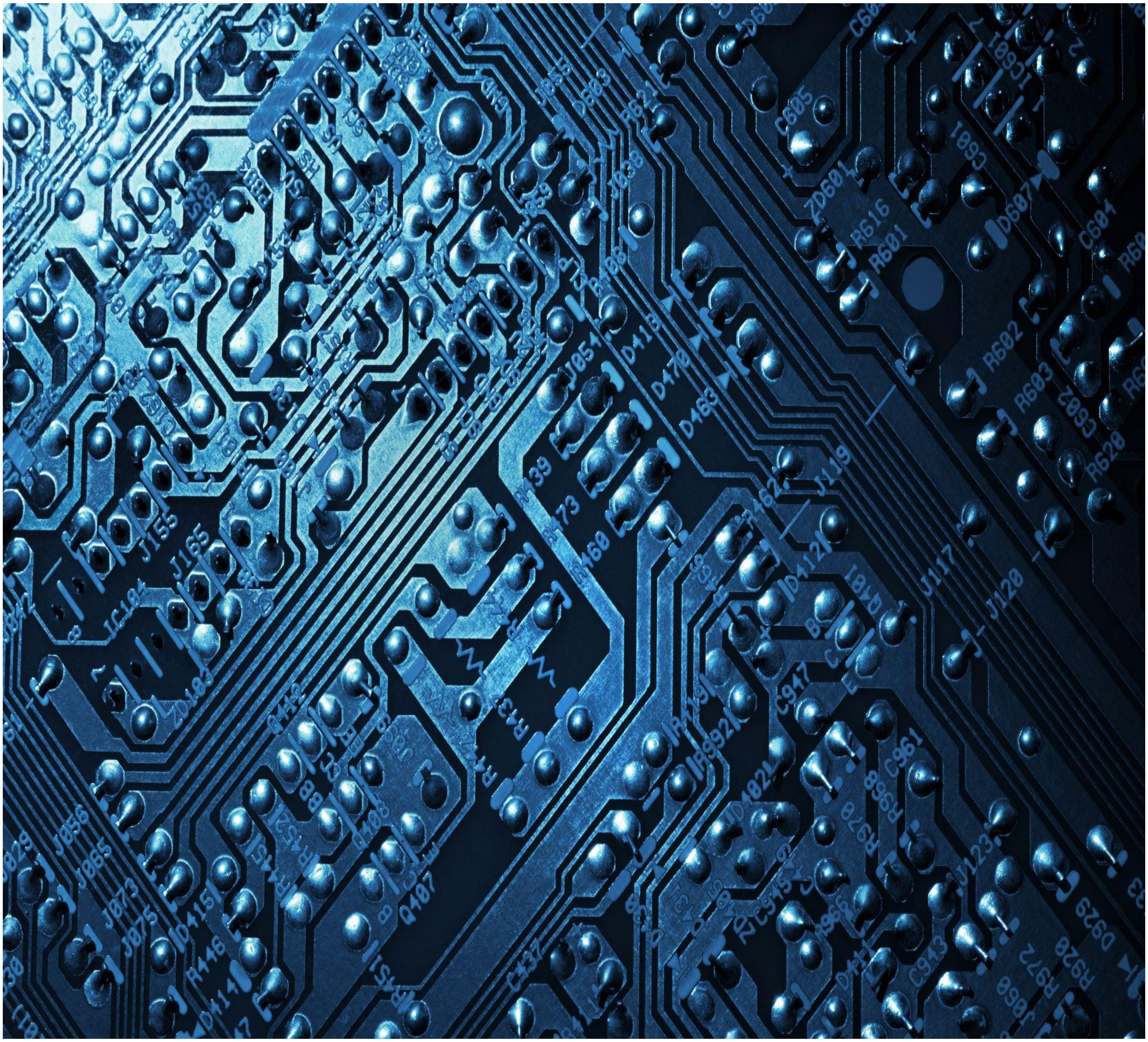
ASSIGNMENT 4

Policies, Backup & Recovery



OSYS 1200 – Intro to Windows Administration
Samantha Best - W0279169
Due November 1st, 2023

Contents

Introduction 3

Task 1 – Security Policies 3

Part 1 – Security with Group Policies 3

Account Lockout 3

Password Policy 4

Secure Boot 4

Windows Automatic Update 5

Part 2 – Audit Policies 6

Advanced Audit Policies 6

Audit Failed Logon Attempts 6

Audit Failed Attempts to Access Shared Files 7

Successful and Failed Changes Made to Security Groups 7

Event Viewer added to custom MMC – Failed to logon as “ABruce” 10

SuccessfulAudit.txt (Event 4719) 11

Event ID 4625 - “ABruce” logon: 2 Failed Attempts 12

Windows PowerShell (elevated) – Get-EventLog 12

FailureAudit.txt 12

Task 2 – Security and Maintenance Center 13

Security and Maintenance Center 13

Change Maintenance Settings 14

Question 1: Network Firewall and Virus Protection 14

Firewall and Network Protection - Domain, Private & Public 15

Question 2: User Account Controls 16

User Account Controls - Modified 17

Task 3 – File backup and Recovery 18

Backup ABruce_Files to Data (F:) 18

Delete ABruce_Files from “E:\CompanyInc\Management” 19

New Backup 20

Restore Previous Version using File History 20

Question 3: Restoring deleted file and NOT entire folder: 20

Previous Version Restored 22

Snapshot PostA4 23

Gold Copy (2 copies) 24

Scripts 26

Resources 26

Conclusion .... **Error! Bookmark not defined.**

Introduction

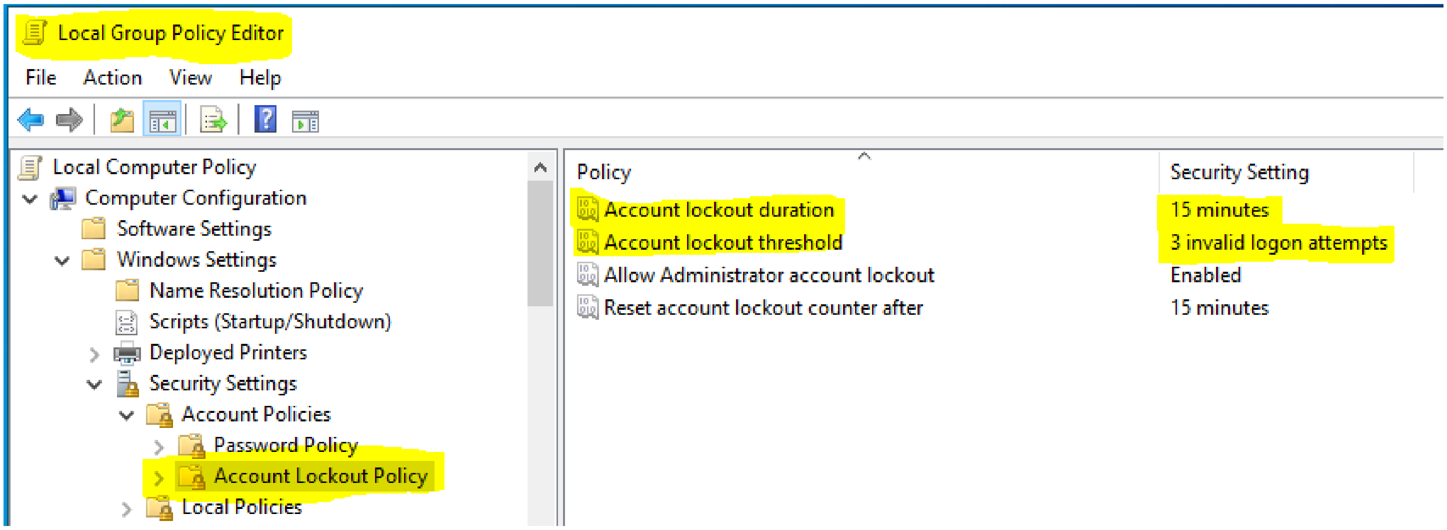
In this assignment, Group Policy Password configurations and Auditing events are initialized and explored using the GUI and Windows PowerShell, as well as scheduling Automatic Windows Updates, setting a Maintenance schedule, and modifying the User Access Controls in Windows Settings. Backups and restoring previous versions demonstrated using File History.

Task 1 – Security Policies

Part 1 – Security with Group Policies

Account Lockout

In the Local Group Policy Editor under "Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy", the Account Lockout Duration and Account Lockout Threshold have been changed. These can also be edited in the **"Local Security Policy**" but are **only effective on local devices** and not a domain.

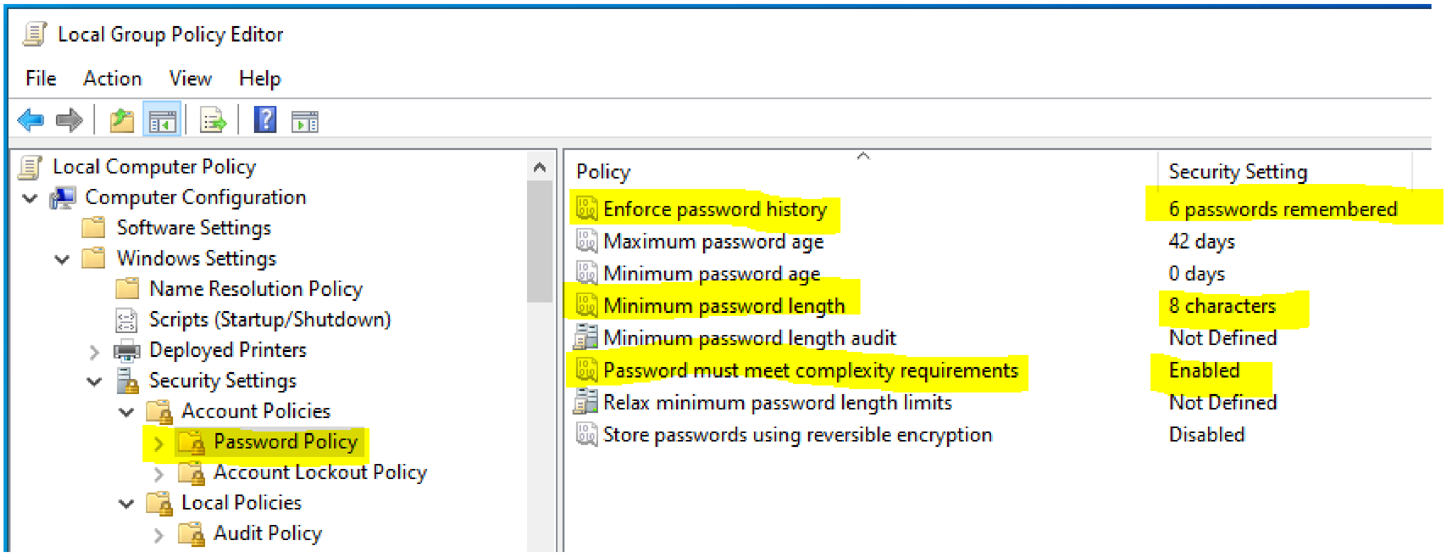


Policy	Security Setting
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	15 minutes

Shown above is the **Account Lockout Duration** set to **"15 minutes"** and the **"Account Lockout Threshold"** set to "**3 invalid logon attempts**".

Password Policy

In the Local Group Policy Editor underneath “Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy”, the Password Policies have been modified.

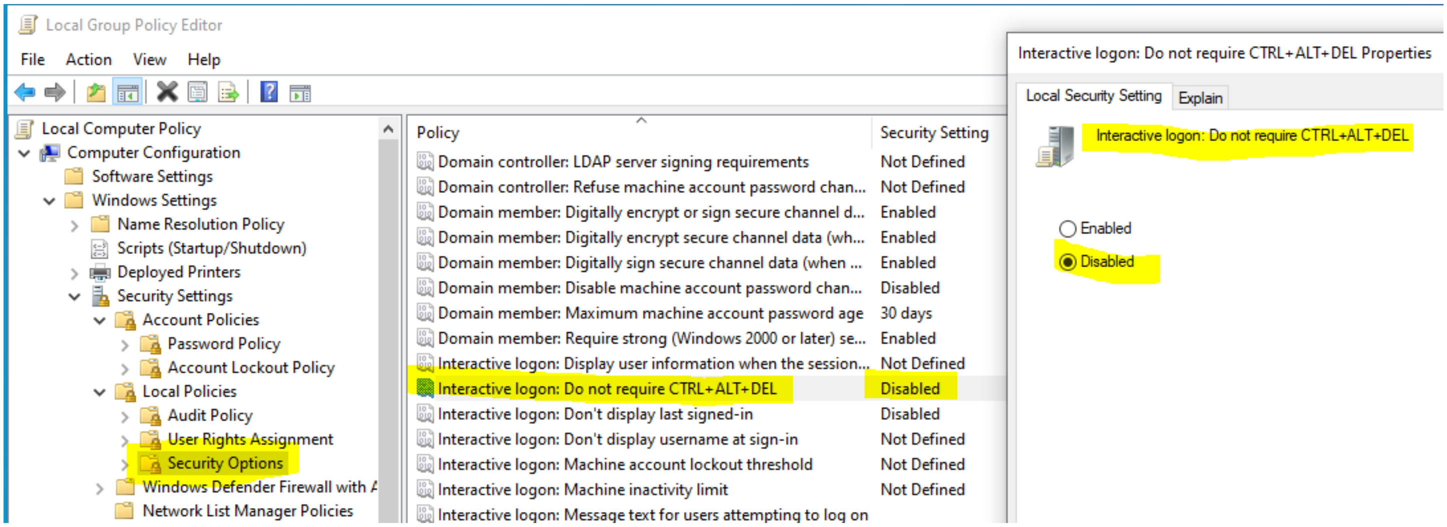


Policy	Security Setting
Enforce password history	6 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	8 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

“Enforce Password History” is now set to 6 passwords remembered, the **“Minimum password length”** is 8 characters, and the “**Password must meet complexity requirements”** is enabled.

Secure Boot

In the Local Group Policy Editor underneath “Security Settings > Local Policies > Security Options”, the “**Interactive logon: Do not require CTRL+ALT+DEL” has been set to “disabled”.** This enables secure boot.



Policy	Security Setting
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	

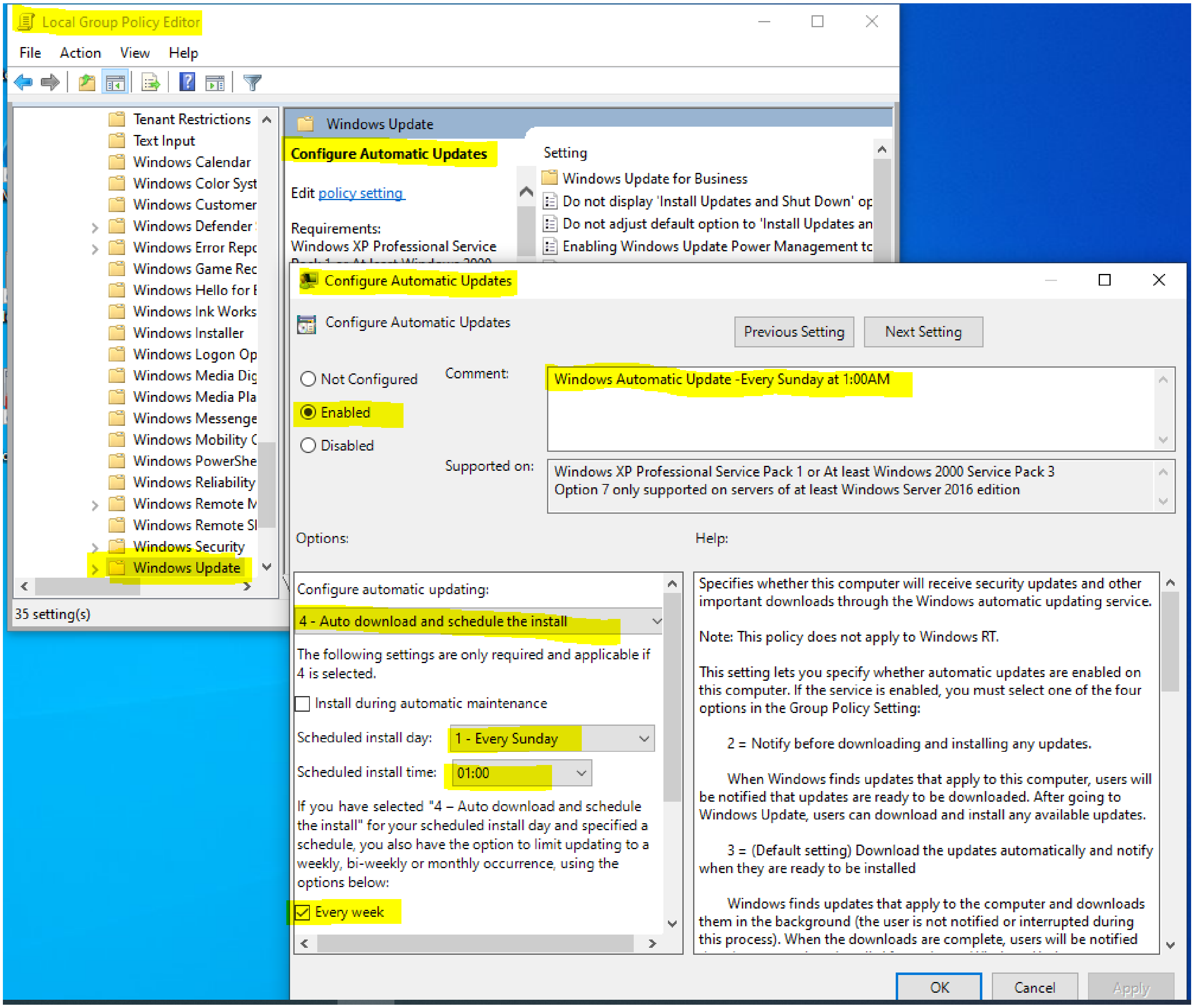
Interactive logon: Do not require CTRL+ALT+DEL

○ Enabled
● Disabled

“Interactive logon: Do not require CTRL+ALT+DEL” set to **DISABLED** in the Local Group Policy Editor. In the VMware application, “**CTRL + ALT + DEL**” for logon can be accessed without making the Host PC open the “Task Manager” by using “**CTRL + ALT + INSERT**” instead and will work the same as CTRL+ALT+DEL. *(VMware pushed a notification regarding CTRL+ALT+DEL and CTRL+ALT+INSERT when using the virtual machine)*

Windows Automatic Update

In the Local Group Policy Editor, inside “Computer Configuration > Administrative Templates > Windows Components > Windows Update” the setting **“Configure Automatic Updates”** is located.



Configure Automatic Updates

Requirements:
Windows XP Professional Service Pack 1 or At least Windows 2000

Configure Automatic Updates

○ Not Configured
● Enabled
○ Disabled

Comment: Windows Automatic Update -Every Sunday at 1:00AM

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3
Option 7 only supported on servers of at least Windows Server 2016 edition

Options:

Configure automatic updating: 4 - Auto download and schedule the install

The following settings are only required and applicable if 4 is selected.

☐ Install during automatic maintenance

Scheduled install day: 1 - Every Sunday

Scheduled install time: 01:00

If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

☑ Every week

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and downloads them in the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified

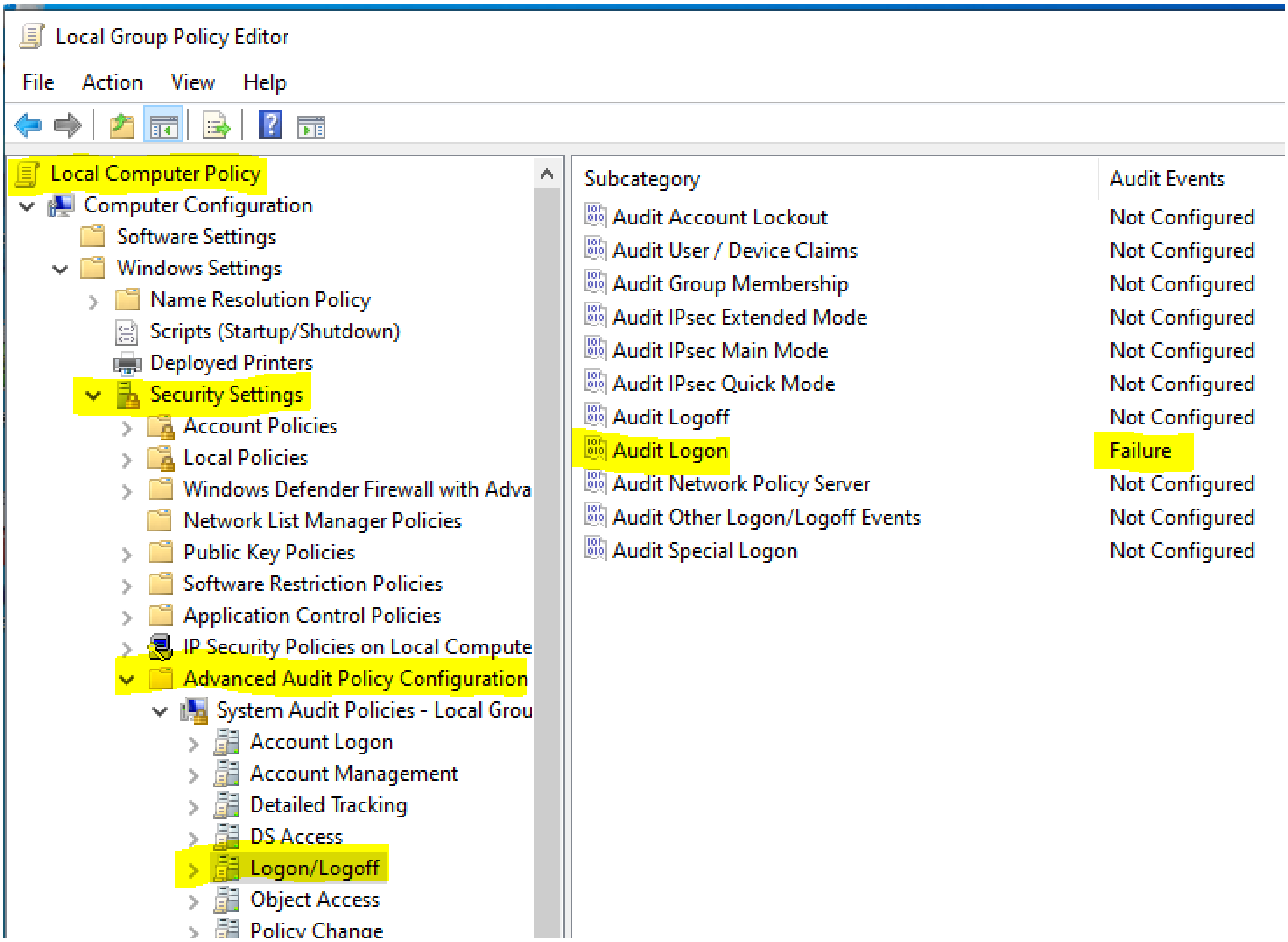
Windows Update was configured to **automatically download and install every Sunday at 1:00:00AM.**

Part 2 – Audit Policies

Advanced Audit Policies

Audit Failed Logon Attempts

In the Local Group Policy Editor under “Computer Configuration > Windows Settings > Security Settings > **Advanced Audit Policy Configuration** > System Audit Policies – Local Group Policy > **Logon/Logoff”**, the **“Audit Logon”** subcategory will be audited during a **“Failure”** or **failed logon attempt**.

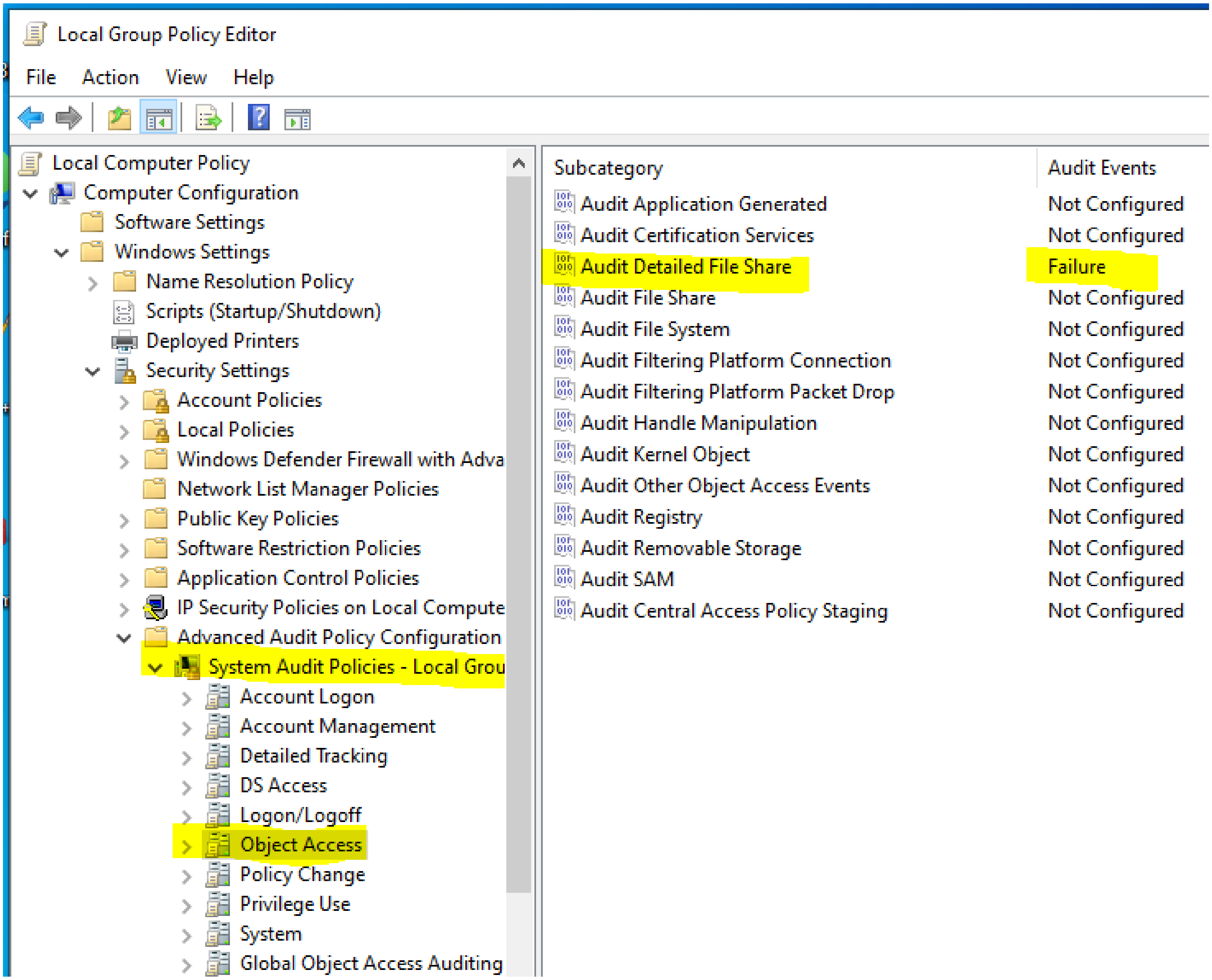


Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

Shown above, the **“Audit Logon”** has been set to failure. This will produce an audit event for all failed logon attempts. For a **network** logon, such as accessing a shared folder, the security audit event is generated on the computer that hosts the resource, for **an interactive logon**, the audit event **is generated on the computer that was accessed.** *(Audit Logon Properties, Windows 10).*

In relation to this, I happened upon the “Account Logon” subsection above and found the “Audit Credential Validation” subcategory. The explanation of this says *“Events in this subcategory occur only on the computer that is authoritative for those credentials. For domain accounts, the domain controller is authoritative. For local accounts, the computer is authoritative.”* *(Audit Credential Validation Properties, Windows 10).* I feel that in a domain or network environment, this setting may be more appropriate instead of using the “Audit Logon” in the “Logon/Logoff” subcategory, since the **Domain Controller** will receive the audit events, as compared to the “Audit Logon” being stored on the local PC, or only being sent to the host PC on a network for a failed logon attempt to access a shared folder. This could probably be configured to send the audit reports wherever required, though it may be more complicated.

Audit Failed Attempts to Access Shared Files

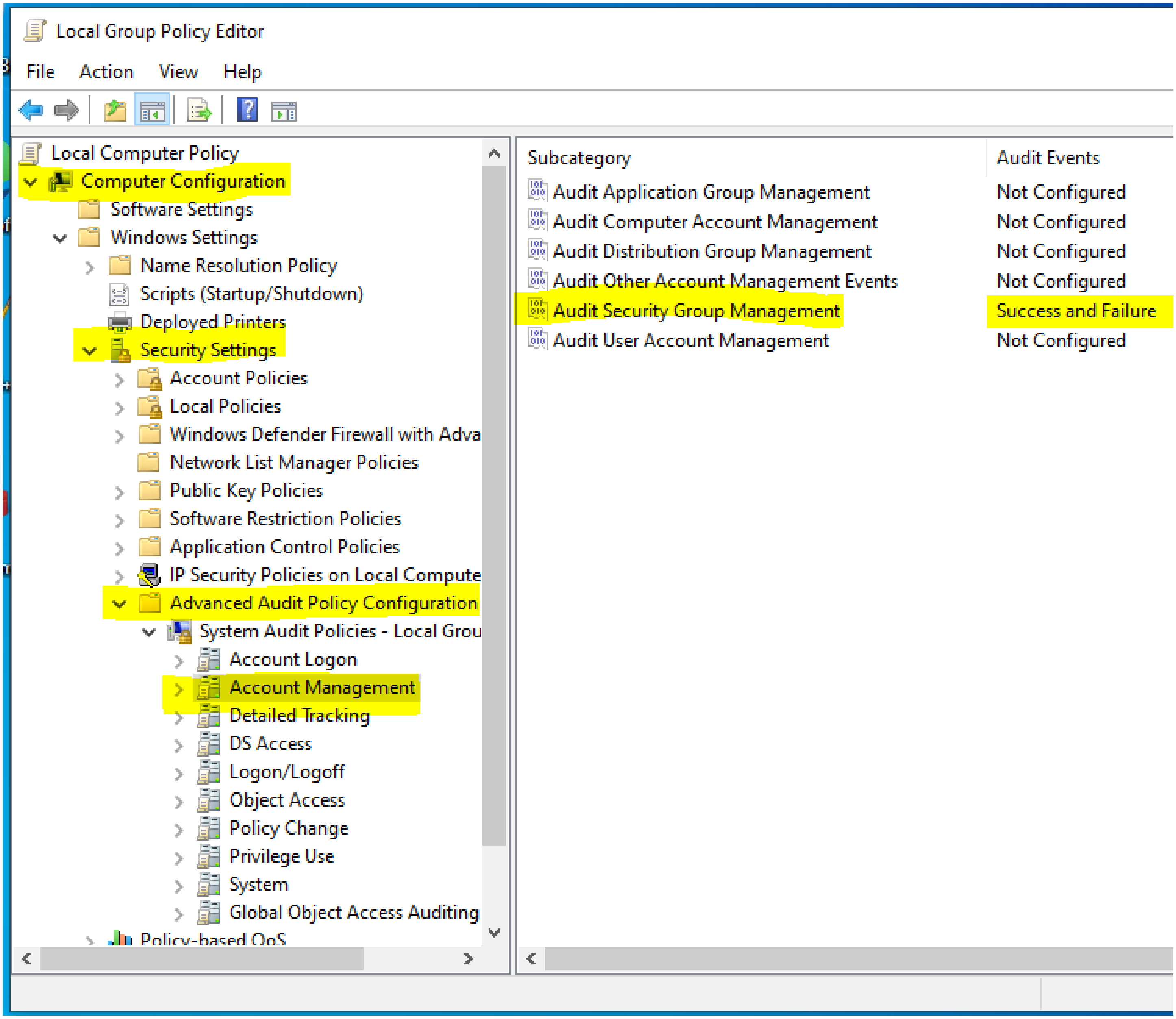


Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Failure
Audit File Share	Not Configured
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

In the Local Group Policy Editor under “Computer Configuration > Windows Settings > Security Settings > **Advanced Audit Policy Configuration** > System Audit Policies – Local Group Policy > **Object Access”**, the **“Audit Detailed File Share”** subcategory will be audited during a **“Failure”** or **failed attempts to access shared files.** The **other options** are “Audit File Share”, and “Audit File Share System”. The “Audit File Share System” will only audit if there is System Access Control Lists (SACLs) on the shared folders that have attempted access. *(Audit Detailed File Share Properties, Windows 10)*

Successful and Failed Changes Made to Security Groups

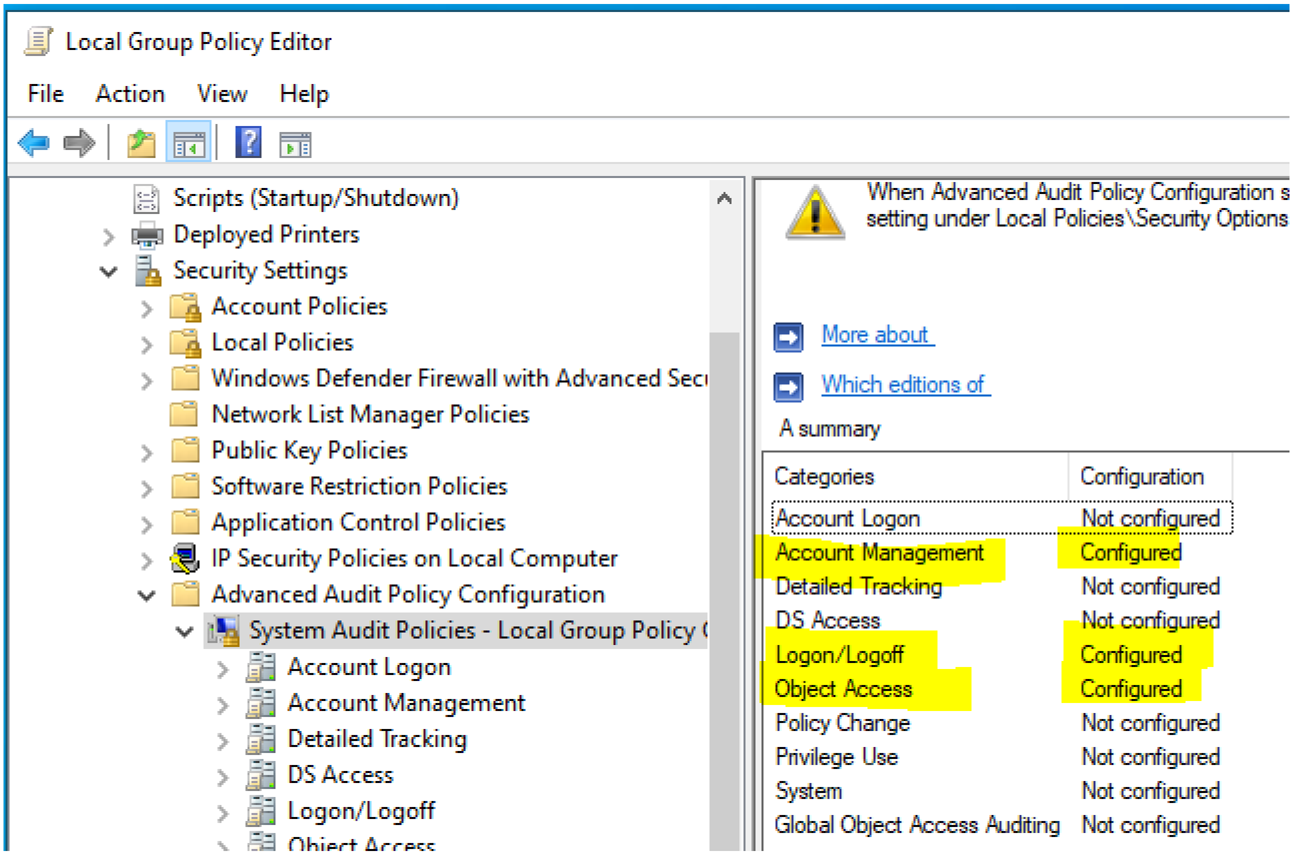
In the Local Group Policy Editor under “Computer Configuration > Windows Settings > Security Settings > **Advanced Audit Policy Configuration** > System Audit Policies – Local Group Policy > **Account Management”**, the **“Audit Security Group Management”** has been set to audit **successful and failed** events.



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Defender Firewall with Adva
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Compute
        - Advanced Audit Policy Configuration
          - System Audit Policies - Local Grou
            - Account Logon
            - Account Management
            - Detailed Tracking
            - DS Access
            - Logon/Logoff
            - Object Access
            - Policy Change
            - Privilege Use
            - System
            - Global Object Access Auditing
      - Policy-based QoS

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Not Configured
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Success and Failure
Audit User Account Management	Not Configured

Shown above, the "success and failure" will audit changes to security groups including when a **security group is created, changed, or deleted.** If a member is **added or removed** from a security group, and if a **Group type is changed**. *(Audit Security Group Management Properties, Windows 10)*


Local Group Policy Editor
File
Action
View
Help
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Policy (
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
More about
Which editions of

When Advanced Audit Policy Configuration s
setting under Local Policies\Security Options

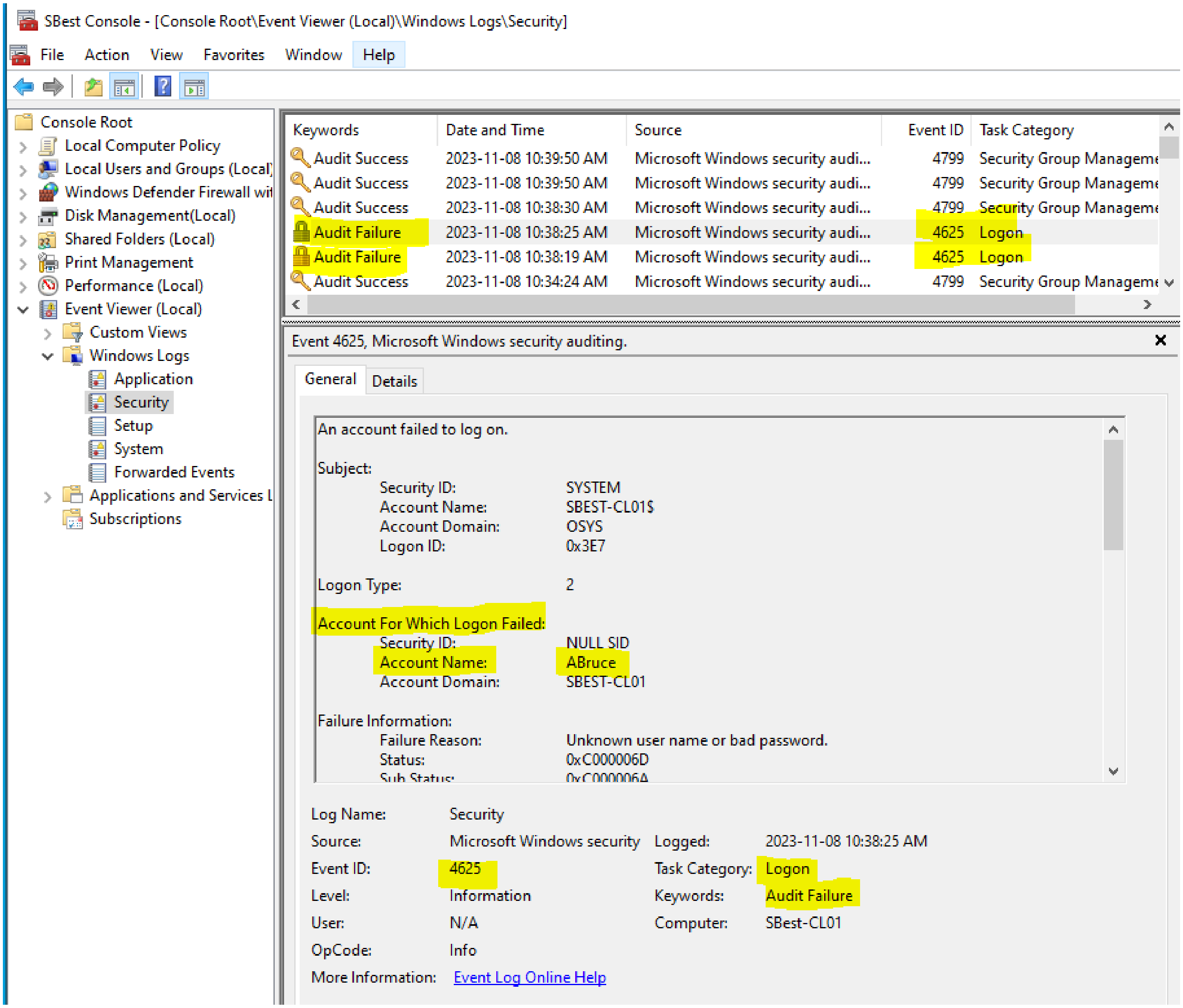
A summary

Categories	Configuration
Account Logon	Not configured
Account Management	Configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Configured
Object Access	Configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Shown above is the **"Local Group Policy Editor"** displaying the 3 Auditing requirements (**Failed logon attempts, failed attempts to access shared files, and successful and failed changes made to security groups**) have been configured.

Event Viewer added to custom MMC – Failed to logon as “ABruce”

In Event Viewer in the MMC, when exploring the “**Windows Logs > Security**” section after two logon failures on the “**ABruce**” user account, the **EVENT ID** for “**Logon” failure** is **4625**. Upon investigating further, the **Event ID 4719** appears when the ***System Audit Policy is changed.*** After failing to logon as **“ABruce”** the **Event ID** is **4625.** See three screenshots below.



SBest Console - [Console Root\Event Viewer (Local)\Windows Logs\Security]

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2023-11-08 10:39:50 AM	Microsoft Windows security audi...	4799	Security Group Manageme
Audit Success	2023-11-08 10:39:50 AM	Microsoft Windows security audi...	4799	Security Group Manageme
Audit Success	2023-11-08 10:38:30 AM	Microsoft Windows security audi...	4799	Security Group Manageme
Audit Failure	2023-11-08 10:38:25 AM	Microsoft Windows security audi...	4625	Logon
Audit Failure	2023-11-08 10:38:19 AM	Microsoft Windows security audi...	4625	Logon
Audit Success	2023-11-08 10:34:24 AM	Microsoft Windows security audi...	4799	Security Group Manageme

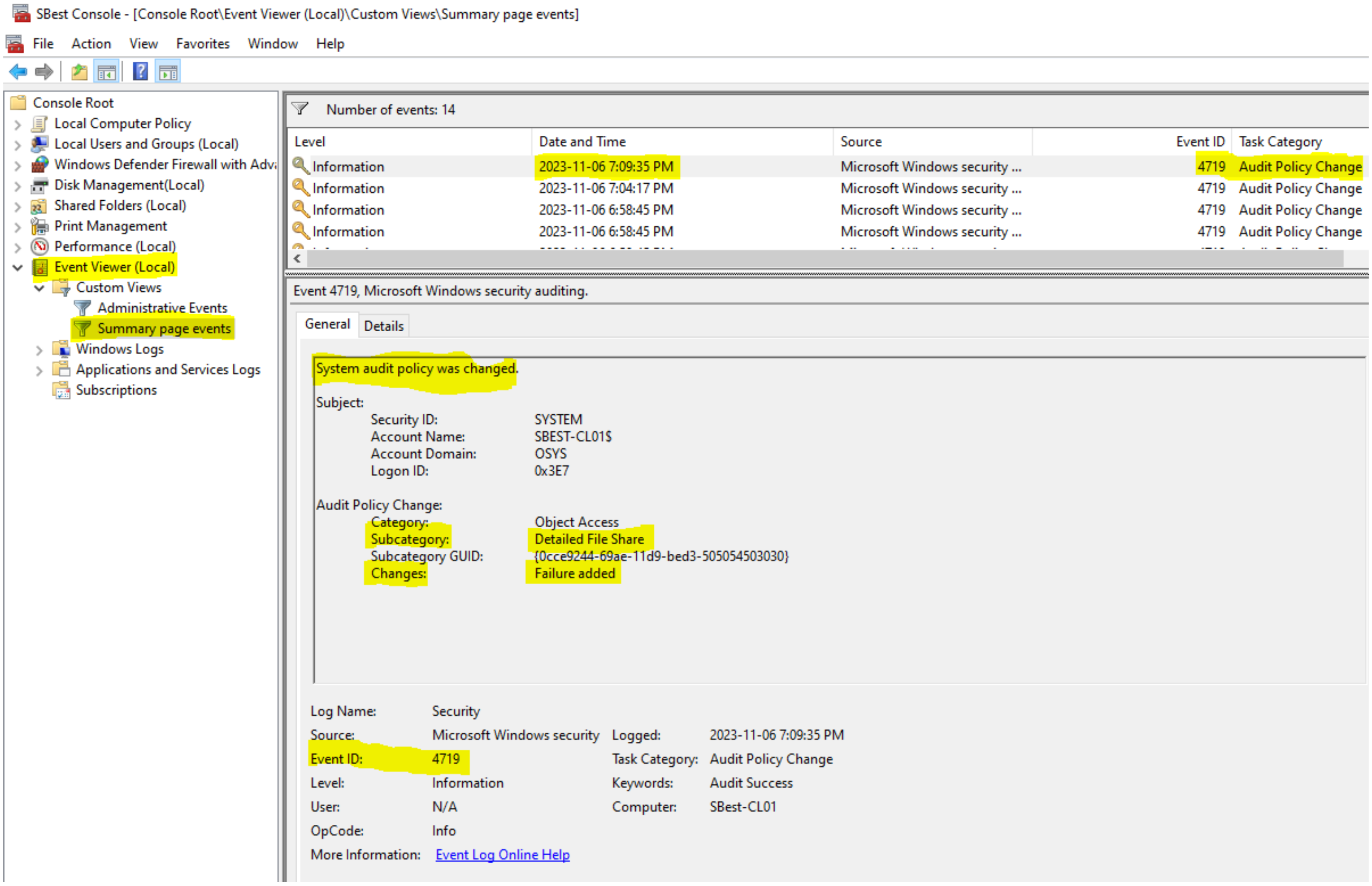
Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
	Security ID:		SYSTEM
	Account Name:		SBEST-CL01$
	Account Domain:		OSYS
	Logon ID:		0x3E7

Logon Type:			2

Account For Which Logon Failed:
	Security ID:		NULL SID
	Account Name:		ABruce
	Account Domain:		SBEST-CL01

Failure Information:
	Failure Reason:		Unknown user name or bad password.
	Status:			0xC000006D
	Sub Status:		0xC000006A
```

Log Name: Security
Source: Microsoft Windows security
Logged: 2023-11-08 10:38:25 AM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: SBest-CL01
OpCode: Info
More Information: Event Log Online Help

Event Viewer > Windows Logs > Security > Filter By “**Event 4625**” > Sort By “Date and Time”.

Event ID 4719 – Audit Policy Changed



Number of events: 14

Level	Date and Time	Source	Event ID	Task Category
Information	2023-11-06 7:09:35 PM	Microsoft Windows security ...	4719	Audit Policy Change
Information	2023-11-06 7:04:17 PM	Microsoft Windows security ...	4719	Audit Policy Change
Information	2023-11-06 6:58:45 PM	Microsoft Windows security ...	4719	Audit Policy Change
Information	2023-11-06 6:58:45 PM	Microsoft Windows security ...	4719	Audit Policy Change

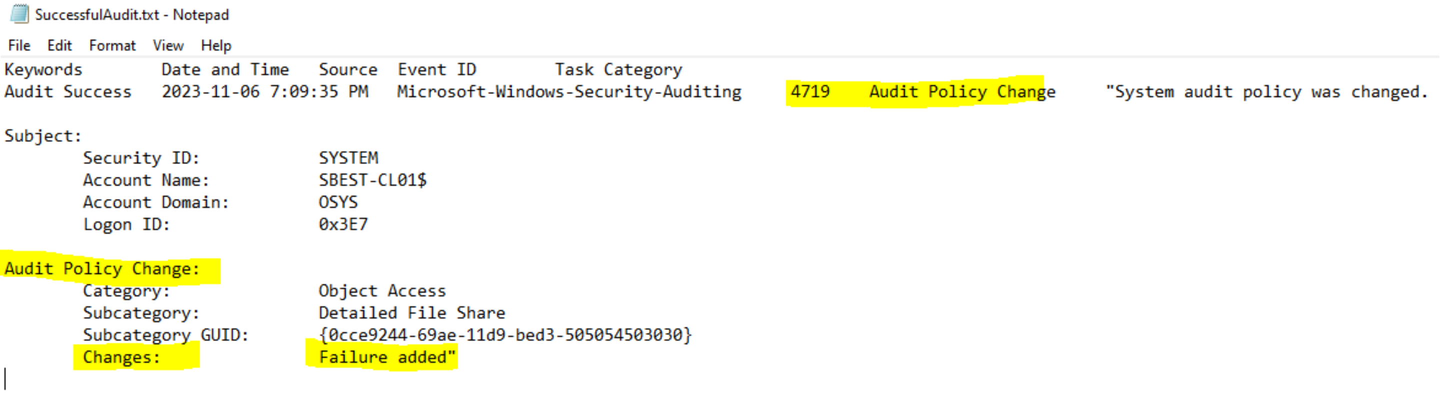
Event 4719, Microsoft Windows security auditing.

```
System audit policy was changed.

Subject:
        Security ID:            SYSTEM
        Account Name:           SBEST-CL01$
        Account Domain:         OSYS
        Logon ID:               0x3E7

Audit Policy Change:
        Category:               Object Access
        Subcategory:            Detailed File Share
        Subcategory GUID:       {0cce9244-69ae-11d9-bed3-505054503030}
        Changes:                Failure added
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2023-11-06 7:09:35 PM
Event ID:	4719	Task Category:	Audit Policy Change
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	SBest-CL01
OpCode:	Info		
More Information:	Event Log Online Help		

Shown above is the **Event Viewer** in the custom MMC. Events were filtered by **date** and **Event ID 4719.** This is showing the **"System audit policy" was changed**. The change made was "**Failure added".**

SuccessfulAudit.txt (Event 4719)

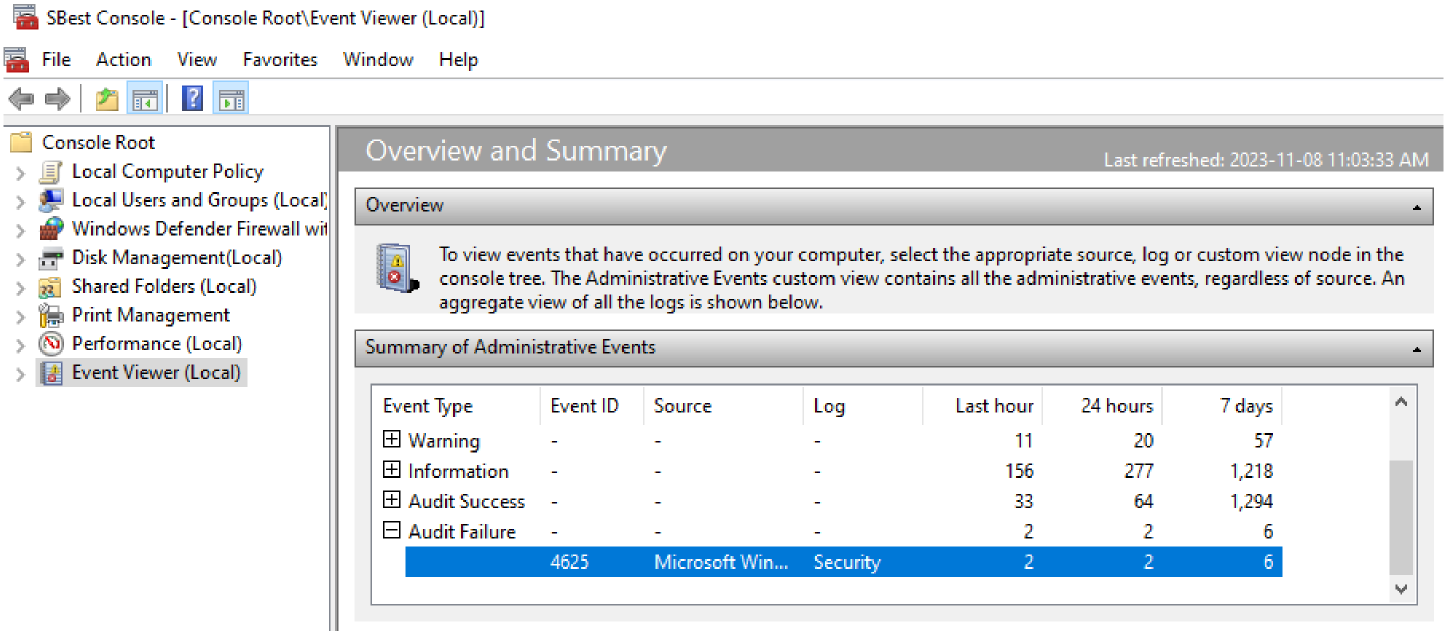


```
Keywords       Date and Time    Source   Event ID         Task Category
Audit Success  2023-11-06 7:09:35 PM  Microsoft-Windows-Security-Auditing    4719     Audit Policy Change     "System audit policy was changed.

Subject:
        Security ID:            SYSTEM
        Account Name:           SBEST-CL01$
        Account Domain:         OSYS
        Logon ID:               0x3E7

Audit Policy Change:
        Category:               Object Access
        Subcategory:            Detailed File Share
        Subcategory GUID:       {0cce9244-69ae-11d9-bed3-505054503030}
        Changes:                Failure added"
```

Shown above is the .txt file for the **"SuccessfulAudit"** saved from "**Event Viewer > Windows Logs > Security**" in the custom MMC. This was saved to **"C:\Reports\".**

Event ID 4625- “ABruce” logon: 2 Failed Attempts

The ABruce account was used to test 2 failed logon attempts.



Overview and Summary

Last refreshed: 2023-11-08 11:03:33 AM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

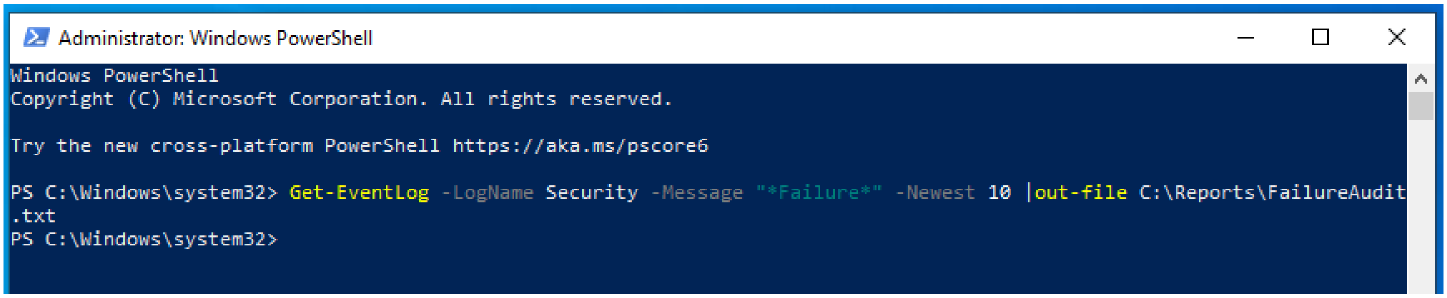
Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊞ Warning	-	-	-	11	20	57
⊞ Information	-	-	-	156	277	1,218
⊞ Audit Success	-	-	-	33	64	1,294
⊟ Audit Failure	-	-	-	2	2	6
	4625	Microsoft Win...	Security	2	2	6

After failing 2 attempts to logon as **“ABruce”,** in the Event Viewer there are 2 **“Audit Failures**” with Event ID **4625**.

Windows PowerShell (elevated) – Get-EventLog

In elevated PowerShell, the cmdlet “**Get-Event Log -LogName Security – Message “*Failure*” -Newest 10 | out-file C:\Reports\FailureAudit.txt**” was used to create a .txt file containing the 10 newest Security Logs in Event Viewer that contain the message “Failure”.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-EventLog -LogName Security -Message "*Failure*" -Newest 10 |out-file C:\Reports\FailureAudit
.txt
PS C:\Windows\system32>
```

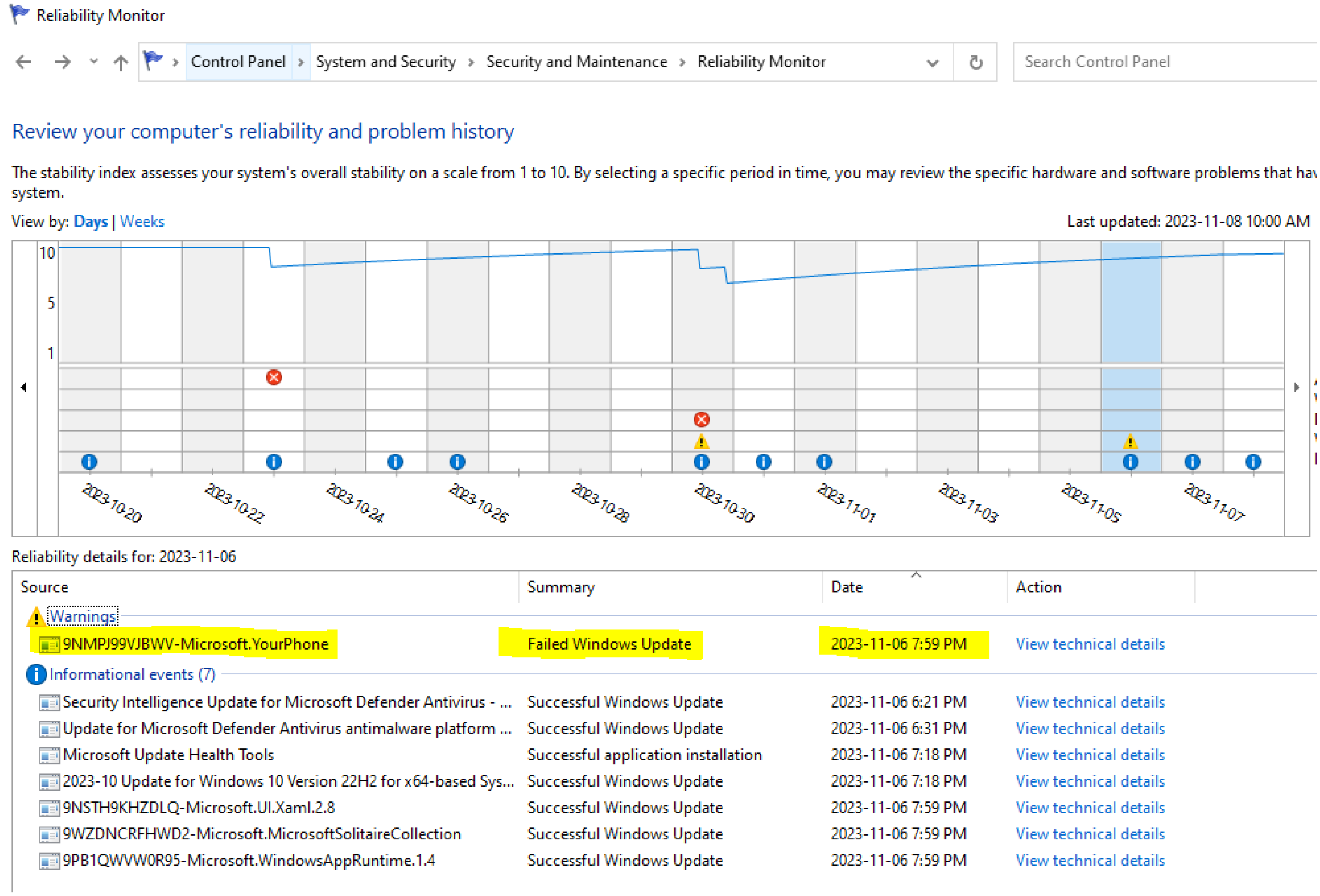
FailureAudit.txt

```
Index Time         EntryType   Source              InstanceID Message

----- ----         ---------   ------              ---------- -------

38933 Nov 08 10:38  FailureA... Microsoft-Windows...        4625 An account failed to log on....

38932 Nov 08 10:38  FailureA... Microsoft-Windows...        4625 An account failed to log on....

38607 Nov 07 08:59  FailureA... Microsoft-Windows...        4625 An account failed to log on....

38606 Nov 07 08:59  FailureA... Microsoft-Windows...        4625 An account failed to log on....

37805 Nov 01 16:36  FailureA... Microsoft-Windows...        4625 An account failed to log on....
```

```
37792 Nov 01 16:34  FailureA... Microsoft-Windows...       4625 An account failed to log on....
36501 Oct 30 11:38  FailureA... Microsoft-Windows...       4625 An account failed to log on....
36488 Oct 30 11:38  FailureA... Microsoft-Windows...       4625 An account failed to log on....
33575 Oct 30 11:31  SuccessA... Microsoft-Windows...       4907 Auditing settings on object were changed....
25863 Oct 30 11:29  SuccessA... Microsoft-Windows...       4907 Auditing settings on object were changed....
```

Task 2 – Security and Maintenance Center

Security and Maintenance Center



Reliability Monitor

Control Panel › System and Security › Security and Maintenance › Reliability Monitor
Search Control Panel

Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that hav system.

View by: Days | Weeks

Last updated: 2023-11-08 10:00 AM

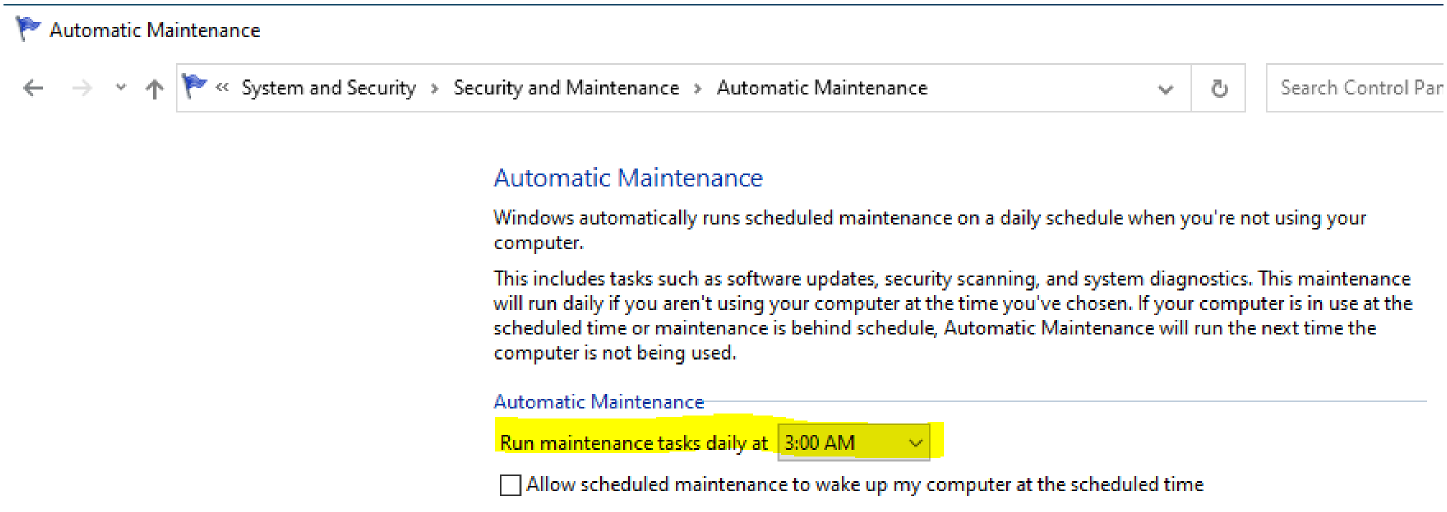
Reliability details for: 2023-11-06

Source	Summary	Date	Action
Warnings			
9NMPJ99VJBWV-Microsoft.YourPhone	Failed Windows Update	2023-11-06 7:59 PM	View technical details
Informational events (7)			
Security Intelligence Update for Microsoft Defender Antivirus - ...	Successful Windows Update	2023-11-06 6:21 PM	View technical details
Update for Microsoft Defender Antivirus antimalware platform ...	Successful Windows Update	2023-11-06 6:31 PM	View technical details
Microsoft Update Health Tools	Successful application installation	2023-11-06 7:18 PM	View technical details
2023-10 Update for Windows 10 Version 22H2 for x64-based Sys...	Successful Windows Update	2023-11-06 7:18 PM	View technical details
9NSTH9KHZDLQ-Microsoft.UI.Xaml.2.8	Successful Windows Update	2023-11-06 7:59 PM	View technical details
9WZDNCRFHWD2-Microsoft.MicrosoftSolitaireCollection	Successful Windows Update	2023-11-06 7:59 PM	View technical details
9PB1QWVW0R95-Microsoft.WindowsAppRuntime.1.4	Successful Windows Update	2023-11-06 7:59 PM	View technical details

Shown above is a warning on **November 6th** when Windows failed to update. **October 30th error** was when I pulled my SSD out while my VM was running 😊 *(I'll try to not do that again)*.

Change Maintenance Settings

In “Start Menu > Security and Maintenance > **Automatic Maintenance**”, the maintenance task was set to run **daily at 3:00am** and will **not** wake the computer to run the tasks.


Automatic Maintenance
« System and Security › Security and Maintenance › Automatic Maintenance
Search Control Par

Automatic Maintenance

Windows automatically runs scheduled maintenance on a daily schedule when you're not using your computer.

This includes tasks such as software updates, security scanning, and system diagnostics. This maintenance will run daily if you aren't using your computer at the time you've chosen. If your computer is in use at the scheduled time or maintenance is behind schedule, Automatic Maintenance will run the next time the computer is not being used.

Automatic Maintenance

Run maintenance tasks daily at 3:00 AM

□ Allow scheduled maintenance to wake up my computer at the scheduled time

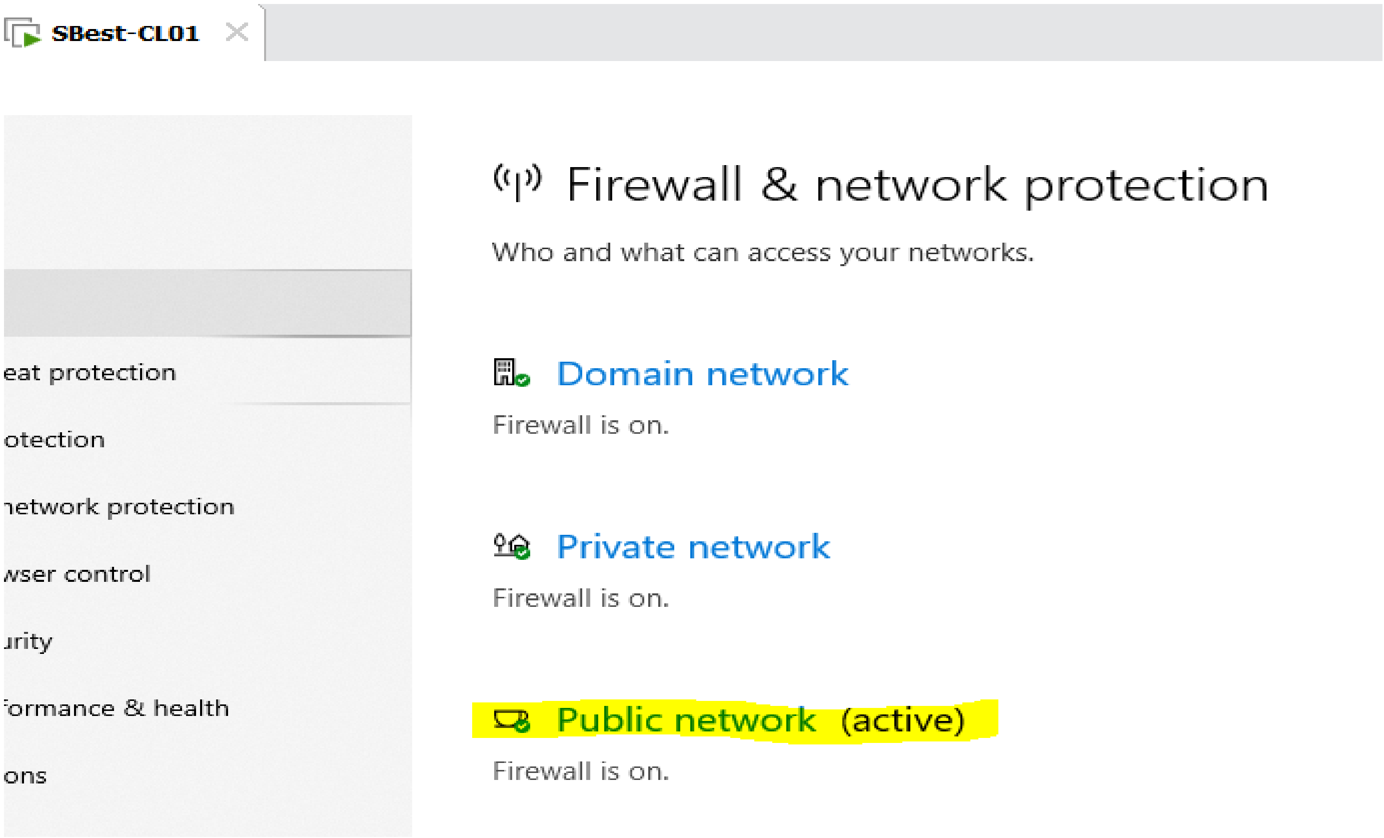
Question 1: Network Firewall and Virus Protection

Under “Firewall” you see 3 networks your firewall may be applied to, please identify them, and give brief descriptions of each. Which one is active? Why are the others **not** active?

1. **Domain Network:** Allows the receival of packets from domain-based network communication. External packets not recognized in the domain network are denied and do not access the PC. This is **not** active because the VM is not on a domain network.
2. **Private Network:** Allows the receival of packets from a trusted private network. This is **not** active because the VM is does not recognize the Host PC network as a private network.
3. **Public Network:** The public network is active. This is set as active because the VM is connected to the internet via the Host PC and has assigned the connection as “public”.

(Microsoft 365 Modern Desktop Administrator Guide to Exam MD-100: Windows 10).

Firewall and Network Protection- Domain, Private & Public



Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

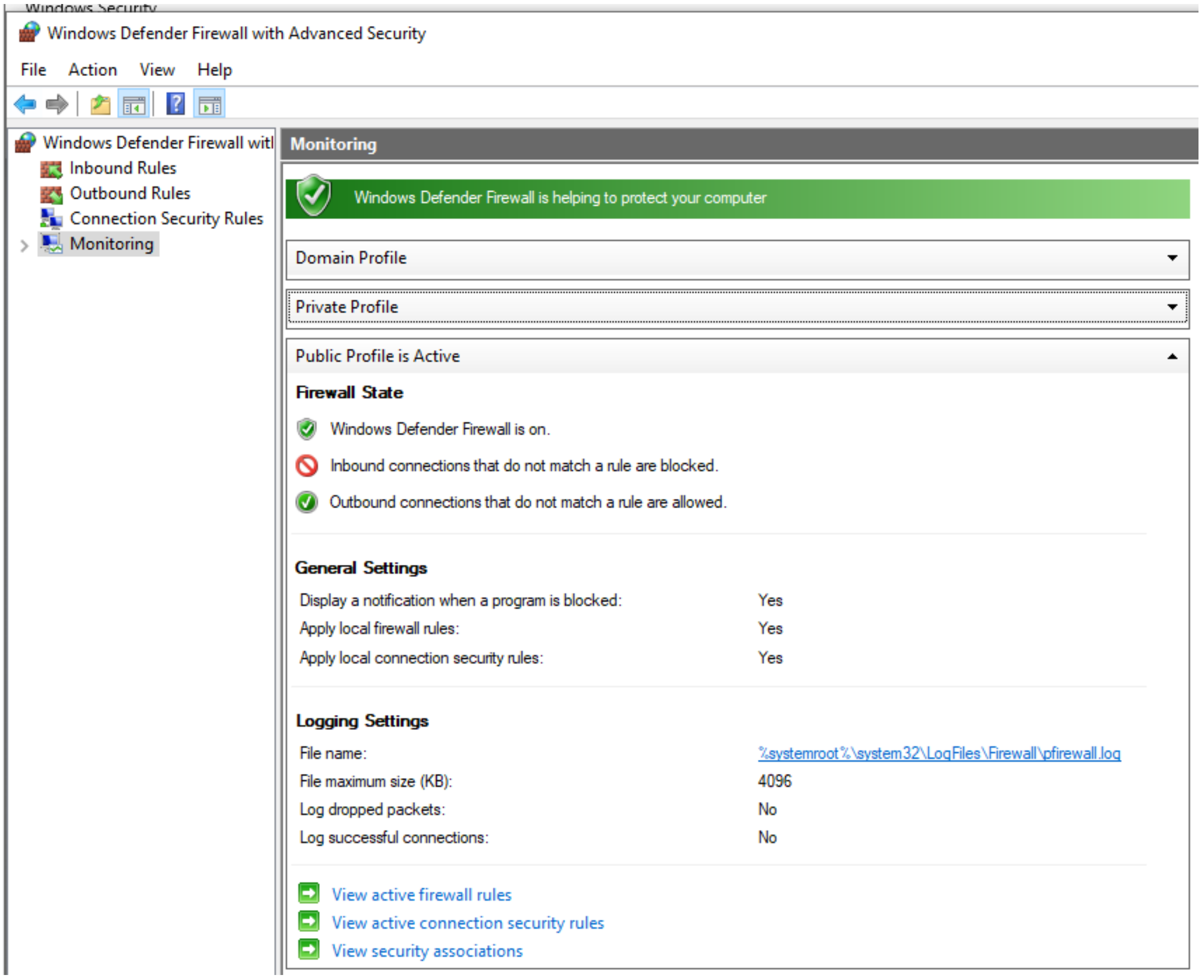
Private network

Firewall is on.

Public network (active)

Firewall is on.

Screenshot above is showing the **“Public network”** is set to **“Active”.**


Windows Security
Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Monitoring

Windows Defender Firewall is helping to protect your computer

Domain Profile

Private Profile

Public Profile is Active

Firewall State

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

General Settings

Display a notification when a program is blocked:	Yes
Apply local firewall rules:	Yes
Apply local connection security rules:	Yes

Logging Settings

File name:	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
File maximum size (KB):	4096
Log dropped packets:	No
Log successful connections:	No

View active firewall rules

View active connection security rules

View security associations

Screenshot above shows more specifics about the Public Profiles Firewall Settings.

Question 2: User Account Controls

What are the 4 UAC change settings available?

Always notify me when:

- Apps try to install software or make changes to my computer.
- I make changes to Windows settings.

Notify me only when apps try to make changes to my computer (default):

- Don’t notify me when I make changes to windows settings.

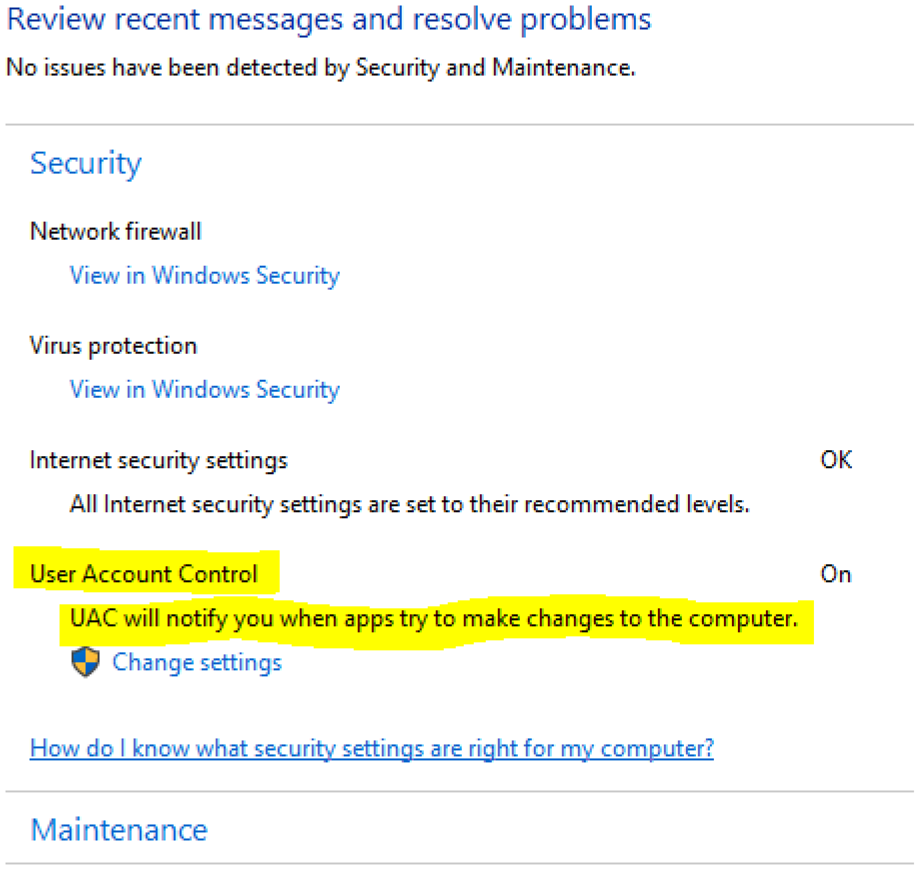
Notify me only when apps try to make changes to my computer (do not dim my desktop)

- Don’t notify me when I make changes to windows settings.

Never notify me when:

- Apps try to install software or make changes to my computer.
- I make changes to Windows settings.

User Account Controls- Modified



Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

Security

Network firewall

View in Windows Security

Virus protection

View in Windows Security

Internet security settings OK

All Internet security settings are set to their recommended levels.

User Account Control On

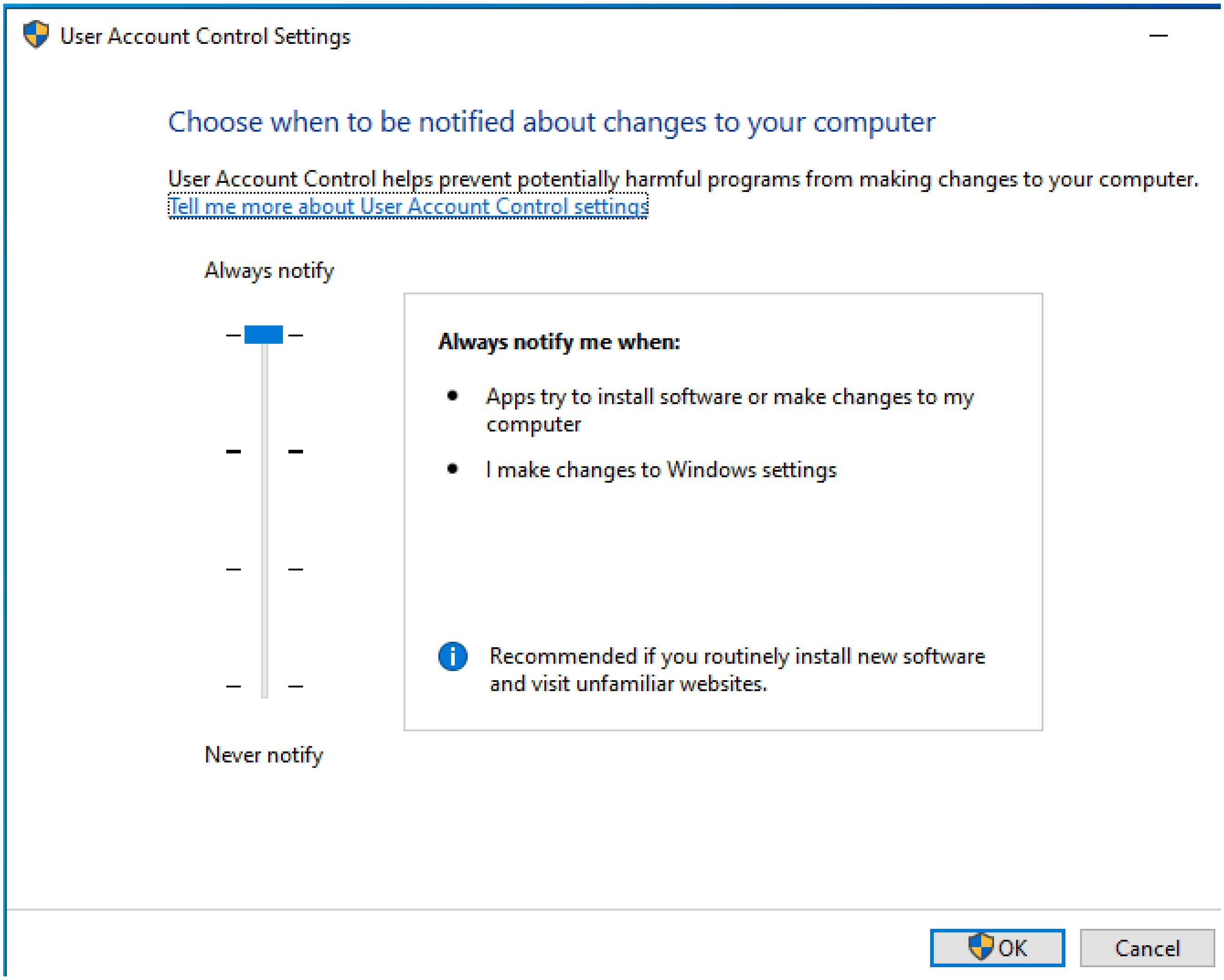
UAC will notify you when apps try to make changes to the computer.

Change settings

How do I know what security settings are right for my computer?

Maintenance

The **UAC's** have been modified to **Always Prompt** when making changes to the Windows Settings.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Always notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

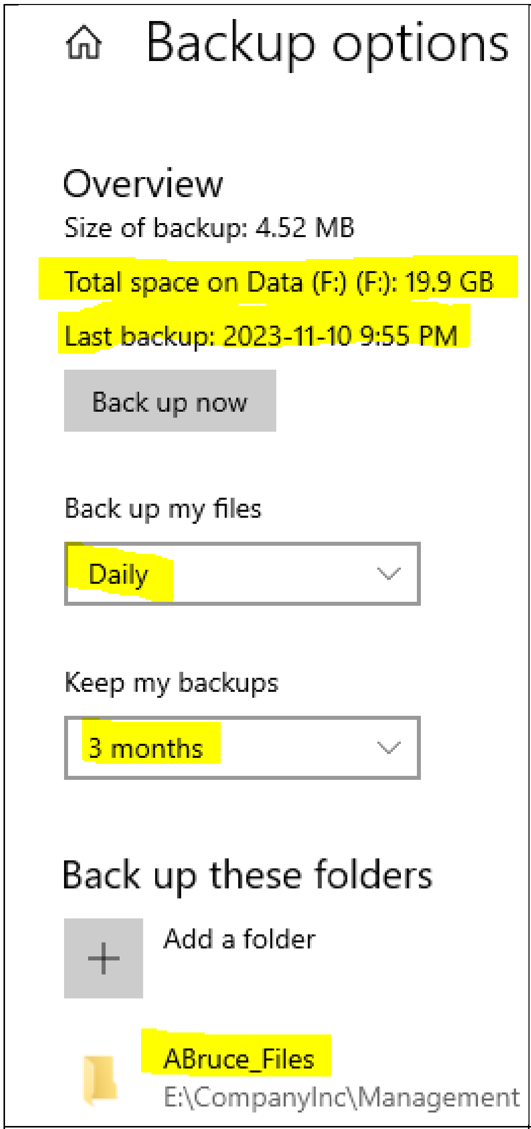
Never notify

Screenshot above showing the User Account Control Settings. Selected currently is to “**Always notify me**” when changes are made to the computer.

Task 3 – File backup and Recovery

Backup ABruce_Files to Data (F:)

In the “Backup” tab in “Update & Security page, the “**Data (F:)** drive was added, and ‘Backup using File History’ was selected. Backups were set to “**Daily**” and saved versions are kept for “**3 months**”. File History was backed up after “ABruce_Files” was added.



Backup options

Overview

Size of backup: 4.52 MB

Total space on Data (F:) (F:): 19.9 GB

Last backup: 2023-11-10 9:55 PM

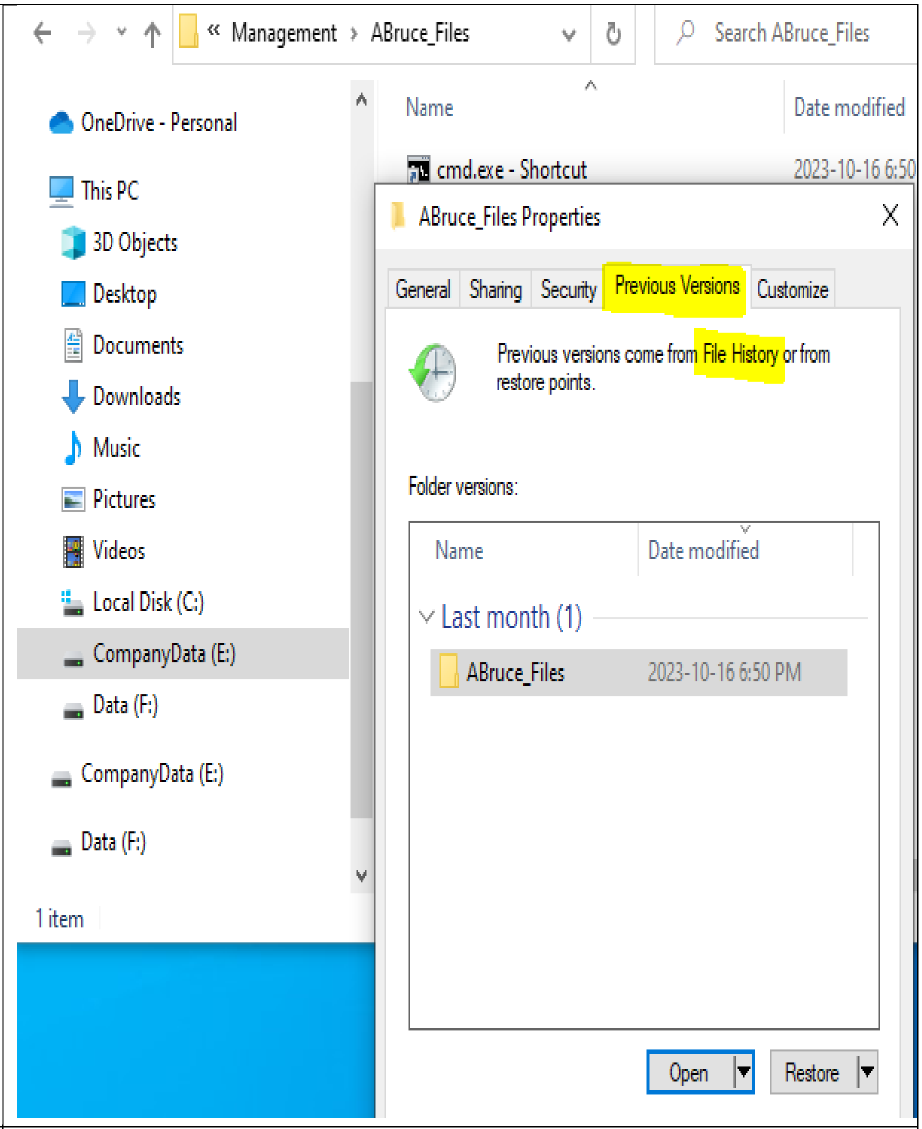
Back up my files: Daily

Keep my backups: 3 months

Back up these folders

ABruce_Files
E:\CompanyInc\Management

Backup settings changed. Backup “ABruce_Files” to **“Data (F:) Daily, keep backups for “3 Months”.**



cmd.exe - Shortcut 2023-10-16 6:50

ABruce_Files Properties

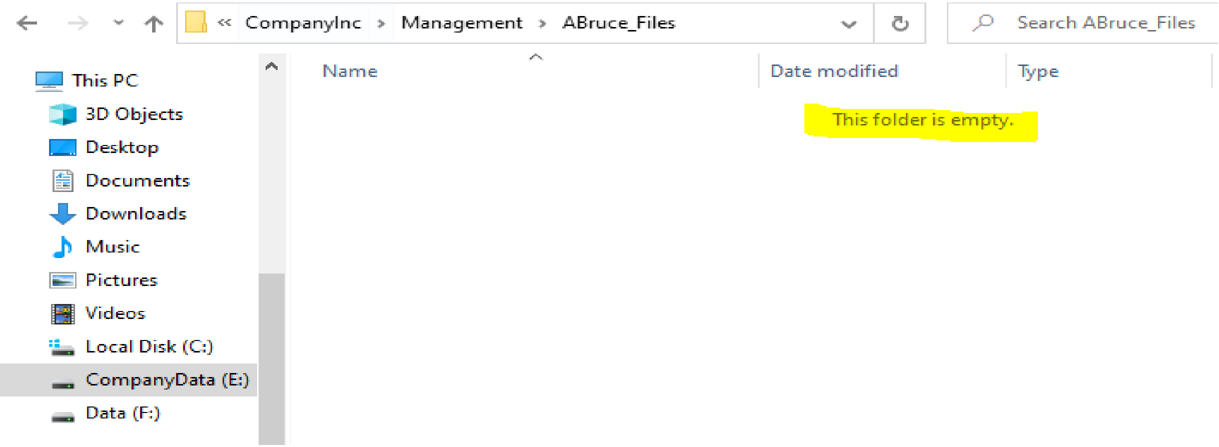
Previous versions come from File History or from restore points.

Folder versions:

Name	Date modified
Last month (1)	
ABruce_Files	2023-10-16 6:50 PM

Previous Version of the “ABruce_Files” folder after backing up to “Data (F:)”

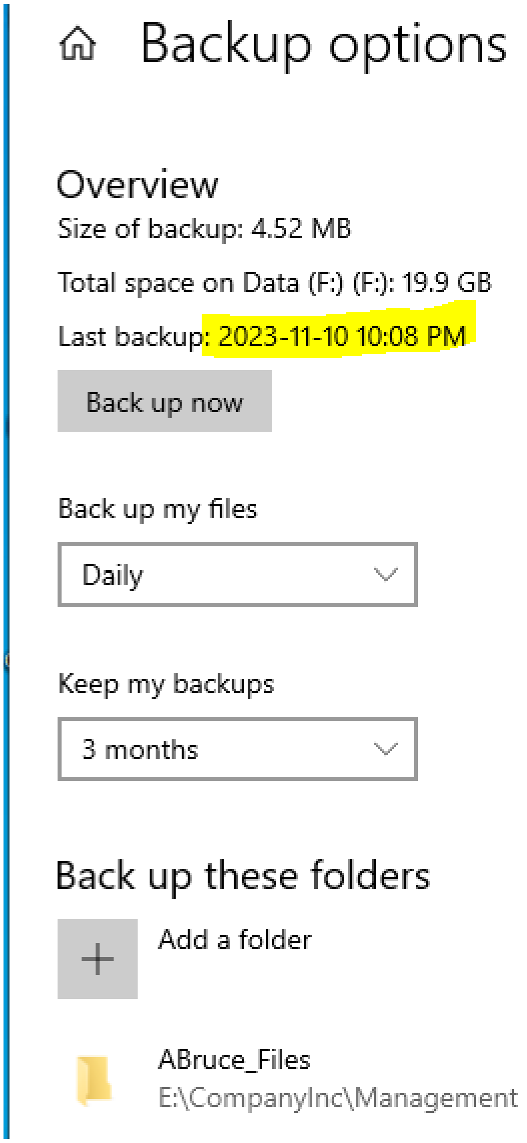
Delete ABruce_Files from “E:\CompanyInc\Management\”.



This folder is empty.

ABruce_Files after “cmd.exe” was deleted shown above.

New Backup



Backup options

Overview

Size of backup: 4.52 MB

Total space on Data (F:) (F:): 19.9 GB

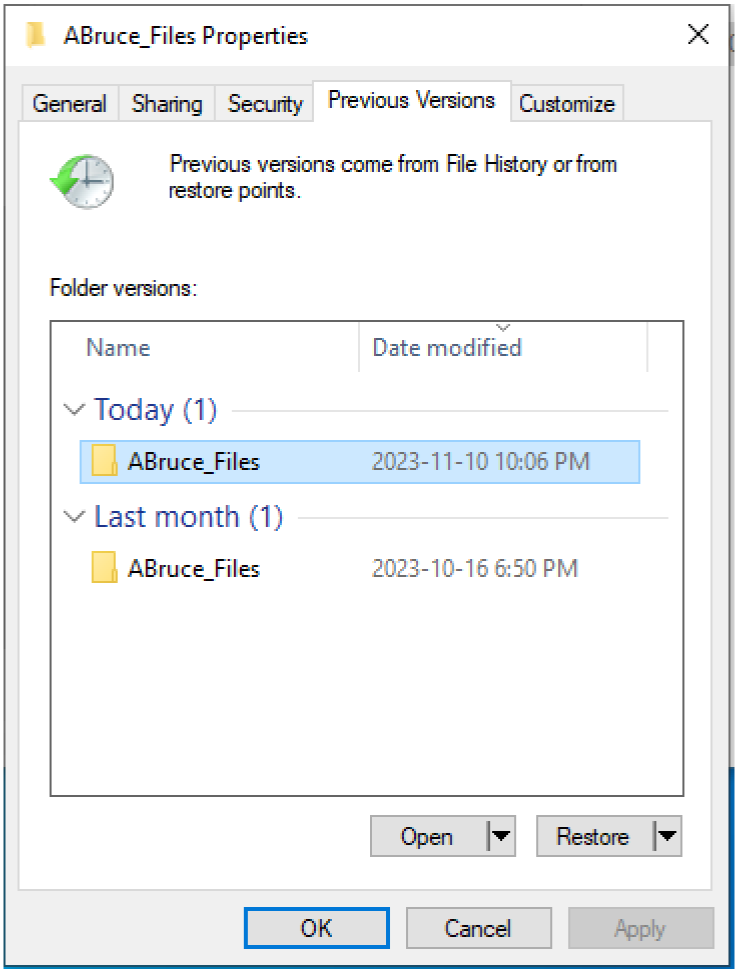
Last backup: 2023-11-10 10:08 PM

Back up my files: Daily

Keep my backups: 3 months

Back up these folders

ABruce_Files
E:\CompanyInc\Management



ABruce_Files Properties

Previous versions come from File History or from restore points.

Folder versions:

Name	Date modified
Today (1)	
ABruce_Files	2023-11-10 10:06 PM
Last month (1)	
ABruce_Files	2023-10-16 6:50 PM

Two screenshots above show the newest backup of “ABruce_Files” after “cmd.exe” was deleted, and on the right is the ABruce_Files “Previous Versions”.

Restore Previous Version using File History

Question 3: Restoring deleted file and NOT entire folder:

What are the steps required to recover just the cmd.exe file you deleted in a previous step but **do NOT recover the entire folder, just the deleted file.**

The steps required to restore a previously deleted file but not recover the entire folder can be done multiple ways, the first explanation is how this file was restored for this assignment:

One way is to access the folder that contained the deleted file, right click on the folder that contained the deleted file and select “**Restore Previous Version**”. This will open the **properties** and you can view the **Previous Versions**. Upon finding the Previous Version you wish to restore, select the **“Open” arrow**, and view in **“File History”.** Select the items you wish to restore and click the **green counterclockwise arrow**. This restores only the selected items to the folder, and **not** the entire folder. *(Wright, B. Pelarski, L. 2021)*

Another option to restore the file outside of "File History" is to refer to "OneDrive" **IF** the folder was previously synced to OneDrive.

For a recently deleted item, if available, you may be able to open "Recycle Bin", right-click on the deleted item, and click "Restore".

Windows "Backup and Restore" is also available to use if the deleted folder or file was **previously** backed up. This is for use for Windows 7 and up.

All three of these options also may not work, depending on how the file was deleted and if the versions of these files were backed up.

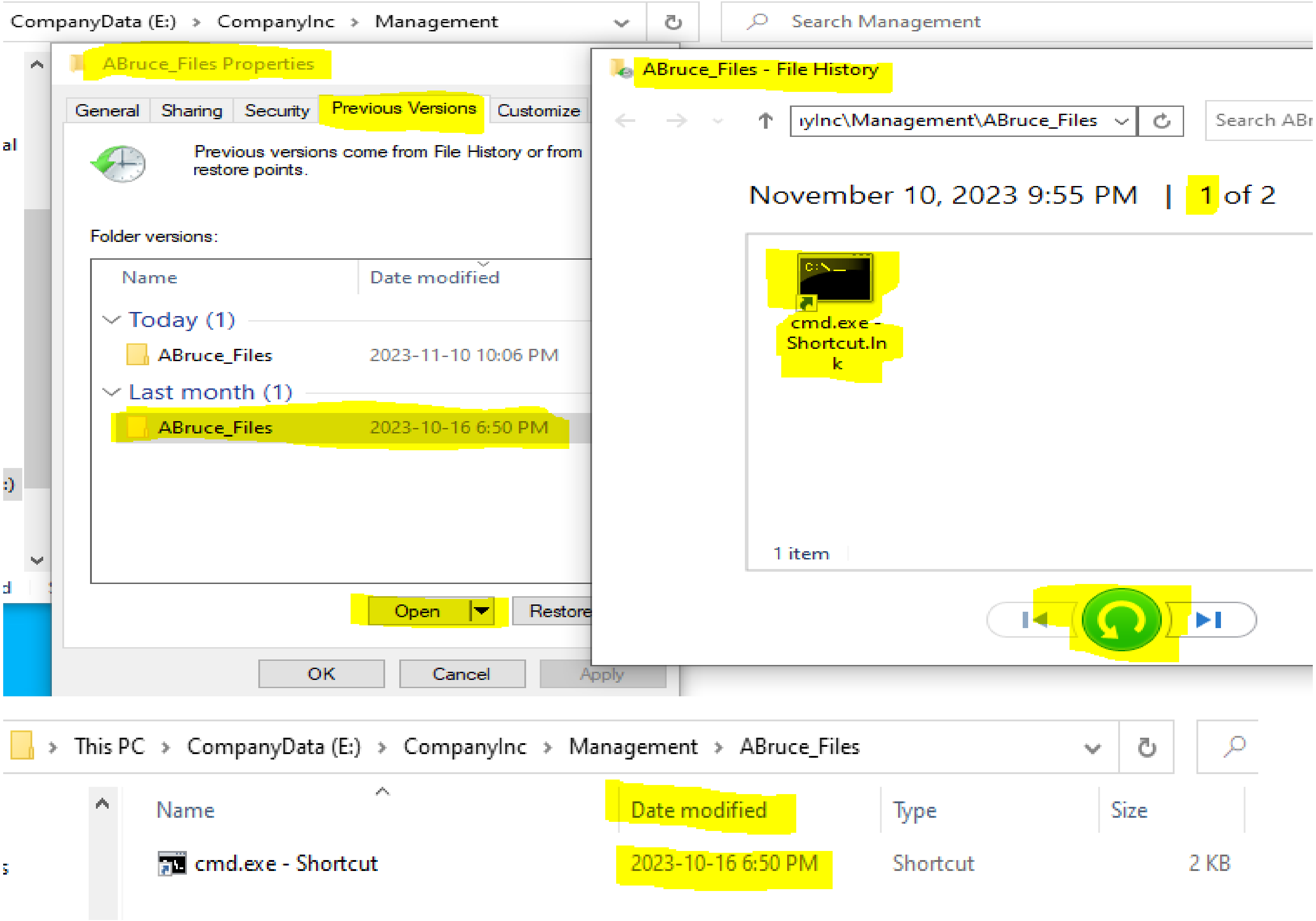
This made me look further into how to recover files if they were **not** previously backed up. I learned that "**Windows File Recovery"** is available to use in Command Prompt.

`winfr source-drive: destination-drive: [/mode] [/switches]` *(Recover Lost Files on Windows 10, Microsoft Support 2020)*

The "winfr" stands for the "Windows File Recovery" application. Source-Drive is replaced with the drive that is being searched (example: **C:\**), and destination drive is replaced with the drive the recovered files will be recovered to (example: **D:\**). These need to be two separate drives when recovering a file or folder. [/mode] for the winfr command is either /regular or /extensive (in this application). [/switches] allow you to add parameters after the "/", which are instructions for the program. *(I did too much reading on this the past couple of days, so to sum up what I've read it would probably come out inaccurate since there is SO much to learn. I'm excited to get more into this since I spent my weekend wondering why things do what they do and how this exactly works)*

Previous Version Restored

See highlighted text above for steps taken to restore the previous version.



CompanyData (E:) › CompanyInc › Management
Search Management
ABruce_Files Properties
General
Sharing
Security
Previous Versions
Customize

Previous versions come from File History or from restore points.

Folder versions:

Name	Date modified
Today (1)	
ABruce_Files	2023-11-10 10:06 PM
Last month (1)	
ABruce_Files	2023-10-16 6:50 PM

Open
Restore
OK
Cancel
Apply
ABruce_Files - File History
ıyInc\Management\ABruce_Files
Search ABr

November 10, 2023 9:55 PM | 1 of 2

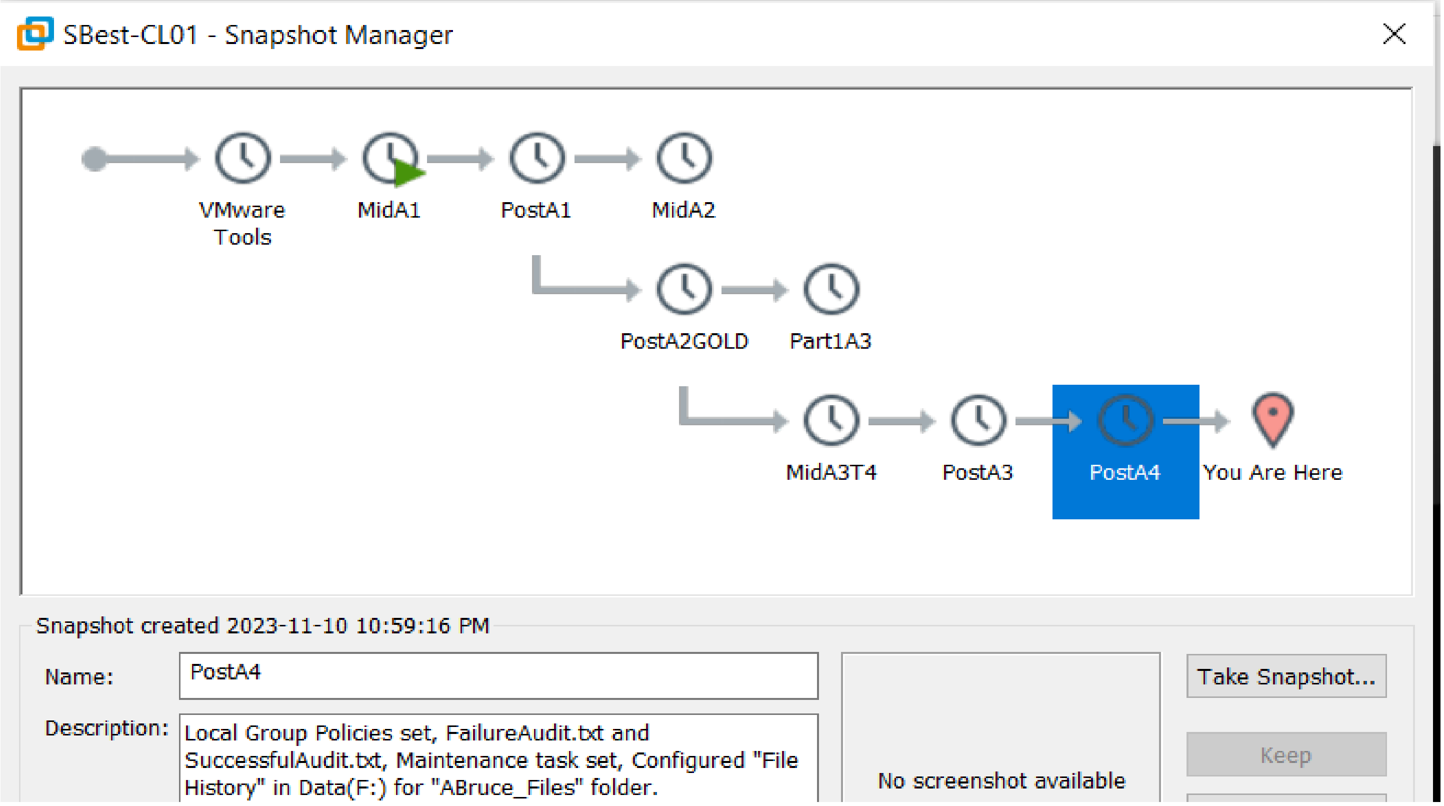
cmd.exe - Shortcut.lnk
1 item
This PC › CompanyData (E:) › CompanyInc › Management › ABruce_Files

Name	Date modified	Type	Size
cmd.exe - Shortcut	2023-10-16 6:50 PM	Shortcut	2 KB

These photos show the process of restoring the previous version of ABruce_Files using File History.

Snapshot PostA4

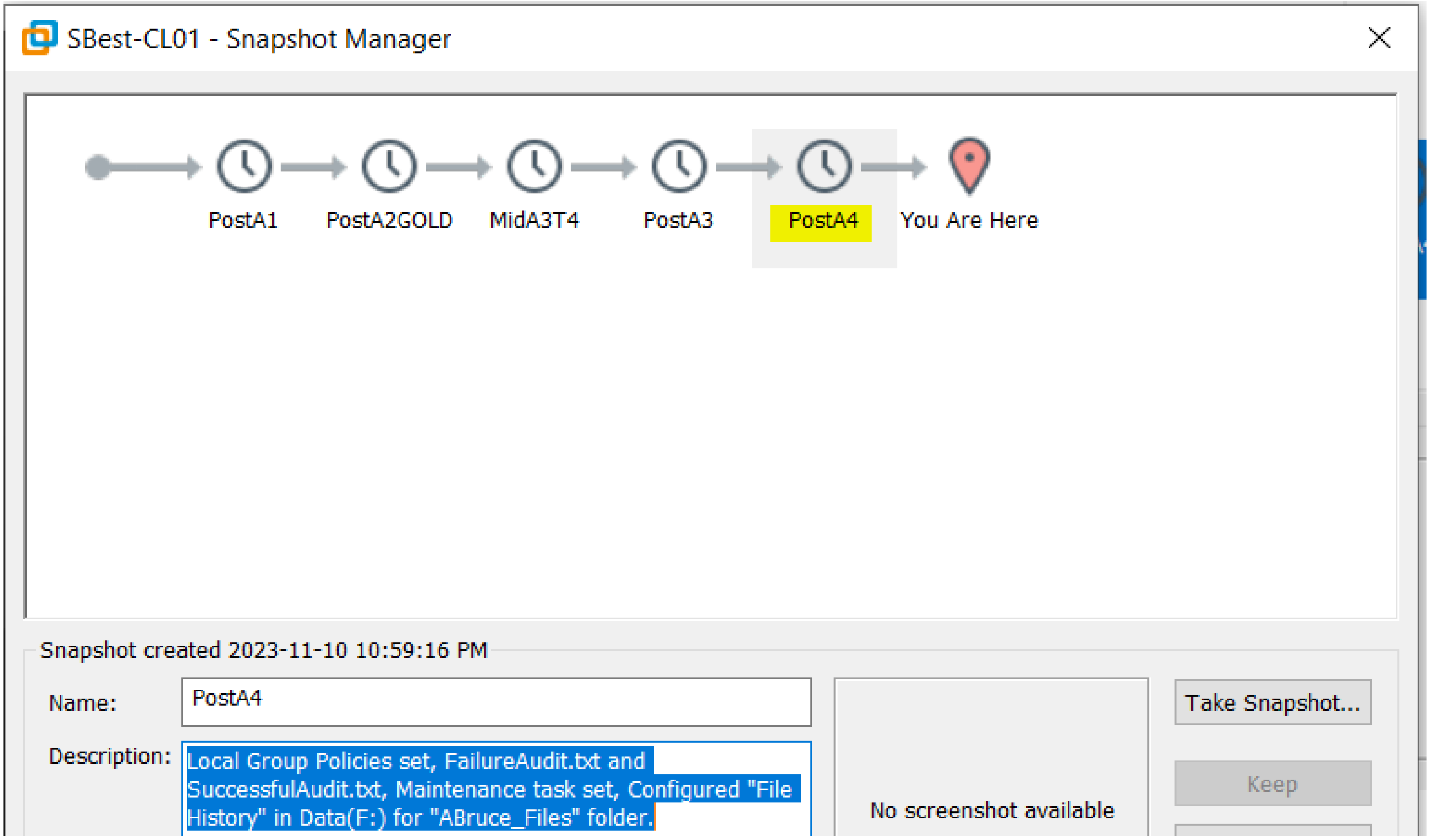
Snapshot of PostA4 taken after completion of all Assignment 4 steps.



Snapshot created 2023-11-10 10:59:16 PM

Name: PostA4

Description: Local Group Policies set, FailureAudit.txt and SuccessfulAudit.txt, Maintenance task set, Configured "File History" in Data(F:) for "ABruce_Files" folder.

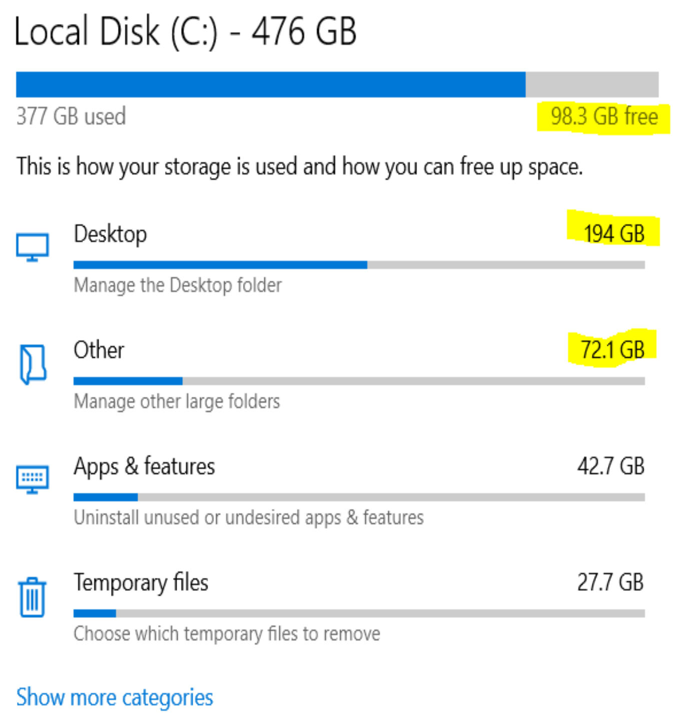


Snapshot created 2023-11-10 10:59:16 PM

Name: PostA4

Description: Local Group Policies set, FailureAudit.txt and SuccessfulAudit.txt, Maintenance task set, Configured "File History" in Data(F:) for "ABruce_Files" folder.

Snapshot Manager view of "PostA4" after removing unnecessary Snapshots from VM. My hard drive had 30GB storage space remaining before Gold Copy was created. Copied Gold Copies to OneDrive, keeping PostA4 Gold Copy on Local PC.



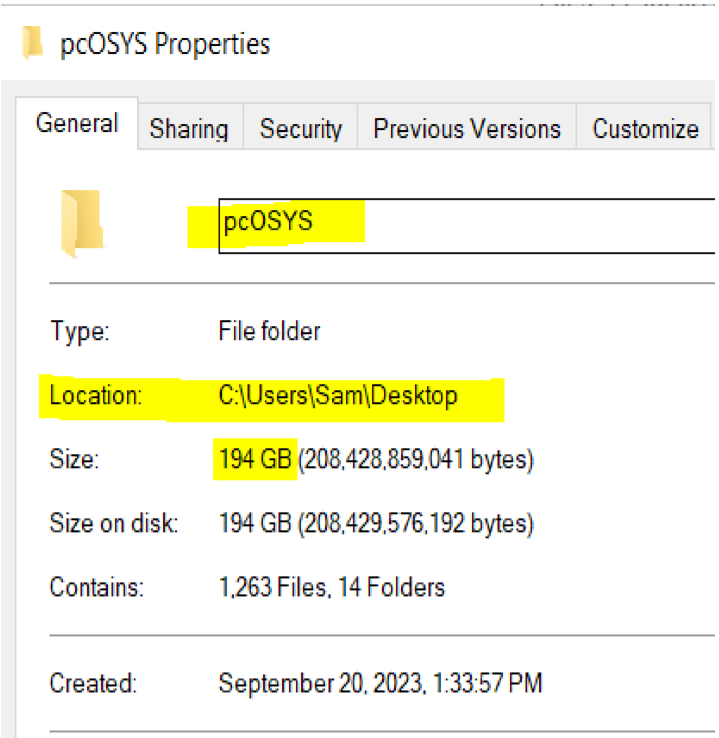
Local Disk (C:) - 476 GB

377 GB used — 98.3 GB free

This is how your storage is used and how you can free up space.

Desktop Manage the Desktop folder	194 GB
Other Manage other large folders	72.1 GB
Apps & features Uninstall unused or undesired apps & features	42.7 GB
Temporary files Choose which temporary files to remove	27.7 GB

Show more categories



pcOSYS Properties

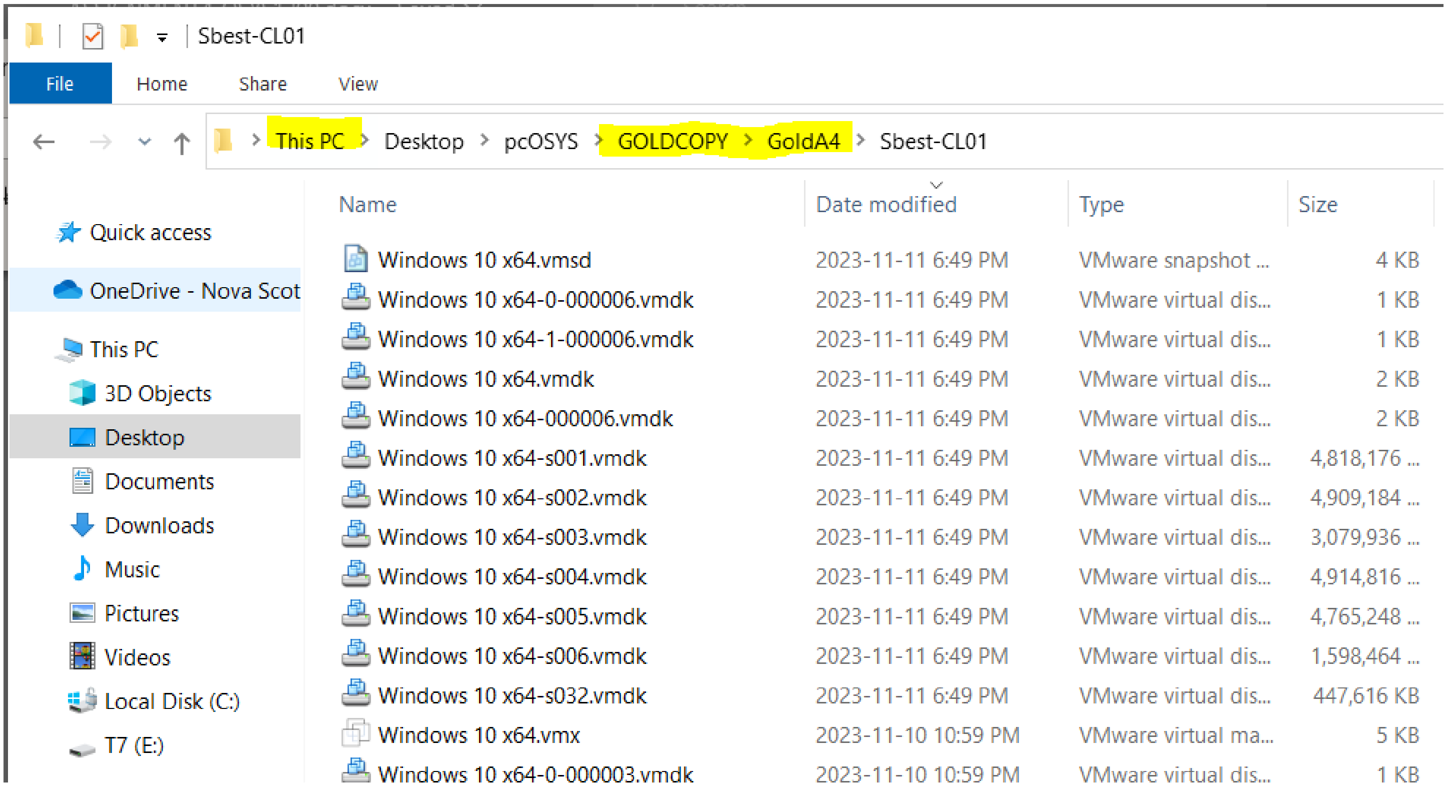
pcOSYS

Type:	File folder
Location:	C:\Users\Sam\Desktop
Size:	194 GB (208,428,859,041 bytes)
Size on disk:	194 GB (208,429,576,192 bytes)
Contains:	1,263 Files, 14 Folders
Created:	September 20, 2023, 1:33:57 PM

Included this because my laptop is *screaming* for storage. I had 30GB of space left on my hard drive, so I removed a bit for now, and I am going to remove all gold copies except the current one. (All other copies **have** been moved to OneDrive). I will invest in a larger SSD to use next semester.

Gold Copy (2 copies)

Two copies of VM created. One copy was moved to my PC, a second copy was backed up to OneDrive.

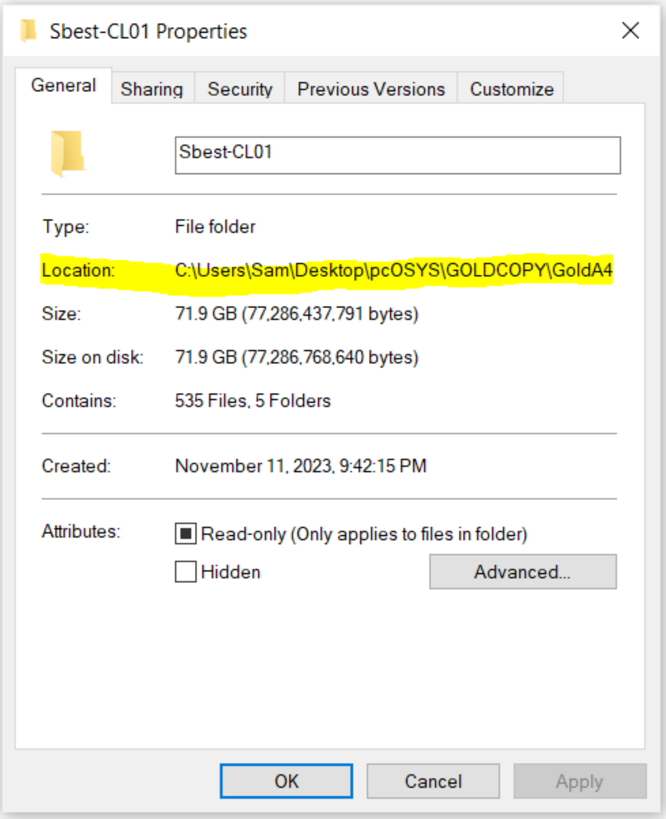


Sbest-CL01

This PC > Desktop > pcOSYS > GOLDCOPY > GoldA4 > Sbest-CL01

Name	Date modified	Type	Size
Windows 10 x64.vmsd	2023-11-11 6:49 PM	VMware snapshot ...	4 KB
Windows 10 x64-0-000006.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	1 KB
Windows 10 x64-1-000006.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	1 KB
Windows 10 x64.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	2 KB
Windows 10 x64-000006.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	2 KB
Windows 10 x64-s001.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	4,818,176 ...
Windows 10 x64-s002.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	4,909,184 ...
Windows 10 x64-s003.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	3,079,936 ...
Windows 10 x64-s004.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	4,914,816 ...
Windows 10 x64-s005.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	4,765,248 ...
Windows 10 x64-s006.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	1,598,464 ...
Windows 10 x64-s032.vmdk	2023-11-11 6:49 PM	VMware virtual dis...	447,616 KB
Windows 10 x64.vmx	2023-11-10 10:59 PM	VMware virtual ma...	5 KB
Windows 10 x64-0-000003.vmdk	2023-11-10 10:59 PM	VMware virtual dis...	1 KB

Gold Copy copied from SSD to host PC.



Sbest-CL01

Type: File folder

Location: C:\Users\Sam\Desktop\pcOSYS\GOLDCOPY\GoldA4

Size: 71.9 GB (77,286,437,791 bytes)

Size on disk: 71.9 GB (77,286,768,640 bytes)

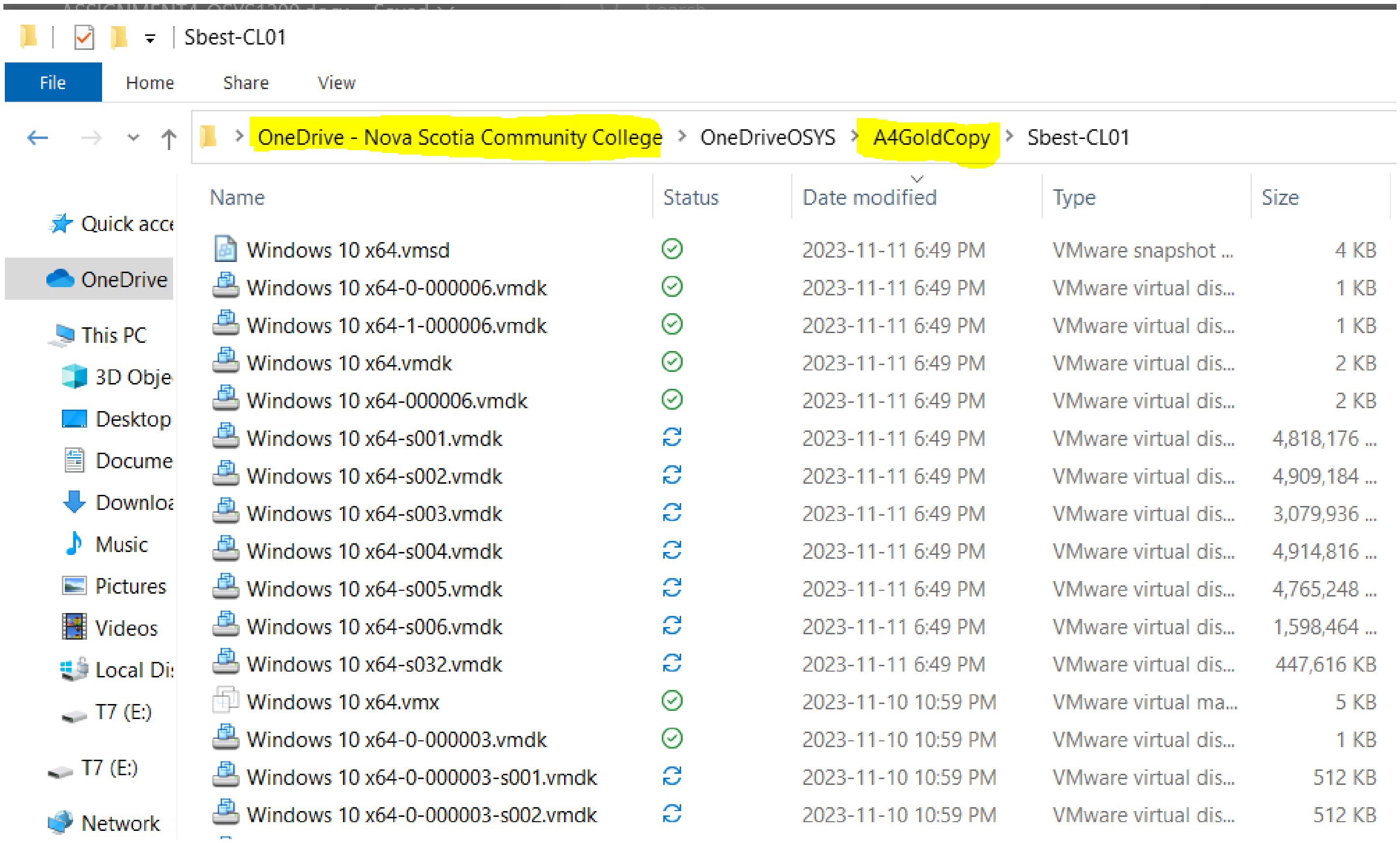
Contains: 535 Files, 5 Folders

Created: November 11, 2023, 9:42:15 PM

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

Properties of **PostA4 gold copy** shown above in my PC.



OneDrive - Nova Scotia Community College > OneDriveOSYS > A4GoldCopy > Sbest-CL01

Name	Status	Date modified	Type	Size
Windows 10 x64.vmsd	✓	2023-11-11 6:49 PM	VMware snapshot ...	4 KB
Windows 10 x64-0-000006.vmdk	✓	2023-11-11 6:49 PM	VMware virtual dis...	1 KB
Windows 10 x64-1-000006.vmdk	✓	2023-11-11 6:49 PM	VMware virtual dis...	1 KB
Windows 10 x64.vmdk	✓	2023-11-11 6:49 PM	VMware virtual dis...	2 KB
Windows 10 x64-000006.vmdk	✓	2023-11-11 6:49 PM	VMware virtual dis...	2 KB
Windows 10 x64-s001.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	4,818,176 ...
Windows 10 x64-s002.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	4,909,184 ...
Windows 10 x64-s003.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	3,079,936 ...
Windows 10 x64-s004.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	4,914,816 ...
Windows 10 x64-s005.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	4,765,248 ...
Windows 10 x64-s006.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	1,598,464 ...
Windows 10 x64-s032.vmdk	⟳	2023-11-11 6:49 PM	VMware virtual dis...	447,616 KB
Windows 10 x64.vmx	✓	2023-11-10 10:59 PM	VMware virtual ma...	5 KB
Windows 10 x64-0-000003.vmdk	✓	2023-11-10 10:59 PM	VMware virtual dis...	1 KB
Windows 10 x64-0-000003-s001.vmdk	⟳	2023-11-10 10:59 PM	VMware virtual dis...	512 KB
Windows 10 x64-0-000003-s002.vmdk	⟳	2023-11-10 10:59 PM	VMware virtual dis...	512 KB

Second copy of Gold Copy copied from SSD to "OneDrive". Sync in progress during screenshot. May take up to 30 minutes to complete.

Scripts

Creation of “FailedAudit.txt” in elevated Windows PowerShell:

```
Get-EventLog -LogName Security -Message “*Failure*” -Newest 10 | out-file C:\Reports\FailureAudit.txt
```

Resources

Bollson, William. (2023, Nov 9). *Top 3 Ways to Recover Deleted Files not in Recycle Bin.* Way 2: Recover Deleted Files Not in Recycle Bin from Previous Versions. Retrieved from: https://4ddig.tenorshare.com/windows-recovery-solutions/how-to-recover-deleted-files-not-in-recycle-bin.html#part4

Microsoft Support. (2020). *Recover Lost Files on Windows 10.* Retrieved from: https://support.microsoft.com/en-us/windows/recover-lost-files-on-windows-10-61f5b28a-f5b8-3cc2-0f8e-a63cb4e1d4c4

NSCC. (2023). *OSYS1200 Assignment 4 v10.27.23.* Retrieved from: https://nscconline.brightspace.com/d2l/le/content/278834/viewContent/4321092/View

Wright, B., Plesniarski, L. (2021). *Microsoft 365 Modern Desktop Administrator Guide to Exam MD-100: Windows 10.* Cengage Learning.