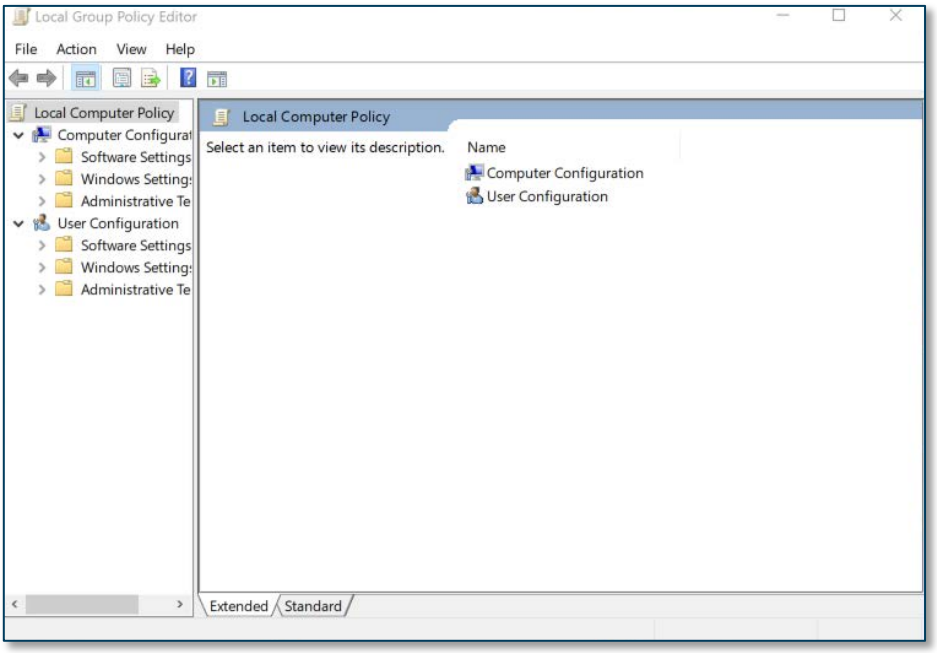


Figure 131 – LGPE Home Screen

4. Select *Computer Configurations* and then *Windows Settings*. The Windows settings display.

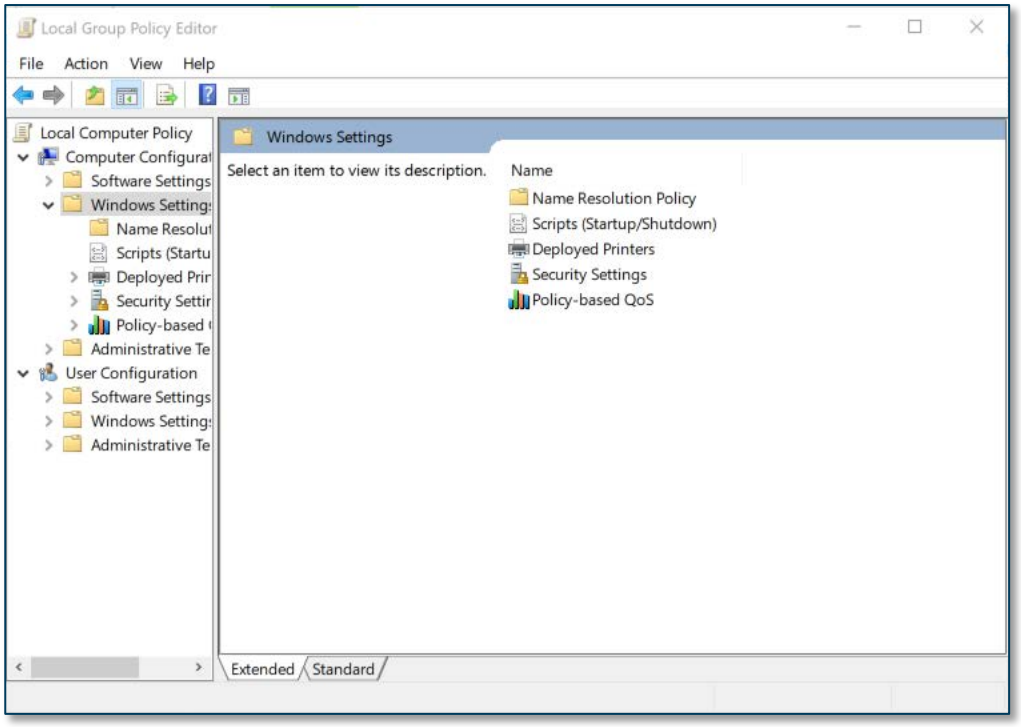


Figure 1242 - LGPE Windows Settings

5. Select *Security Settings* and then *Local Policies*.

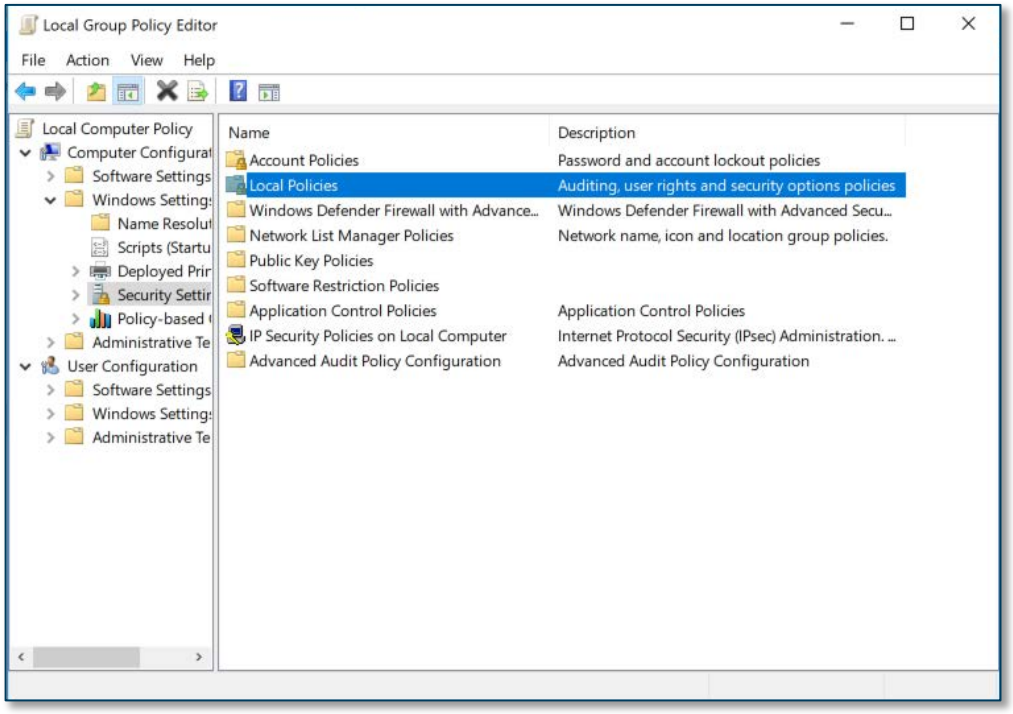


Figure 1253 - LGPE Local Policies

6. Select *Security Options* and then double click *Interactive logon: Machine interactivity limit*. The *Interactive logon: Machine inactivity limit Properties* window displays.

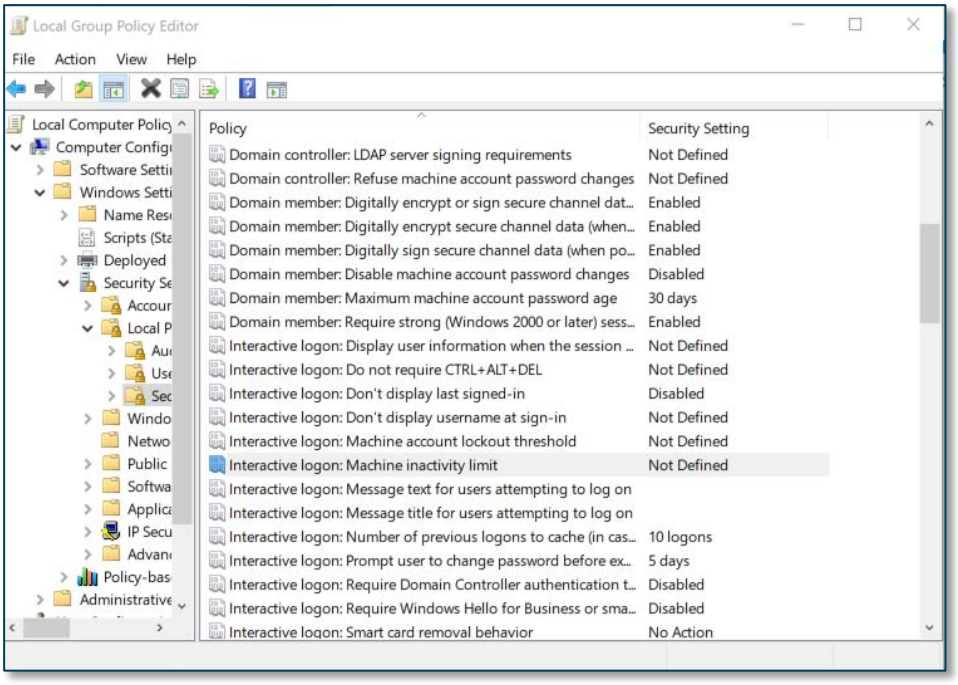


Figure 1264- Selecting Interactive Logon Settings

7. Enter the inactivity time limit (in seconds). The CIS Windows 10 Benchmark recommends 900 seconds or fewer. In this case, 600 seconds is 10 minutes.

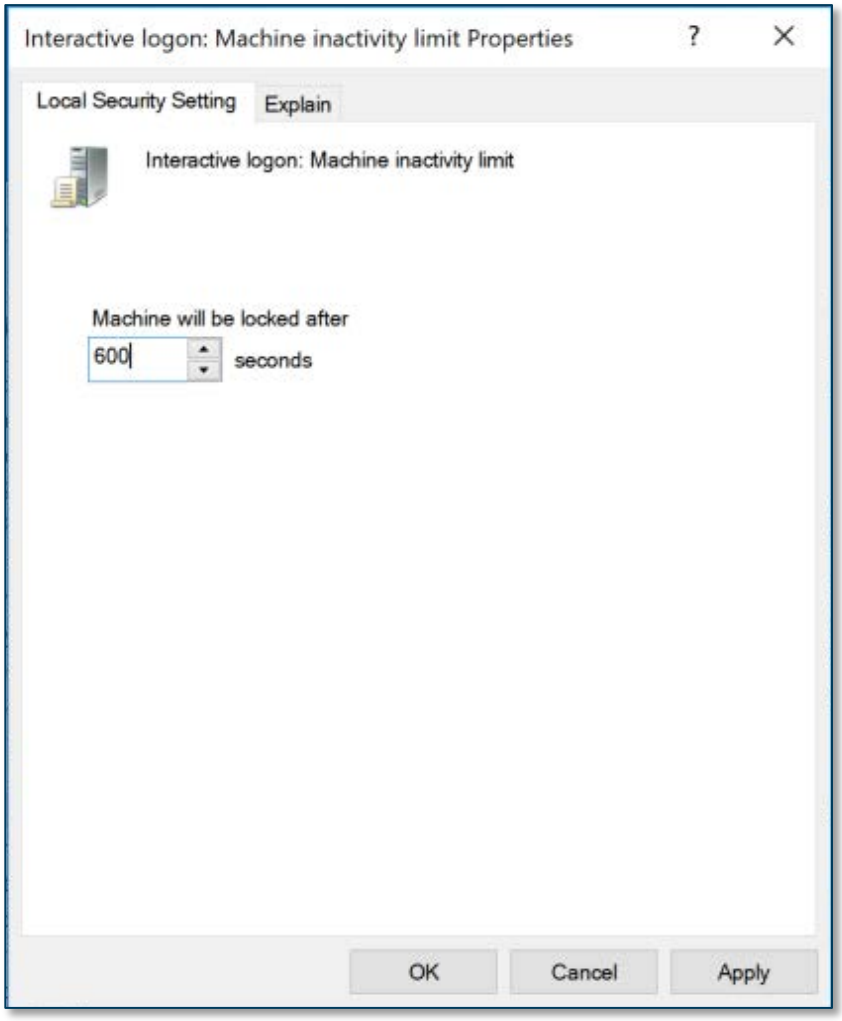


Figure 127 - Interactive Logon Settings

8. Click OK.

About This Document

In this document, guidance is provided on how to apply the security best practices found in CIS Controls Version 7.1 to Windows 10 Pro environments. As a non-profit driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at controlsinfo@cisecurity.org.

CIS is using an alternative format to host this document in order to keep up with the quick changes in the cybersecurity space to that end, visit https://www.cisecurity.org/controls/ to find the most up to date version of this document. Feel free to reach out to us at controlsinfo@cisecurity.org for any questions.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org