Scenario

As a security team member of Structureality Inc, I’m working to improve Wer organization's security stance. Often the best path to a secure IT infrastructure starts with thorough planning and analysis. I will perform a gap analysis of the current configuration of a system against a security template.

In this lab, I will use security templates to manage a Windows Server configuration, which will entail using the Microsoft Policy Analyzer to perform a security baseline template review and gap analysis.

I will be working from a virtual machine named PC10, hosting Windows Server 2019 and functioning as a client.

Objectives

This activity is designed to test Wer understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

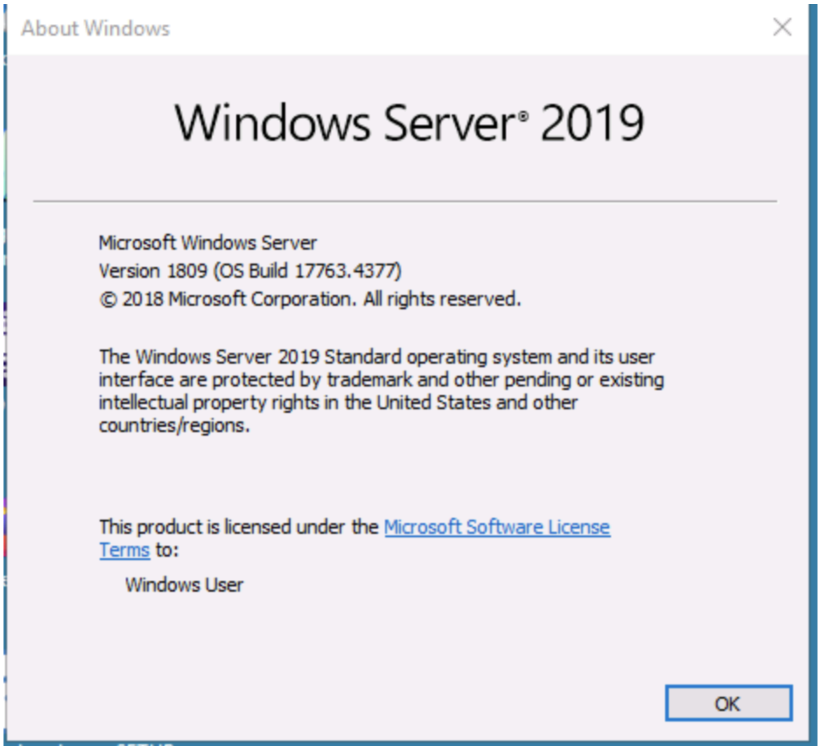
- 1.2 Summarize fundamental security concepts.
- 3.2 Given a scenario, apply security principles to secure enterprise infrastructure
- 4.1 Given a scenario, apply common security techniques to computing resources.
- 4.4 Explain security alerting and monitoring concepts and tools.
- 5.1 Summarize elements of effective security governance.

Perform gap analysis

Gap analysis is the act of comparing the current configuration of a system with a template, configuration file, baseline, security framework, or settings documentation. This is an essential operation to discover the differences between the intended or expected configuration of a system and its actual operating configuration. In this exercise, We will perform a gap analysis.

---

1. Log in as admin with password
2. Determine the build number for the Windows Server 2019 running in the PC virtual machine using **winver**. [On the search window]



About Windows

Windows Server® 2019

Microsoft Windows Server
Version 1809 (OS Build 17763.4377)
© 2018 Microsoft Corporation. All rights reserved.

The Windows Server 2019 Standard operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

Windows User

Here, the Version is 1809 and OS Build is 17763.4377

3. Open powerShell as Administrator and type copy D:\* c:\LABFILES

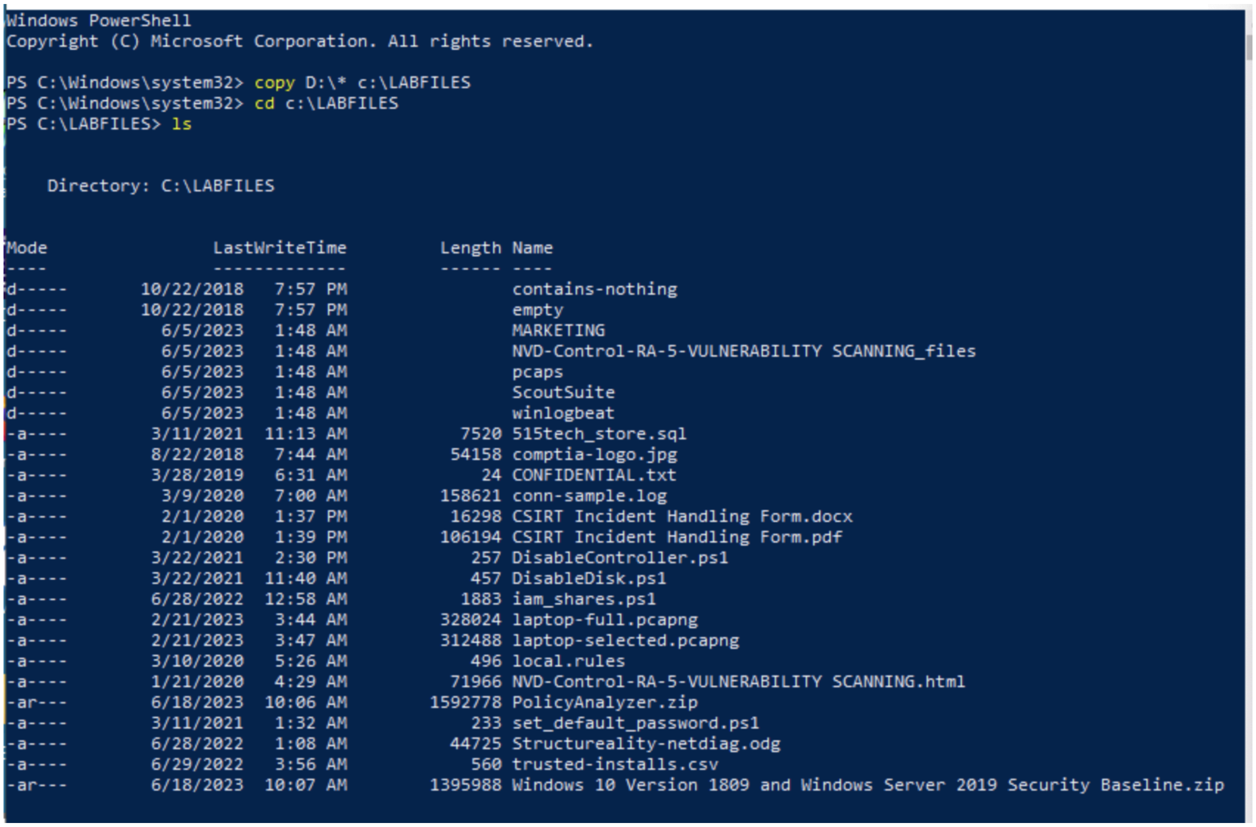
This command copies *PolicyAnalyzer.zip* and *Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip* from the read-only removable media virtual optical disc (i.e., D:) to C:\LABFILES.

These two files are from the Microsoft Security Compliance Toolkit. The baseline file was selected based on the OS version and build number.

The Microsoft Security Compliance Toolkit includes the Policy Analyzer tool as well as numerous security configuration template files. Searching for "Microsoft Security Compliance Toolkit" will help We locate the download area on the Microsoft website where these items are hosted. They have been provided for We the Student-Resources-L01.ISO media.

4. Enter cd c:\LABFILES to change into the directory.
5. Enter ls to view the contents of the directory.

[ls" is a Linux command (one of many) that are supported by Windows PowerShell. The "dir" will also display the directory contents.]



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

PS C:\Windows\system32> copy D:\* c:\LABFILES
PS C:\Windows\system32> cd c:\LABFILES
PS C:\LABFILES> ls


    Directory: C:\LABFILES


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/22/2018   7:57 PM                contains-nothing
d-----        10/22/2018   7:57 PM                empty
d-----          6/5/2023   1:48 AM                MARKETING
d-----          6/5/2023   1:48 AM                NVD-Control-RA-5-VULNERABILITY SCANNING_files
d-----          6/5/2023   1:48 AM                pcaps
d-----          6/5/2023   1:48 AM                ScoutSuite
d-----          6/5/2023   1:48 AM                winlogbeat
-a----         3/11/2021  11:13 AM           7520 515tech_store.sql
-a----         8/22/2018   7:44 AM          54158 comptia-logo.jpg
-a----         3/28/2019   6:31 AM             24 CONFIDENTIAL.txt
-a----          3/9/2020   7:00 AM         158621 conn-sample.log
-a----          2/1/2020   1:37 PM          16298 CSIRT Incident Handling Form.docx
-a----          2/1/2020   1:39 PM         106194 CSIRT Incident Handling Form.pdf
-a----         3/22/2021   2:30 PM            257 DisableController.ps1
-a----         3/22/2021  11:40 AM            457 DisableDisk.ps1
-a----         6/28/2022  12:58 AM           1883 iam_shares.ps1
-a----         2/21/2023   3:44 AM         328024 laptop-full.pcapng
-a----         2/21/2023   3:47 AM         312488 laptop-selected.pcapng
-a----         3/10/2020   5:26 AM            496 local.rules
-a----         1/21/2020   4:29 AM          71966 NVD-Control-RA-5-VULNERABILITY SCANNING.html
-ar---         6/18/2023  10:06 AM        1592778 PolicyAnalyzer.zip
-a----         3/11/2021   1:32 AM            233 set_default_password.ps1
-a----         6/28/2022   1:08 AM          44725 Structureality-netdiag.odg
-a----         6/29/2022   3:56 AM            560 trusted-installs.csv
-ar---         6/18/2023  10:07 AM        1395988 Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip
```

PolicyAnalyzer.zip and *Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip* in the list of files.

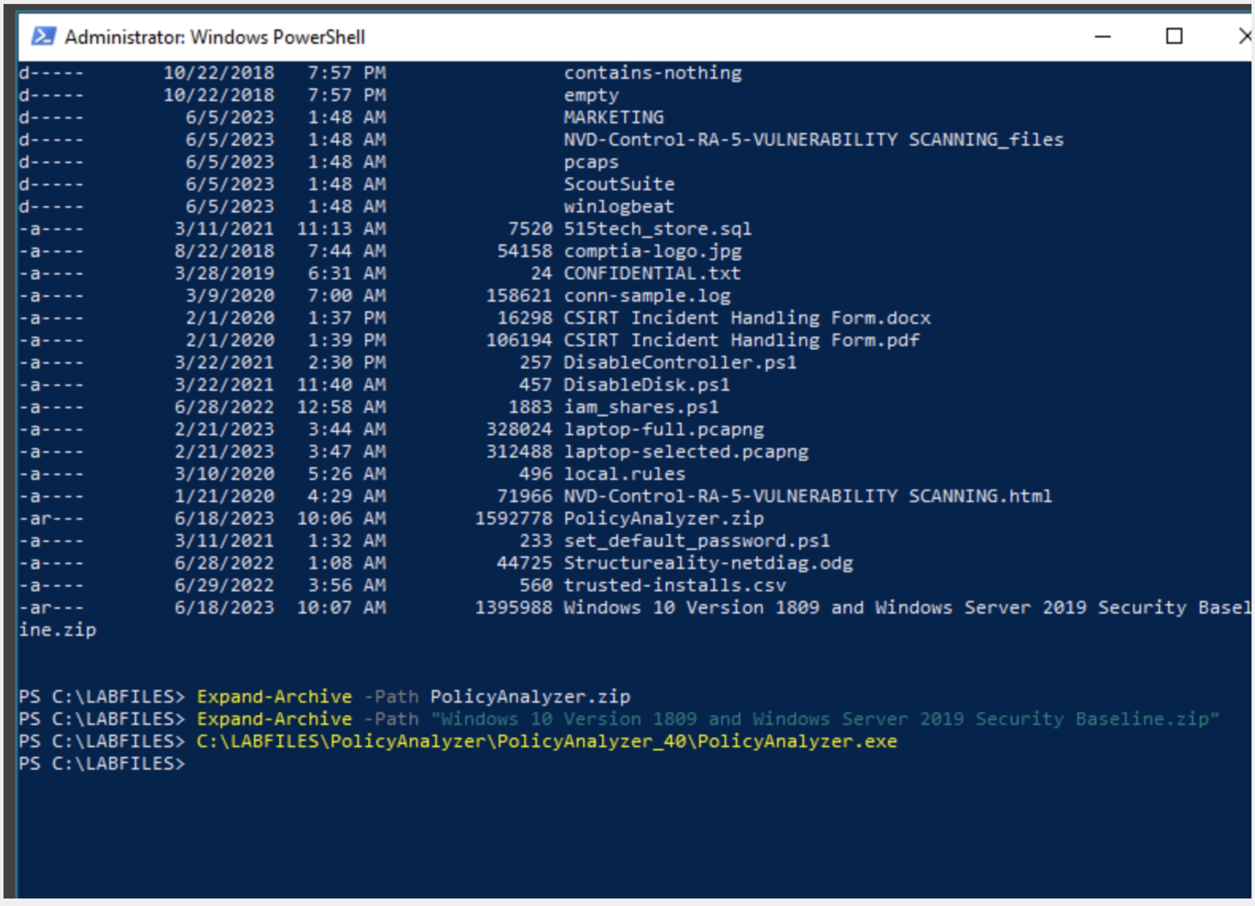
6. Enter the following commands to extract the contents of the zip files into their own sub-directories:

   ```
   Expand-Archive -Path PolicyAnalyzer.zip
   ```

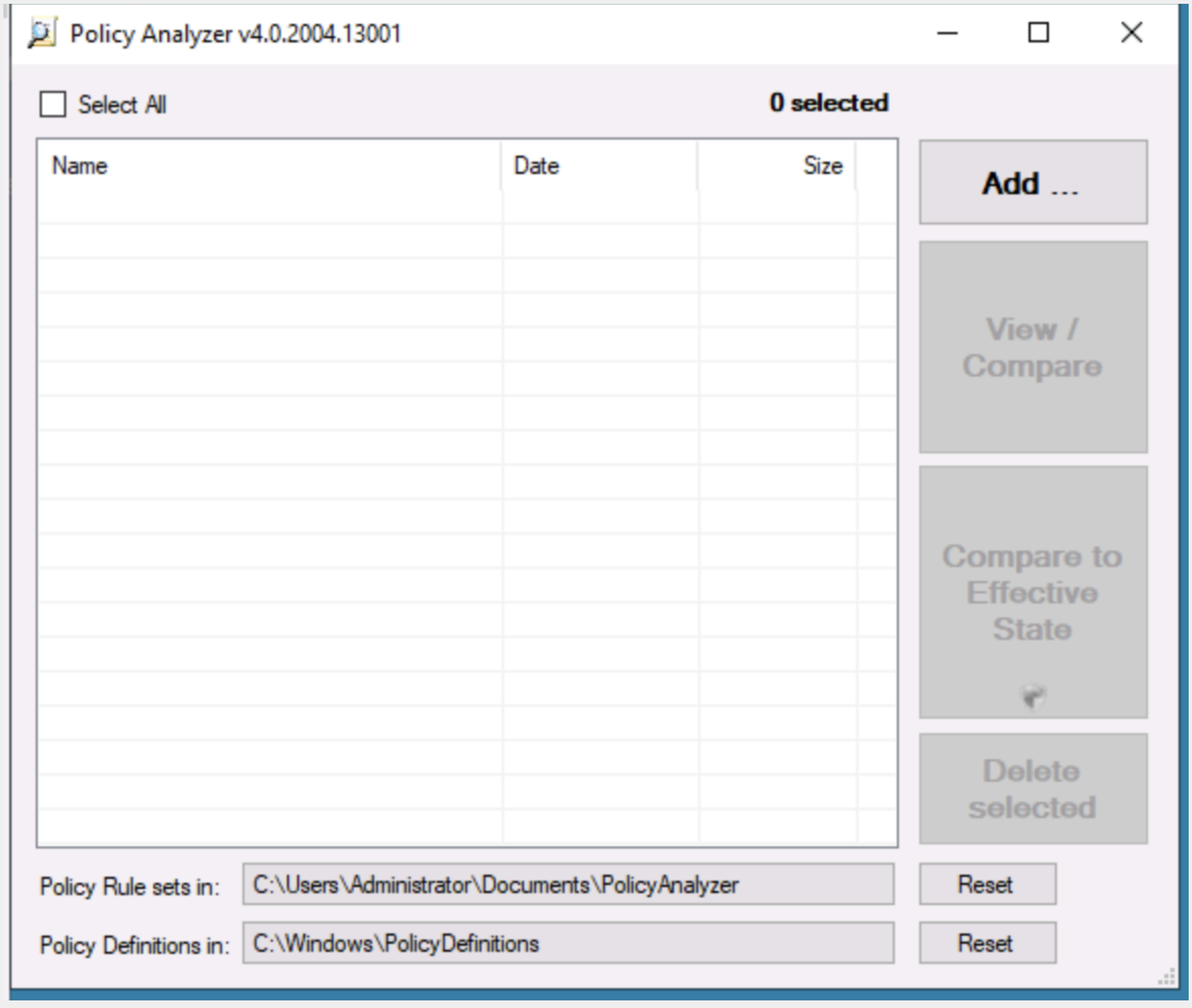
   ```
   Expand-Archive -Path "Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip"
   ```

7. Enter the following command to open the Policy Analyzer application:

   ```
   C:\LABFILES\PolicyAnalyzer\PolicyAnalyzer_40\PolicyAnalyzer.exe
   ```



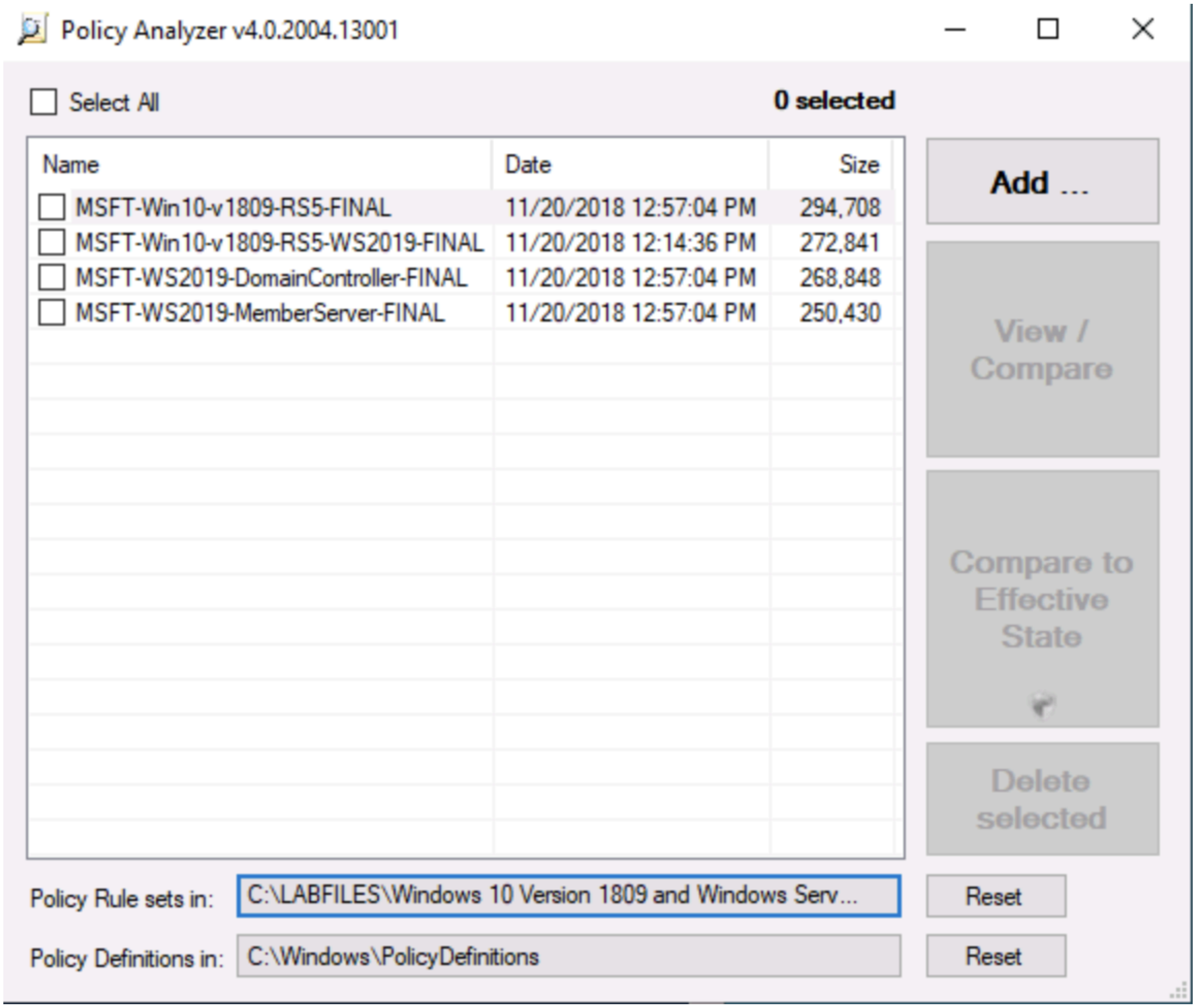
```
d-----       10/22/2018   7:57 PM                contains-nothing
d-----       10/22/2018   7:57 PM                empty
d-----         6/5/2023   1:48 AM                MARKETING
d-----         6/5/2023   1:48 AM                NVD-Control-RA-5-VULNERABILITY SCANNING_files
d-----         6/5/2023   1:48 AM                pcaps
d-----         6/5/2023   1:48 AM                ScoutSuite
d-----         6/5/2023   1:48 AM                winlogbeat
-a----        3/11/2021  11:13 AM           7520 515tech_store.sql
-a----        8/22/2018   7:44 AM          54158 comptia-logo.jpg
-a----        3/28/2019   6:31 AM             24 CONFIDENTIAL.txt
-a----         3/9/2020   7:00 AM         158621 conn-sample.log
-a----         2/1/2020   1:37 PM          16298 CSIRT Incident Handling Form.docx
-a----         2/1/2020   1:39 PM         106194 CSIRT Incident Handling Form.pdf
-a----        3/22/2021   2:30 PM            257 DisableController.ps1
-a----        3/22/2021  11:40 AM            457 DisableDisk.ps1
-a----        6/28/2022  12:58 AM           1883 iam_shares.ps1
-a----        2/21/2023   3:44 AM         328024 laptop-full.pcapng
-a----        2/21/2023   3:47 AM         312488 laptop-selected.pcapng
-a----        3/10/2020   5:26 AM            496 local.rules
-a----        1/21/2020   4:29 AM          71966 NVD-Control-RA-5-VULNERABILITY SCANNING.html
-ar---        6/18/2023  10:06 AM        1592778 PolicyAnalyzer.zip
-a----        3/11/2021   1:32 AM            233 set_default_password.ps1
-a----        6/28/2022   1:08 AM          44725 Structureality-netdiag.odg
-a----        6/29/2022   3:56 AM            560 trusted-installs.csv
-ar---        6/18/2023  10:07 AM        1395988 Windows 10 Version 1809 and Windows Server 2019 Security Basel
ine.zip


PS C:\LABFILES> Expand-Archive -Path PolicyAnalyzer.zip
PS C:\LABFILES> Expand-Archive -Path "Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip"
PS C:\LABFILES> C:\LABFILES\PolicyAnalyzer\PolicyAnalyzer_40\PolicyAnalyzer.exe
PS C:\LABFILES>
```



Policy Rule sets in: C:\Users\Administrator\Documents\PolicyAnalyzer

Policy Definitions in: C:\Windows\PolicyDefinitions

8. At the bottom of the Policy Analyzer window, select the **Policy Rule sets in** field.
9. On the *Pick the folder containing the Policy Analyzer Policy Rules files* window, in left pane select **Local Disk (C:)**, in the right pane double-click **LABFILES**, double-click **Windows 10 Version 1809 and Windows Server 2019 Security Baseline**, double-click **Documentation**, then select **Select Folder**.



□ Select All

0 selected

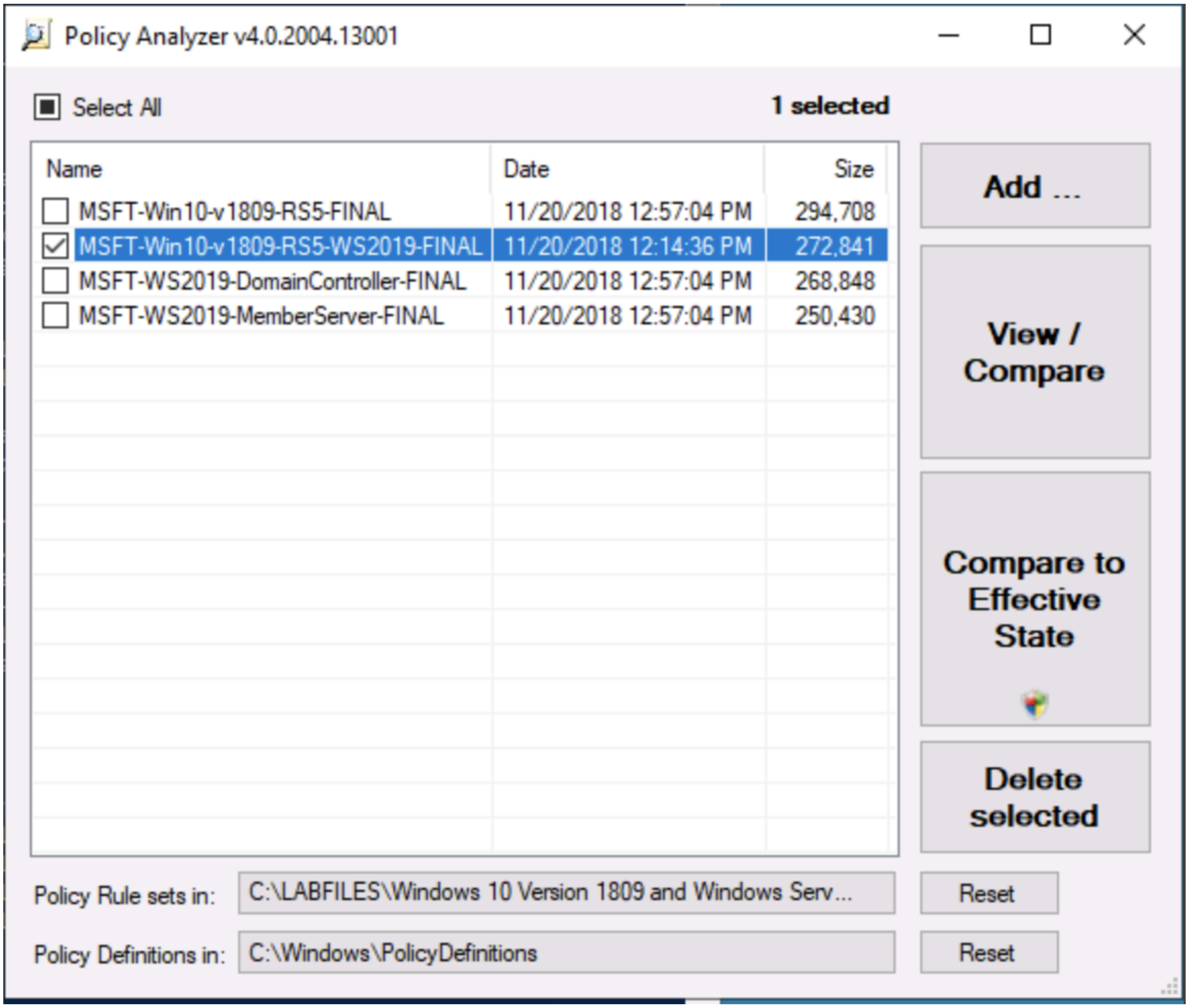
Name	Date	Size
□ MSFT-Win10-v1809-RS5-FINAL	11/20/2018 12:57:04 PM	294,708
□ MSFT-Win10-v1809-RS5-WS2019-FINAL	11/20/2018 12:14:36 PM	272,841
□ MSFT-WS2019-DomainController-FINAL	11/20/2018 12:57:04 PM	268,848
□ MSFT-WS2019-MemberServer-FINAL	11/20/2018 12:57:04 PM	250,430

Policy Rule sets in: C:\LABFILES\Windows 10 Version 1809 and Windows Serv...

Policy Definitions in: C:\Windows\PolicyDefinitions

The Policy Analyzer window should now show several policy rule sets.

10. Perform a View/Compare of MSFT-Win10-v1809-RS5-WS2019-FINAL using Policy Analyzer by marking the **MSFT-Win10-v1809-RS5-WS2019-FINAL** checkbox, then selecting **View / Compare**.



Policy Analyzer v4.0.2004.13001

▣ Select All

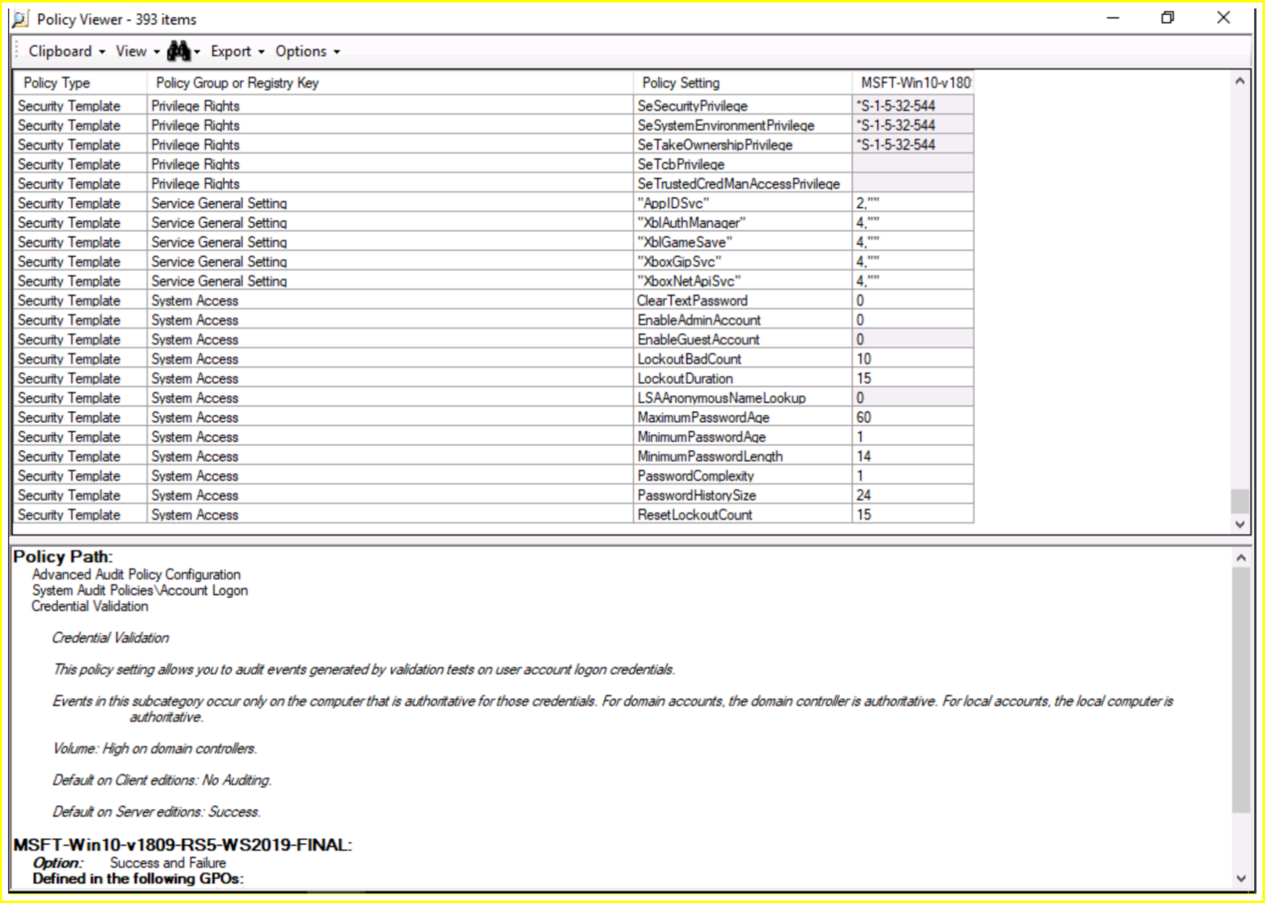
1 selected

	Name	Date	Size
☐	MSFT-Win10-v1809-RS5-FINAL	11/20/2018 12:57:04 PM	294,708
☑	MSFT-Win10-v1809-RS5-WS2019-FINAL	11/20/2018 12:14:36 PM	272,841
☐	MSFT-WS2019-DomainController-FINAL	11/20/2018 12:57:04 PM	268,848
☐	MSFT-WS2019-MemberServer-FINAL	11/20/2018 12:57:04 PM	250,430

Policy Rule sets in: C:\LABFILES\Windows 10 Version 1809 and Windows Serv...

Policy Definitions in: C:\Windows\PolicyDefinitions

The *Policy Viewer* window will be displayed, showing the various policy settings contained in the MSFT-Win10-v1809-RS5-WS2019-FINAL policy rule set.



Policy Type	Policy Group or Registry Key	Policy Setting	MSFT-Win10-v180
Security Template	Privilege Rights	SeSecurityPrivilege	*S-1-5-32-544
Security Template	Privilege Rights	SeSystemEnvironmentPrivilege	*S-1-5-32-544
Security Template	Privilege Rights	SeTakeOwnershipPrivilege	*S-1-5-32-544
Security Template	Privilege Rights	SeTcbPrivilege	
Security Template	Privilege Rights	SeTrustedCredManAccessPrivilege	
Security Template	Service General Setting	"AppIDSvc"	2,""
Security Template	Service General Setting	"XblAuthManager"	4,""
Security Template	Service General Setting	"XblGameSave"	4,""
Security Template	Service General Setting	"XboxGipSvc"	4,""
Security Template	Service General Setting	"XboxNetApiSvc"	4,""
Security Template	System Access	ClearTextPassword	0
Security Template	System Access	EnableAdminAccount	0
Security Template	System Access	EnableGuestAccount	0
Security Template	System Access	LockoutBadCount	10
Security Template	System Access	LockoutDuration	15
Security Template	System Access	LSAAnonymousNameLookup	0
Security Template	System Access	MaximumPasswordAge	60
Security Template	System Access	MinimumPasswordAge	1
Security Template	System Access	MinimumPasswordLength	14
Security Template	System Access	PasswordComplexity	1
Security Template	System Access	PasswordHistorySize	24
Security Template	System Access	ResetLockoutCount	15

Policy Path:
Advanced Audit Policy Configuration
System Audit Policies\Account Logon
Credential Validation

Credential Validation

This policy setting allows you to audit events generated by validation tests on user account logon credentials.

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 local computer is authoritative.

Volume: High on domain controllers.

Default on Client editions: No Auditing.

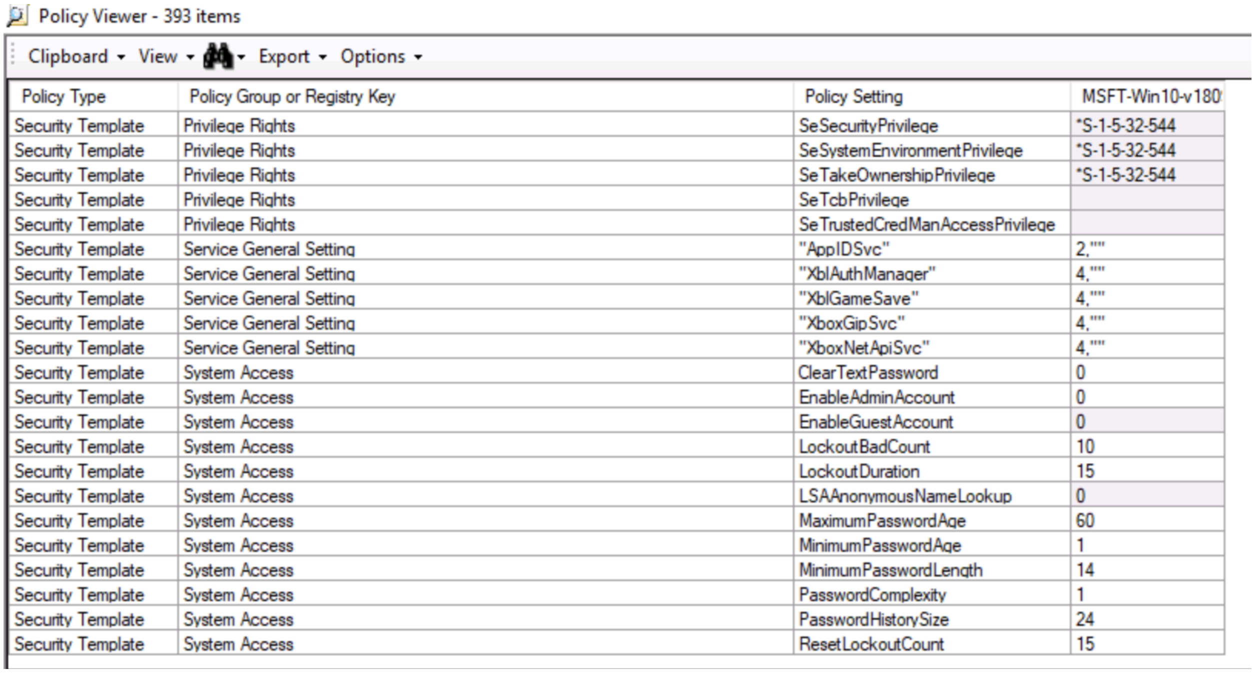
Default on Server editions: Success.

MSFT-Win10-v1809-RS5-WS2019-FINAL:
Option: Success and Failure
Defined in the following GPOs:

This feature, View/Compare, shows the settings currently in the baseline security template file.

11. Scroll to the bottom of the list and locate the **LockoutBadCount**, which is 9th from the bottom.

    What is the baseline value from the security template for the policy setting item of LockoutBadCount? 10



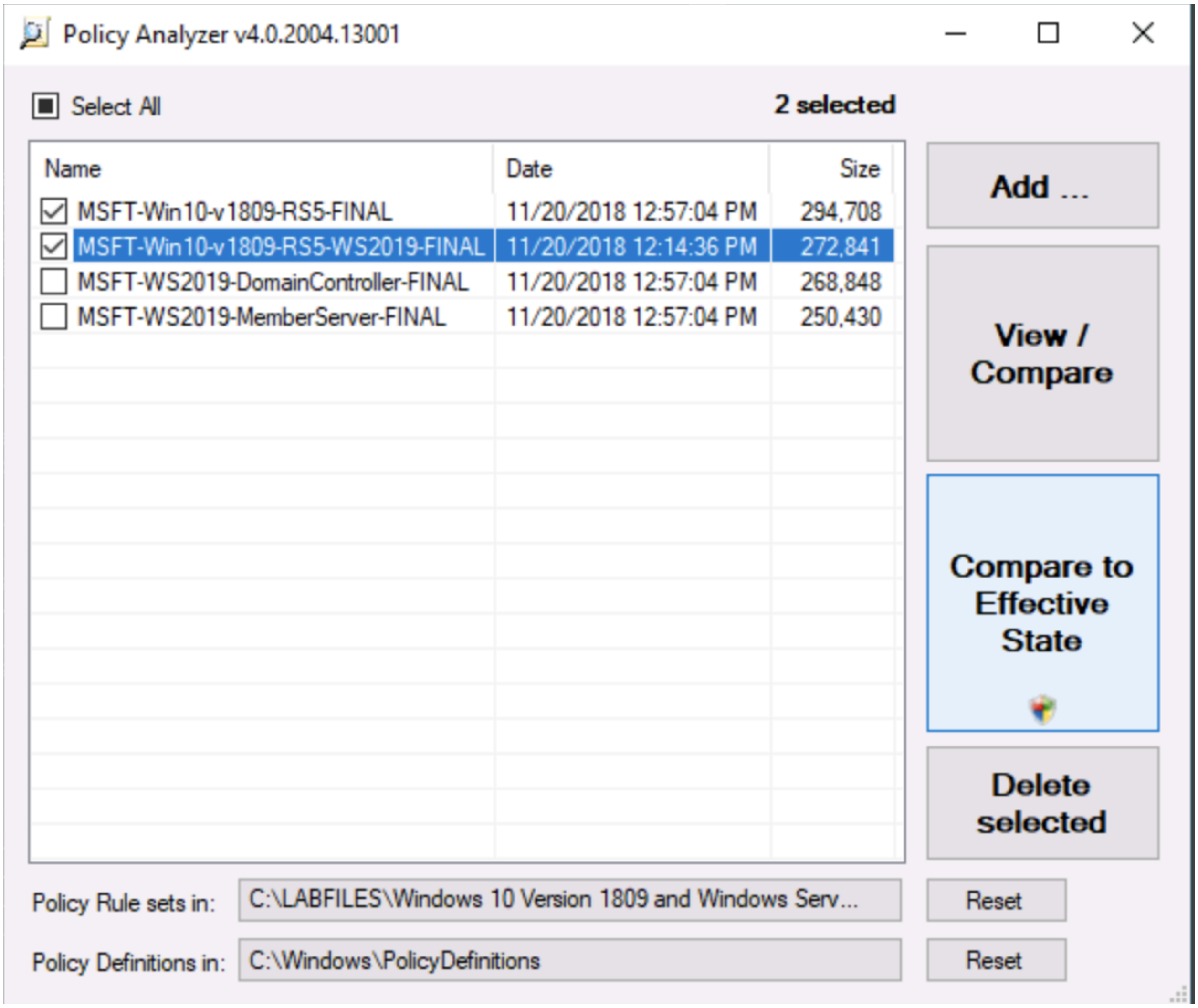
Policy Viewer - 393 items

Policy Type	Policy Group or Registry Key	Policy Setting	MSFT-Win10-v180
Security Template	Privilege Rights	SeSecurityPrivilege	*S-1-5-32-544
Security Template	Privilege Rights	SeSystemEnvironmentPrivilege	*S-1-5-32-544
Security Template	Privilege Rights	SeTakeOwnershipPrivilege	*S-1-5-32-544
Security Template	Privilege Rights	SeTcbPrivilege	
Security Template	Privilege Rights	SeTrustedCredManAccessPrivilege	
Security Template	Service General Setting	"AppIDSvc"	2,""
Security Template	Service General Setting	"XblAuthManager"	4,""
Security Template	Service General Setting	"XblGameSave"	4,""
Security Template	Service General Setting	"XboxGipSvc"	4,""
Security Template	Service General Setting	"XboxNetApiSvc"	4,""
Security Template	System Access	ClearTextPassword	0
Security Template	System Access	EnableAdminAccount	0
Security Template	System Access	EnableGuestAccount	0
Security Template	System Access	LockoutBadCount	10
Security Template	System Access	LockoutDuration	15
Security Template	System Access	LSAAnonymousNameLookup	0
Security Template	System Access	MaximumPasswordAge	60
Security Template	System Access	MinimumPasswordAge	1
Security Template	System Access	MinimumPasswordLength	14
Security Template	System Access	PasswordComplexity	1
Security Template	System Access	PasswordHistorySize	24
Security Template	System Access	ResetLockoutCount	15

12. Also near the bottom, locate **MinimumPasswordLength**, which is 4th from the bottom.

    What is the baseline value from the security template for the policy setting item of MinimumPasswordLength? 14

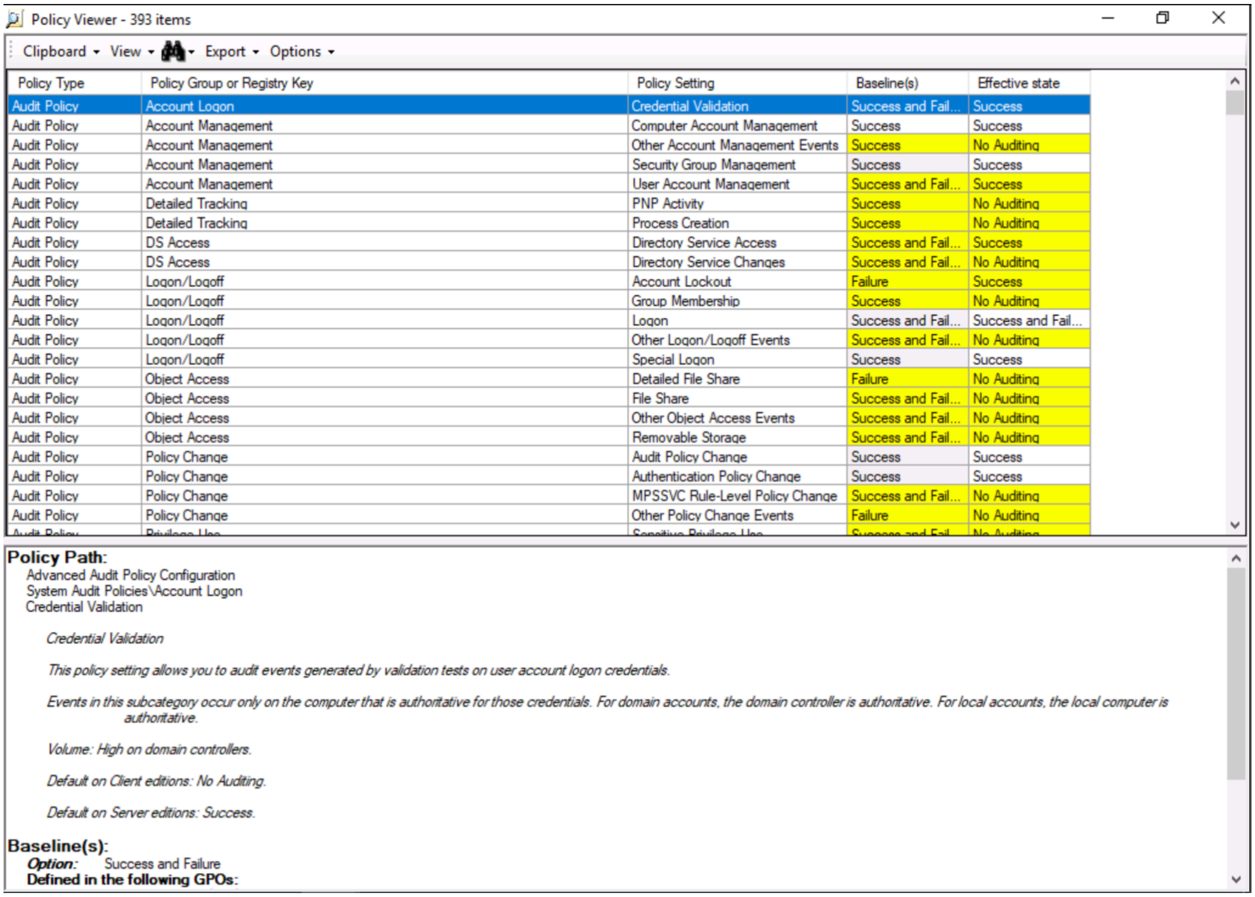
13. Perform a **Compare to Effective State** of MSFT-Win10-v1809-RS5-WS2019-FINAL using Policy Analyzer by marking the **MSFT-Win10-v1809-RS5-WS2019-FINAL** checkbox, then selecting **Compare to Effective State**.



Name	Date	Size
☑ MSFT-Win10-v1809-RS5-FINAL	11/20/2018 12:57:04 PM	294,708
☑ MSFT-Win10-v1809-RS5-WS2019-FINAL	11/20/2018 12:14:36 PM	272,841
☐ MSFT-WS2019-DomainController-FINAL	11/20/2018 12:57:04 PM	268,848
☐ MSFT-WS2019-MemberServer-FINAL	11/20/2018 12:57:04 PM	250,430

Policy Rule sets in: C:\LABFILES\Windows 10 Version 1809 and Windows Serv...

Policy Definitions in: C:\Windows\PolicyDefinitions



Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success
Audit Policy	Account Management	Computer Account Management	Success	Success
Audit Policy	Account Management	Other Account Management Events	Success	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success and Fail...	Success
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	DS Access	Directory Service Access	Success and Fail...	Success
Audit Policy	DS Access	Directory Service Changes	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Special Logon	Success	Success
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success	Success
Audit Policy	Policy Change	Authentication Policy Change	Success	Success
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	Failure	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	No Auditing

Policy Path:
Advanced Audit Policy Configuration
System Audit Policies\Account Logon
Credential Validation

Credential Validation

This policy setting allows you to audit events generated by validation tests on user account logon credentials.

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 local computer is authoritative.

Volume: High on domain controllers.

Default on Client editions: No Auditing.

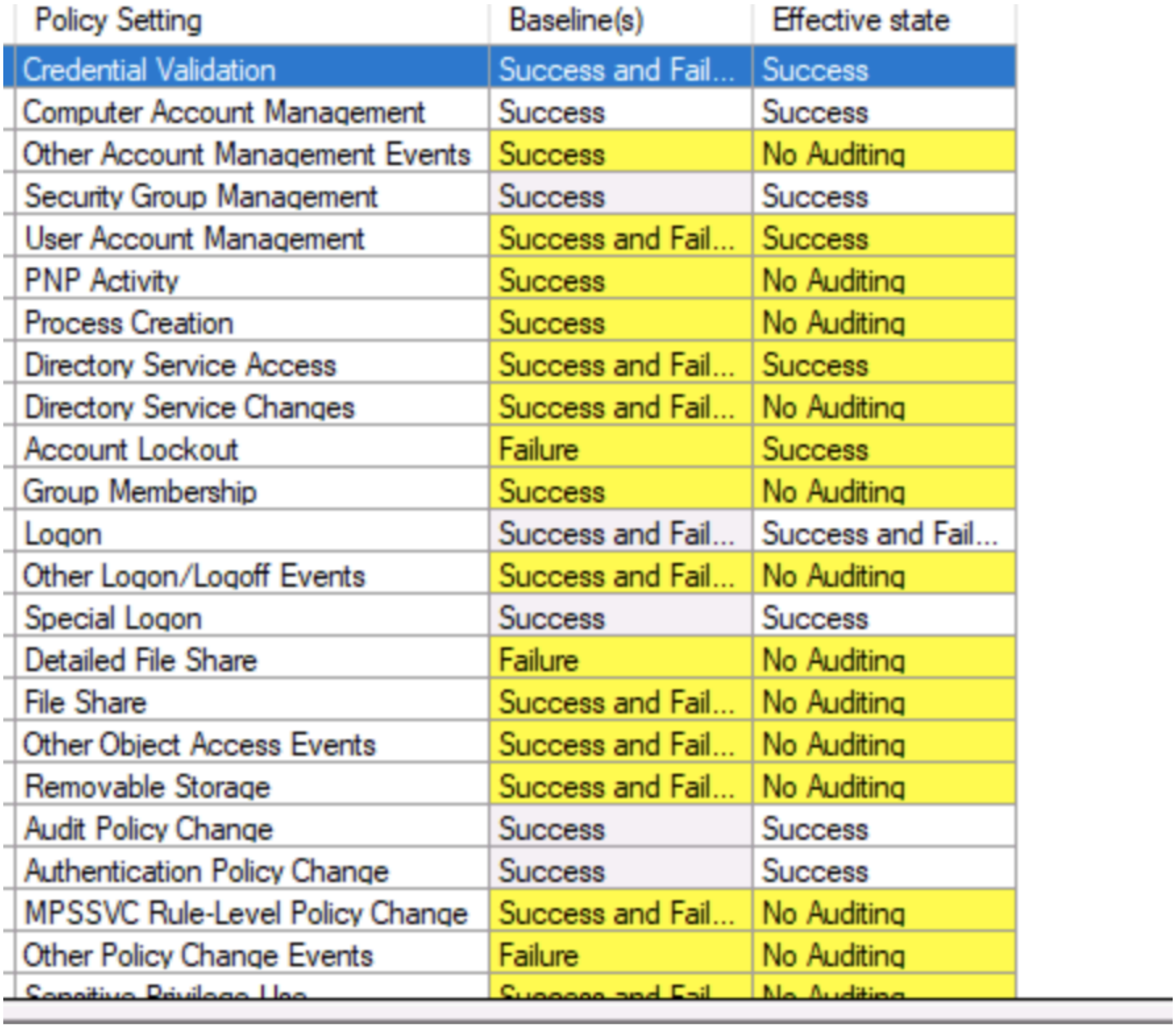
Default on Server editions: Success.

Baseline(s):
Option: Success and Failure
Defined in the following GPOs:

This feature, *Compare to Effective State*, performs a gap analysis between the baseline security template file and the current in-use values of the local operating system.

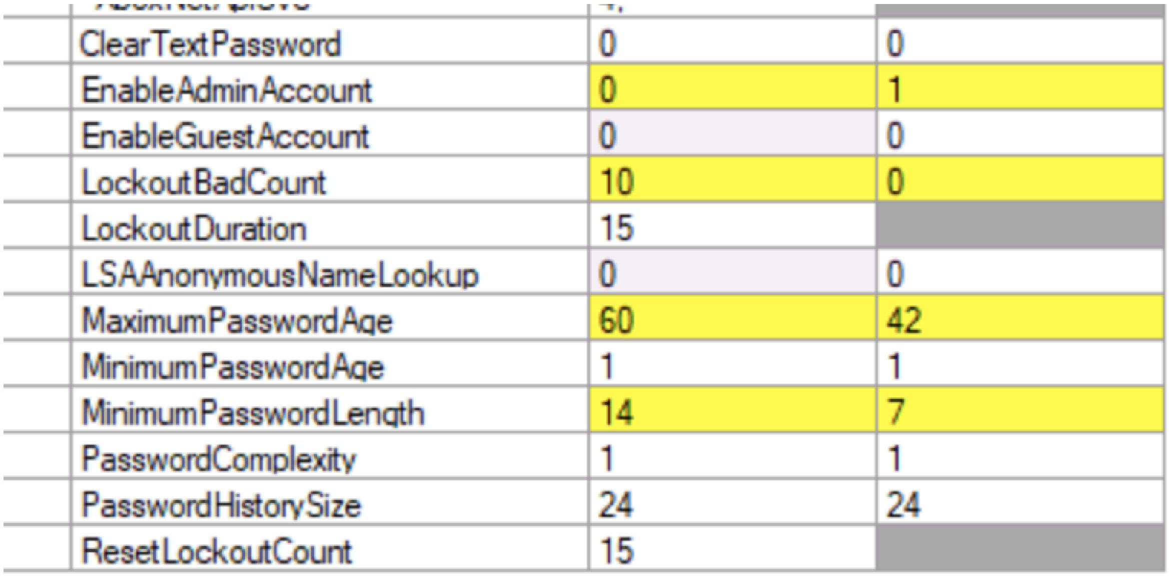
The *Policy Viewer* window will be displayed, showing a comparison between the various policy settings contained in the MSFT-Win10-v1809-RS5-WS2019-FINAL policy rule set and the current operating system (labeled as "Effective state").

14. Notice that many items are highlighted in yellow. These are where there are differences between the baseline file and the current effective state of the live operating system environment of PC10.



Policy Setting	Baseline(s)	Effective state
Credential Validation	Success and Fail...	Success
Computer Account Management	Success	Success
Other Account Management Events	Success	No Auditing
Security Group Management	Success	Success
User Account Management	Success and Fail...	Success
PNP Activity	Success	No Auditing
Process Creation	Success	No Auditing
Directory Service Access	Success and Fail...	Success
Directory Service Changes	Success and Fail...	No Auditing
Account Lockout	Failure	Success
Group Membership	Success	No Auditing
Logon	Success and Fail...	Success and Fail...
Other Logon/Logoff Events	Success and Fail...	No Auditing
Special Logon	Success	Success
Detailed File Share	Failure	No Auditing
File Share	Success and Fail...	No Auditing
Other Object Access Events	Success and Fail...	No Auditing
Removable Storage	Success and Fail...	No Auditing
Audit Policy Change	Success	Success
Authentication Policy Change	Success	Success
MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Other Policy Change Events	Failure	No Auditing
Sensitive Privilege Use	Success and Fail...	No Auditing

15. Notice the Effective state value of LockoutBadCount is 0, and MinimumPasswordLength is 7.



ClearTextPassword	0	0
EnableAdminAccount	0	1
EnableGuestAccount	0	0
LockoutBadCount	10	0
LockoutDuration	15	
LSAAnonymousNameLookup	0	0
MaximumPasswordAge	60	42
MinimumPasswordAge	1	1
MinimumPasswordLength	14	7
PasswordComplexity	1	1
PasswordHistorySize	24	24
ResetLockoutCount	15	

16. Is the PC10 system in compliance with the security template based on the gap analysis results? NO
17. Performing gap analysis forces systems into compliance. False
18. Gap analysis is a process that identifies how an organization's security systems deviate from those required or recommended by a framework. True
19. When should gap analysis be performed? (Select all that apply)
    - ☑ ~~when meeting a new industry or legal compliance requirement~~
    - ☑ ~~after significant time has past~~
    - ☑ ~~when first adopting a framework~~
    - ☐ when decommissioning legacy hardware
20. What is the purpose of a gap analysis? discovering the differences between the intended or expected configuration of a system and its actual operating configuration
21. Which of the following statements is false in regard to gap analysis? A single security template is sufficient to analyze all systems