**AUDIT RESULT:**

"21.8 (L2) Ensure 'Enable File Hash Computation' is set to 'Enable': [FAILED]"

**CONCLUSION:**

No fix required, but note the reasoning.

**INVESTIGATION:**

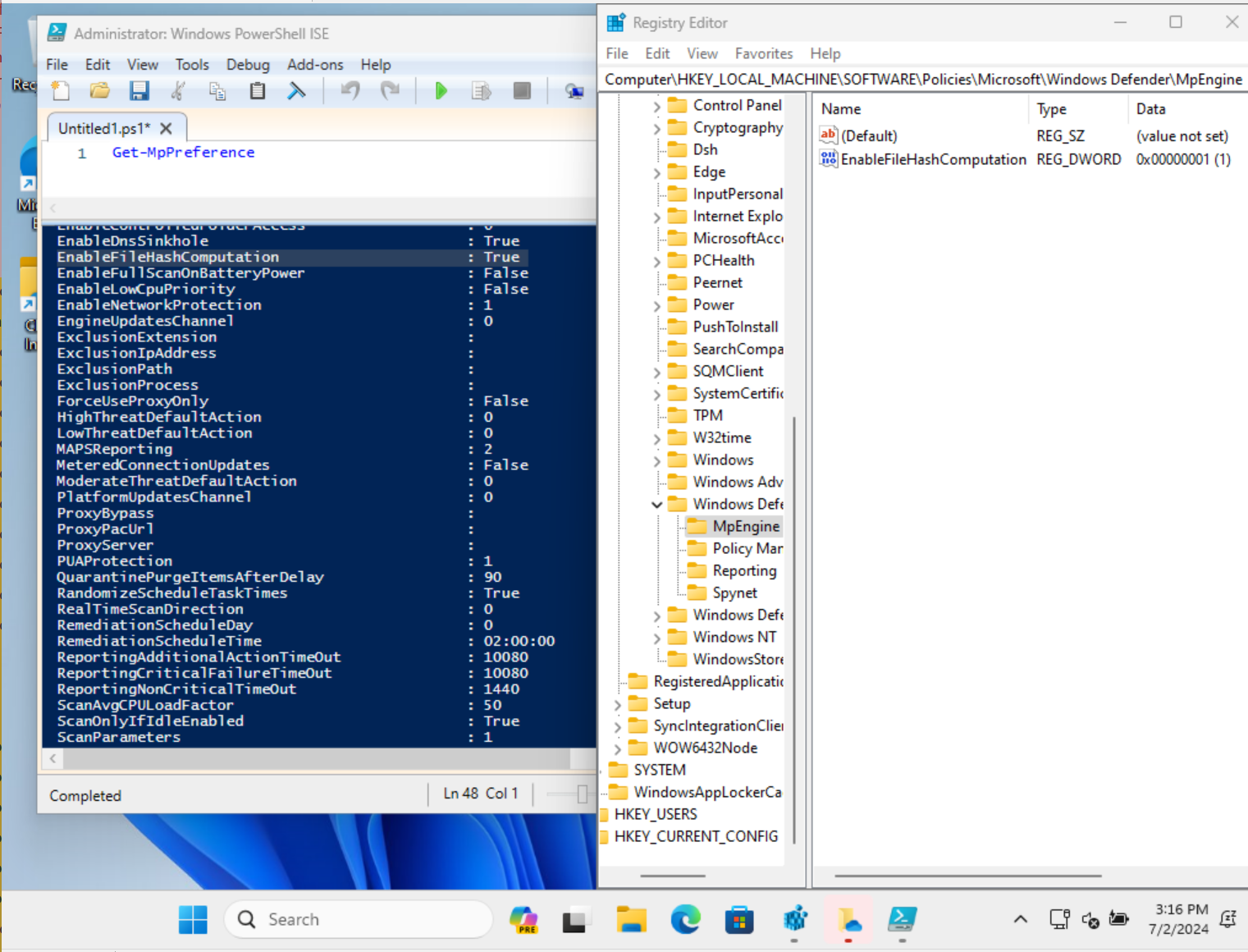
The file hash config is enabled, but CIS/Tenable are referencing the registry key **HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:EnableFileHashComputation** .

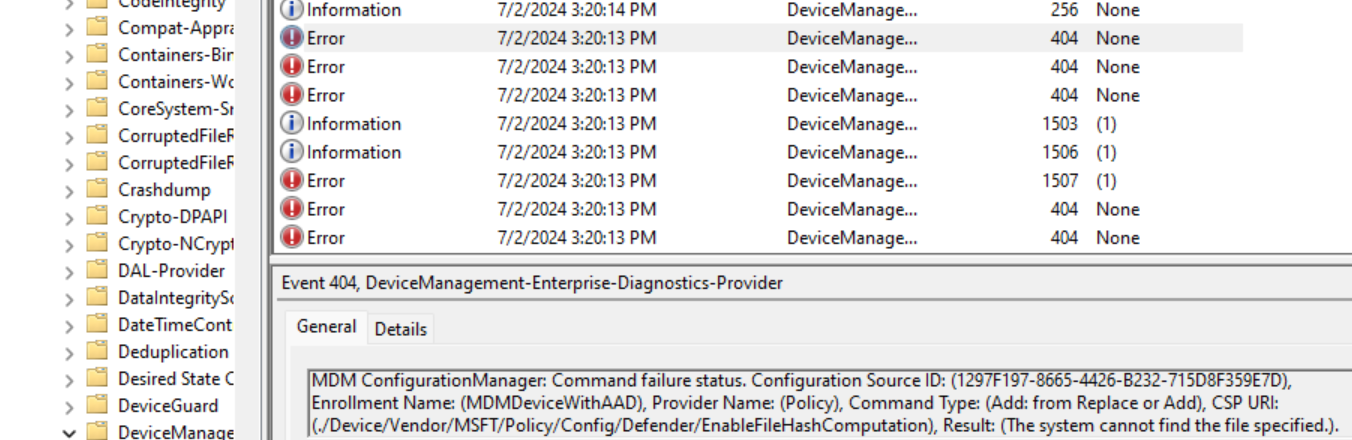
There is currently no “Defender” OMAURI for EnableFileHashComputation, but there is an OMAURI for “MpEngine”. This configuration is setting the following registry key: **HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine:EnableFileHashComputation**  to **1**

This effectively applies EnableFileHashComputation and it cannot be disabled with powershell using the set-mppreference feature.

Additional Notes: I attempted creating the OMAURI “./Device/Vendor/MSFT/Policy/Config/Defender/EnableFileHashComputation”, but this resulted in an error in the event viewer. OMAURI thus does not exist in the Defender URI as of 2024.07.02.

**PROOF:**





**AUDIT RESULT:**

"24.1 (L1) Ensure 'Alphanumeric Device Password Required' is set to 'Password, Numeric PIN, or Alphanumeric PIN required': [FAILED]"

**CONCLUSION:**

No fix required. Appears to be set properly.

**INVESTIGATION:**

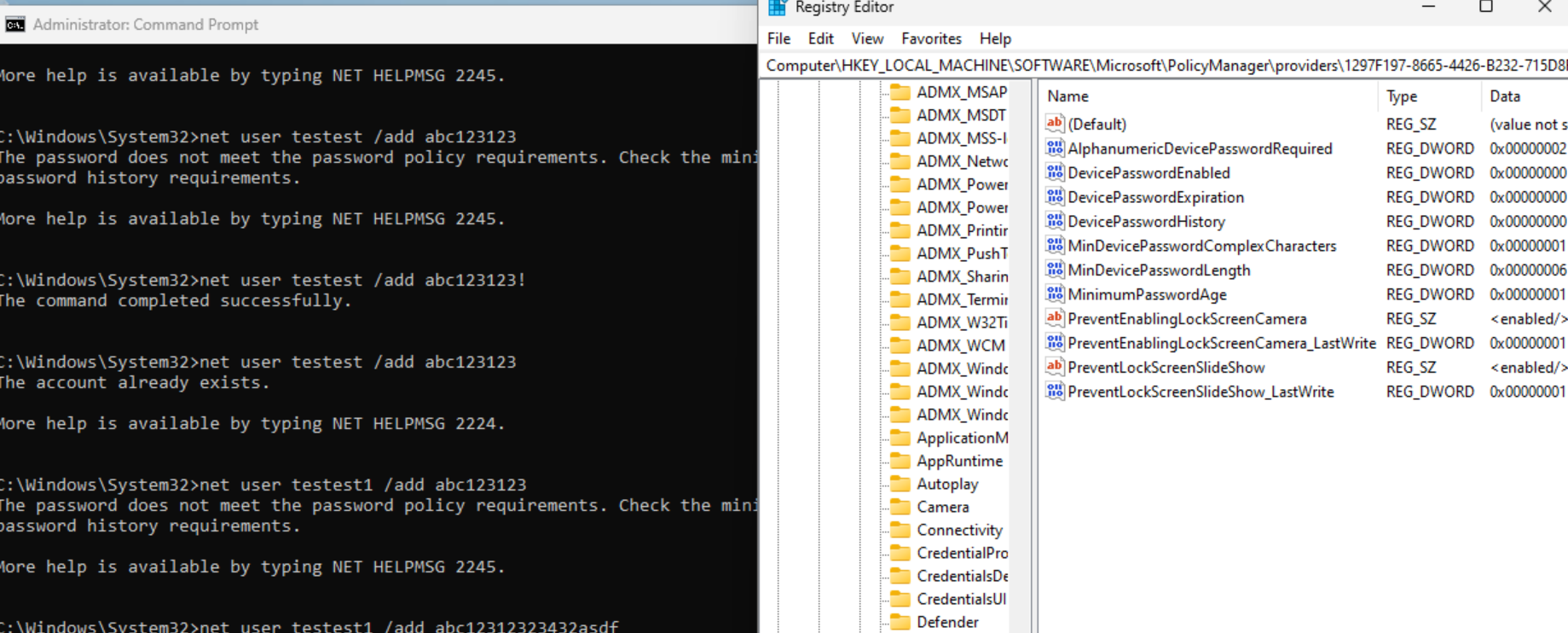
The specified registry keys in the CIS Benchmark exist and are set to the proper value.

**HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:AlphanumericDevicePasswordRequired** = 2

When attempting to create a user without a special character, the attempt failed which is the expected result when this is configured.

The audit file appears to be correct.

**PROOF:**

****

**AUDIT RESULT:**

"24.4 (L1) Ensure 'Min Device Password Complex Characters' is set to 'Digits lowercase letters and uppercase letters are required': [FAILED]"

**CONCLUSION:**

Policy setting was missing in configuration. It has been added.

**INVESTIGATION:**

The Powershell configuration was observed to be missing the setting.

**AUDIT RESULT:**

"24.5 (L1) Ensure 'Min Device Password Length' is set to '14 or more character(s)': [FAILED]"

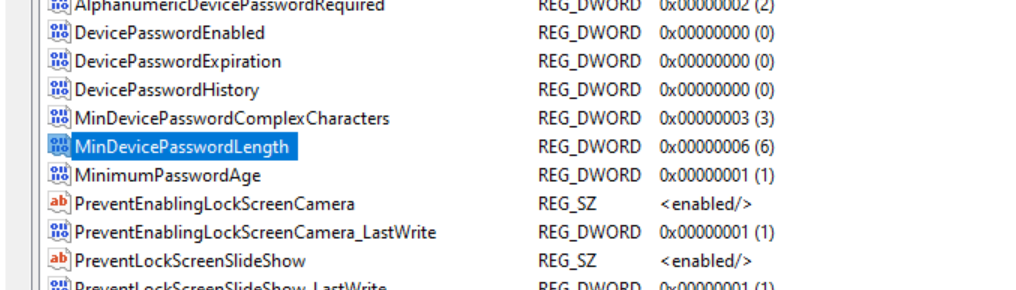
**CONCLUSION:**

Update the configuration to 14.

**INVESTIGATION:**

The min password is set to 6. This is a misconfiguration. This was set because it was thought this would control the Windows hello Pin. However, there is an alternate way to control Windows Hello Pin using the Passport registry key. This has been updated in the configuration to correct the issue.

**PROOF:**



**AUDIT RESULT:**

"3.10.19.2 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE': [FAILED]"

**CONCLUSION:**

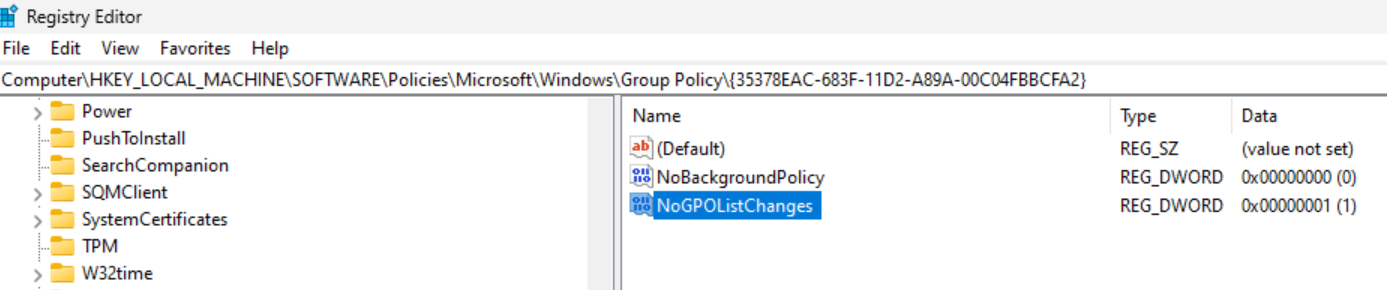
Policy needs to update CSE\_NOBACKGROUND10 to True instead of False.

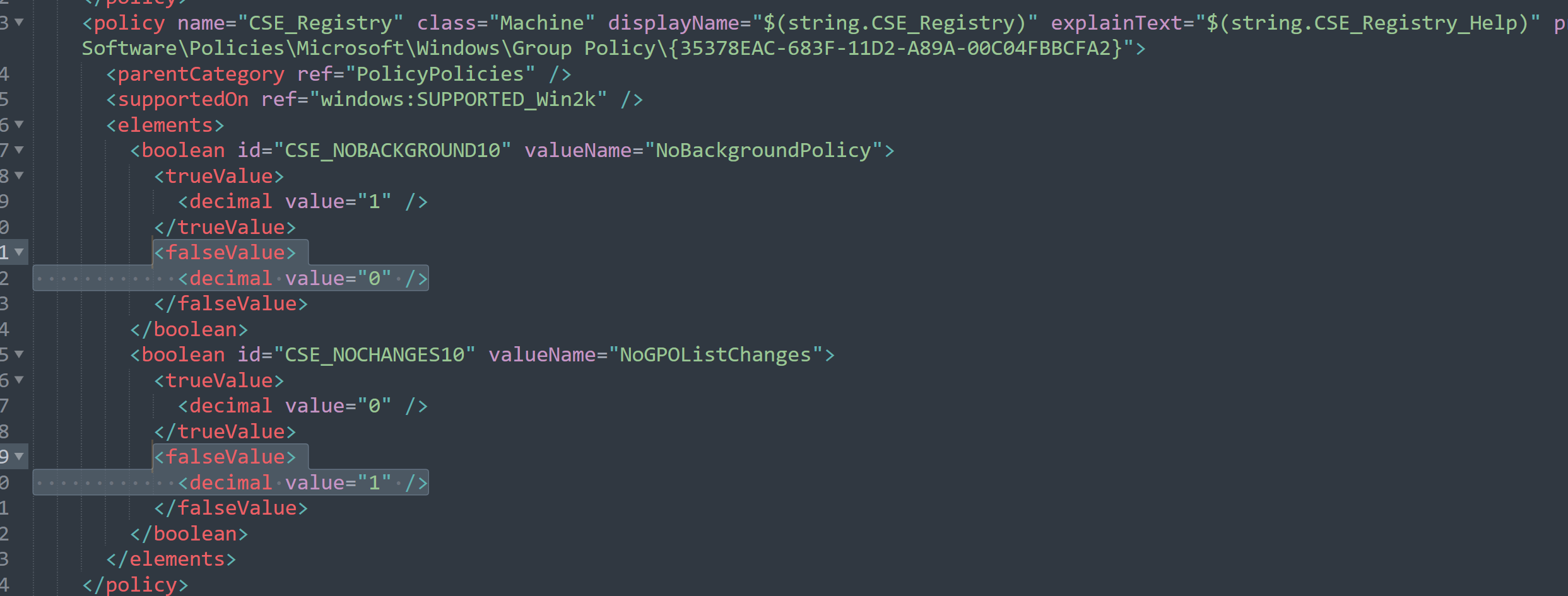
**INVESTIGATION:**

The registry value of HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\NoGPOListChanges was set to 1 which is not the desired configuration. This configuration is bundled in with the 3.10.19.1 option and that one was applied successfully.

It seems that the Group Policy object has reversed the True and False for NoGPOListChanges. The configuration should be set to the opposite of what it is currently. The correct value is noted appropriately in the CIS configuration benchmark. Policy will be updated.

**PROOF:**





**AUDIT RESULT:**

"3.10.19.4 (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE': [FAILED]"

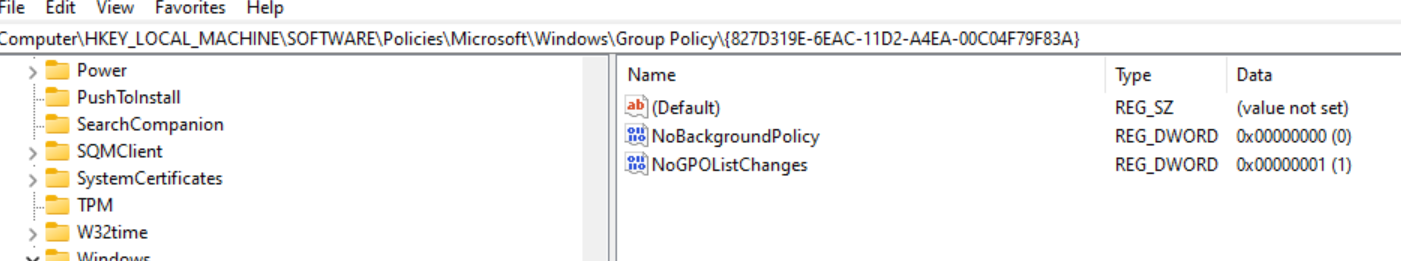
**CONCLUSION:**

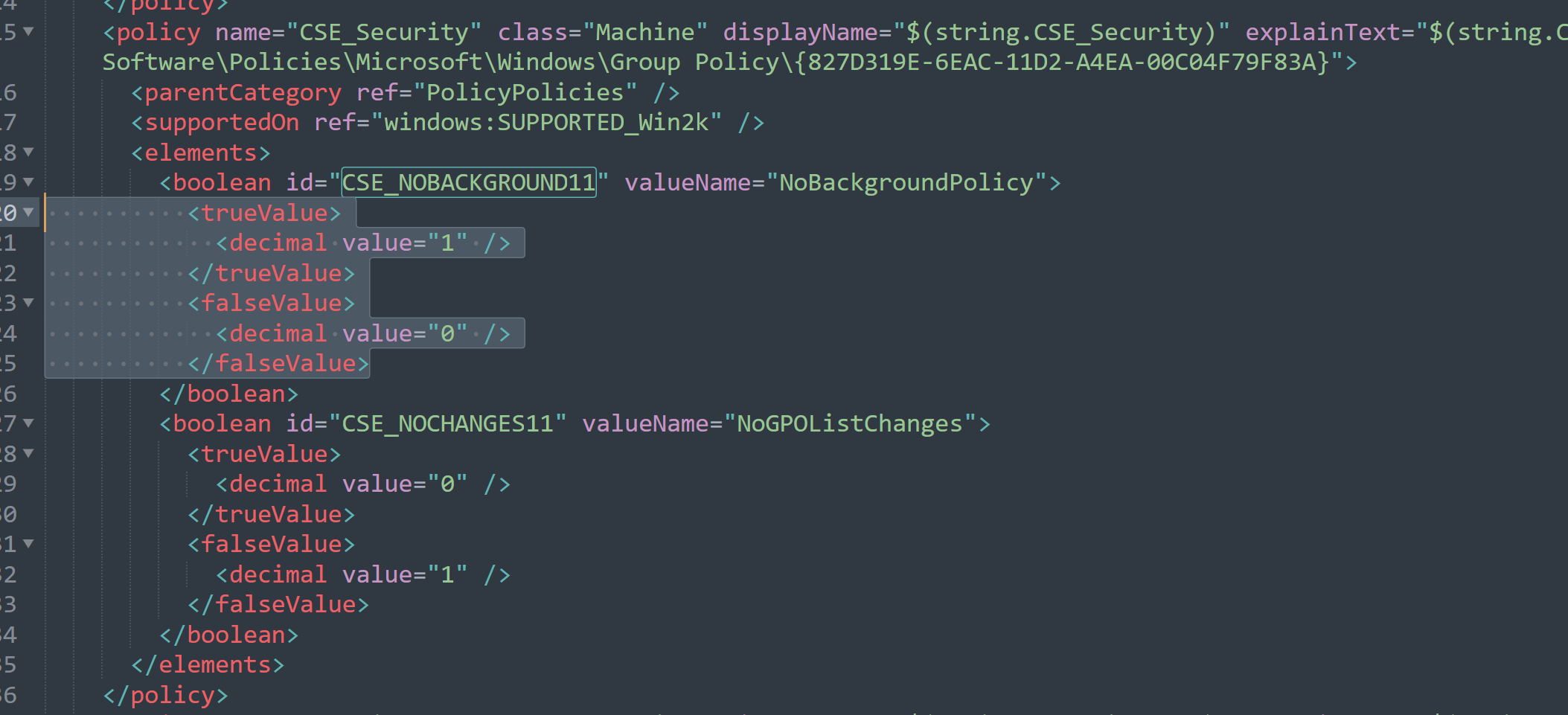
Policy needs to update CSE\_NOBACKGROUND11 to True instead of False.

**INVESTIGATION:**

The registry value of HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\NoGPOListChanges was set to 1 which is not the desired configuration. This configuration is bundled in with the 3.10.19.1 option and that one was applied successfully.

It seems that the Group Policy object has reversed the True and False for NoGPOListChanges. The configuration should be set to the opposite of what it is currently. The correct value is noted appropriately in the CIS configuration benchmark. Policy will be updated.

**PROOF:** ****



**AUDIT RESULT:**

"3.10.20.1.1 (L2) Ensure 'Turn off access to the Store' is set to 'Enabled': [FAILED]"

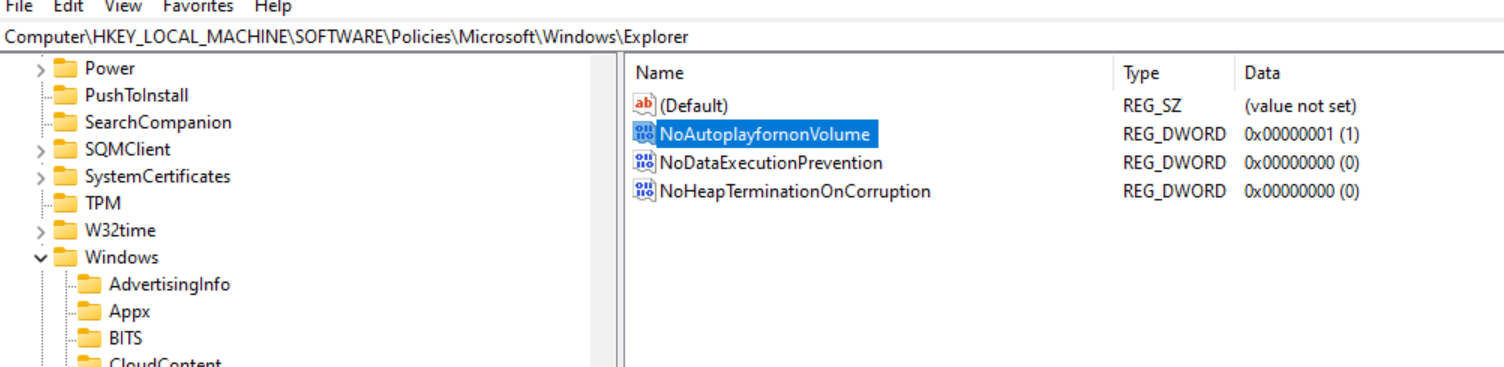
**CONCLUSION:**

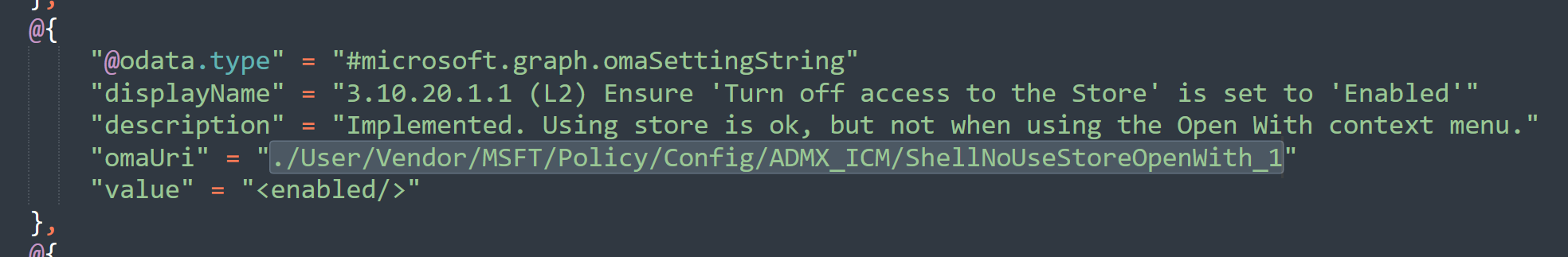
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_ICM/ShellNoUseStoreOpenWith\_2**

**INVESTIGATION:**

The registry value of HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoUseStoreOpenWith is not set properly. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI with the ShellNoUseStoreOpenWith\_2 URI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**





**AUDIT RESULT:**

"3.10.20.1.2 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled': [FAILED]"

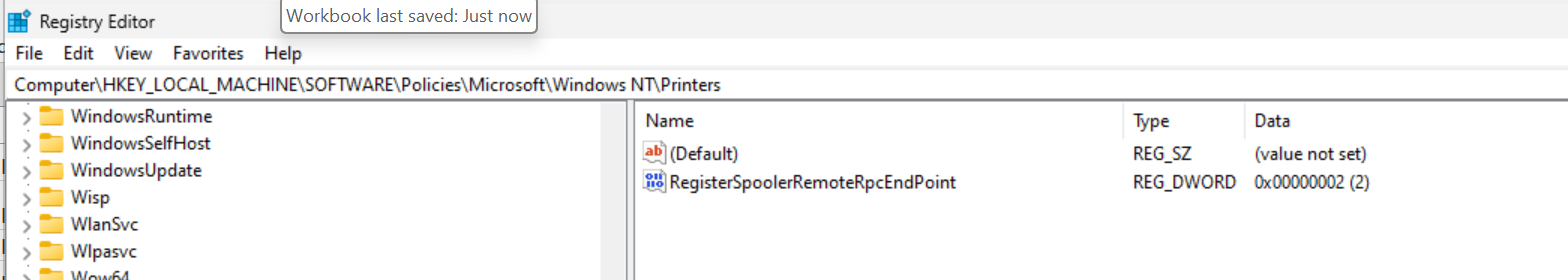
**CONCLUSION:**

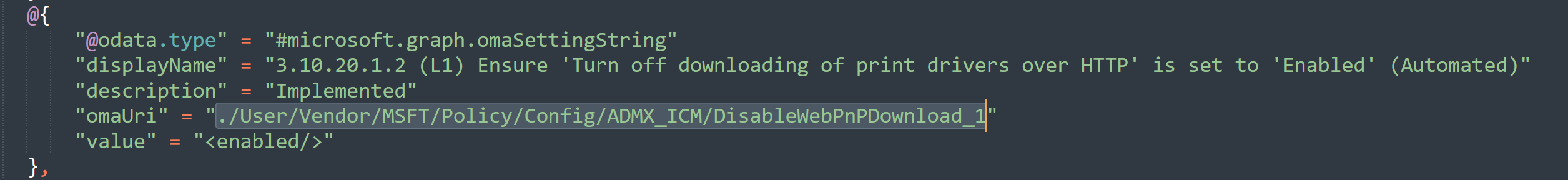
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/Connectivity/DisableDownloadingOfPrintDriversOverHTTP**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableWebPnPDownload is not found. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**



****

**AUDIT RESULT:**

"3.10.20.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled': [FAILED]"

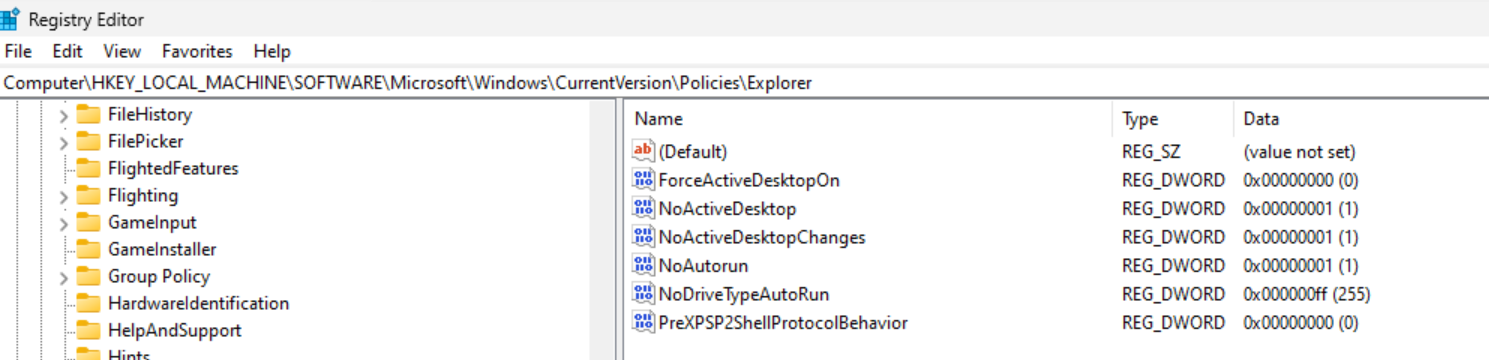
**CONCLUSION:**

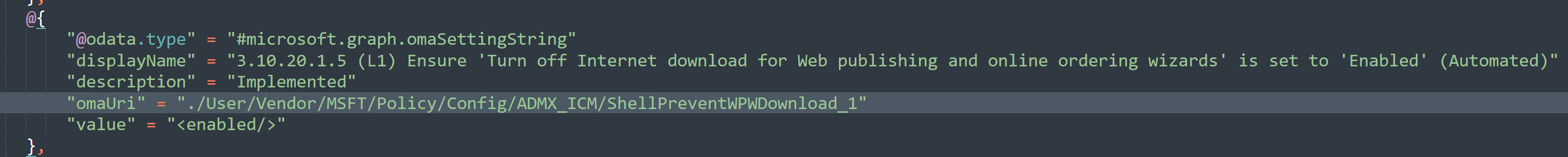
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/Connectivity/DisableInternetDownloadForWebPublishingAndOnlineOrderingWizards**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoWebServices is not found. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**

****

****

**AUDIT RESULT:**

"3.10.20.1.6 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled': [FAILED]"

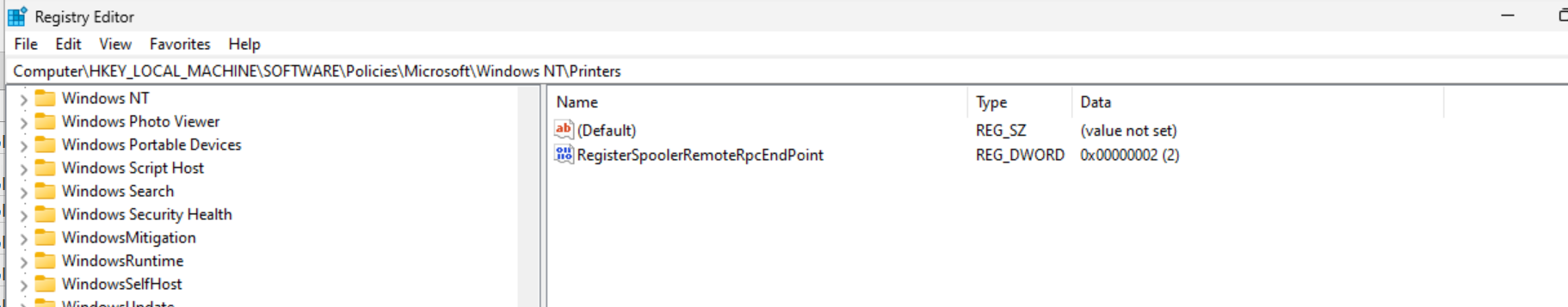
**CONCLUSION:**

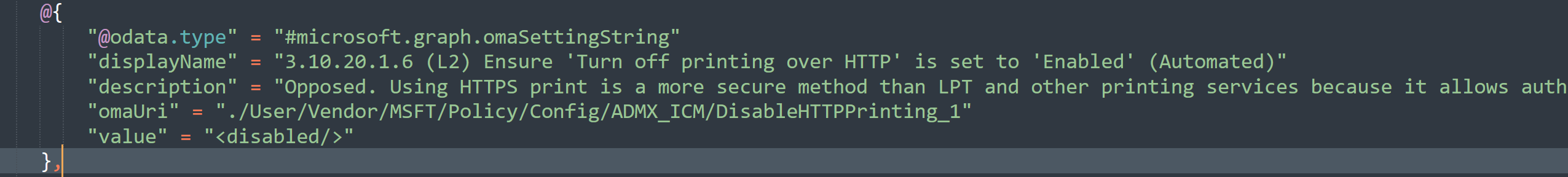
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/Connectivity/DiablePrintingOverHTTP**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableHTTPPrinting is not found. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**

****

****

**AUDIT RESULT:**

"3.10.20.1.9 (L2) Ensure 'Turn off the 'Order Prints' picture task' is set to 'Enabled': [FAILED]"

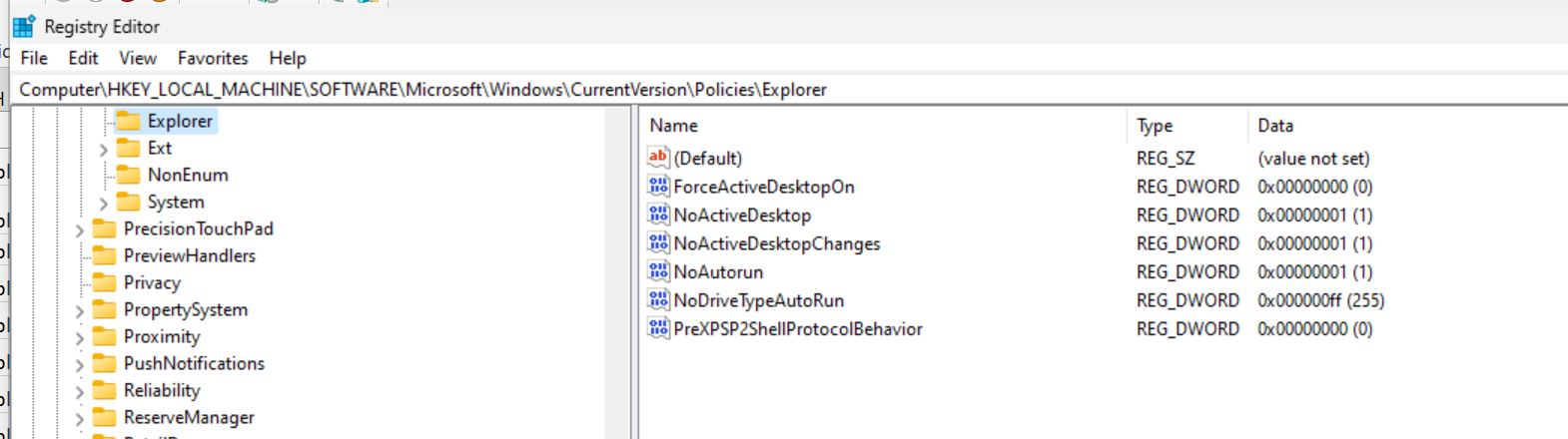
**CONCLUSION:**

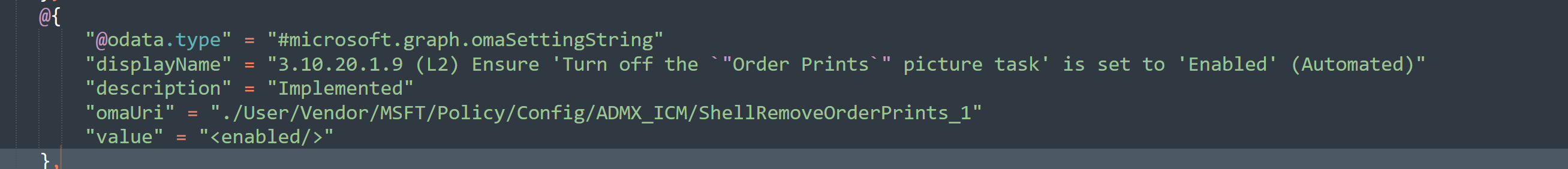
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_ICM/ShellRemoveOrderPrints\_2**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoOnlinePrintsWizard is not found. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**

****

****

**AUDIT RESULT:**

"3.10.20.1.10 (L2) Ensure 'Turn off the 'Publish to Web' task for files and folders' is set to 'Enabled': [FAILED]"

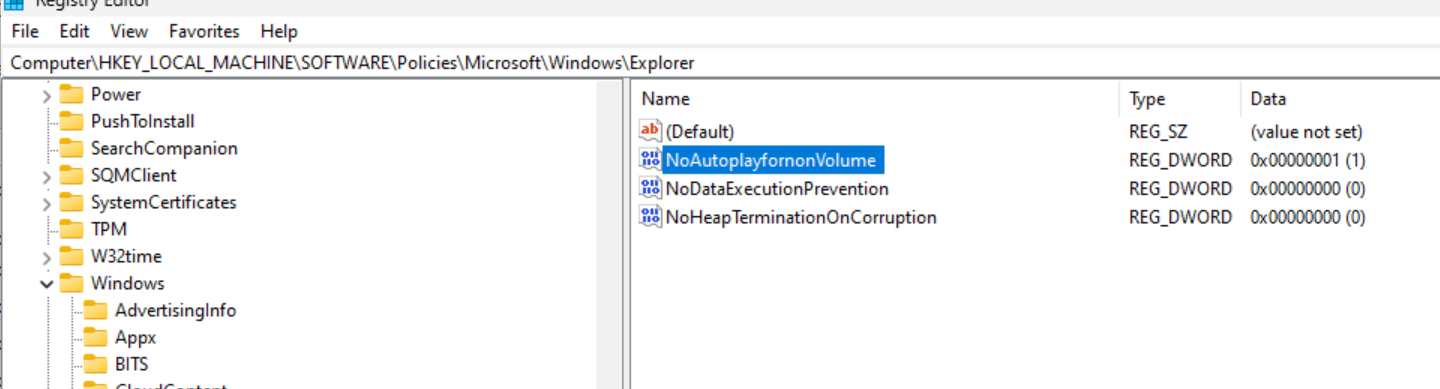
**CONCLUSION:**

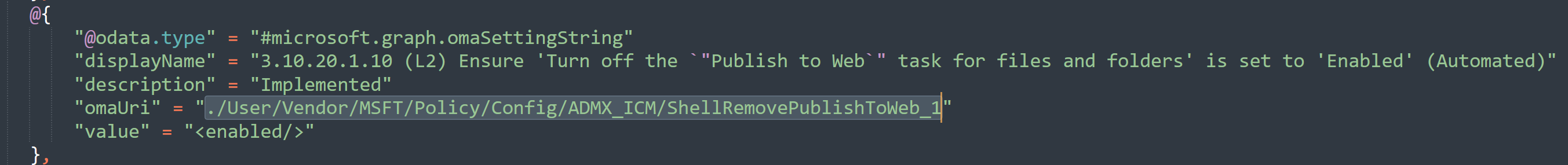
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_ICM/ShellRemovePublishToWeb\_2**

**INVESTIGATION:**

The registry value of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoPublishingWizard is not set properly. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI with the ShellRemovePublishToWeb\_2 URI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**

****



**AUDIT RESULT:**

"3.10.20.1.11 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled': [FAILED]"

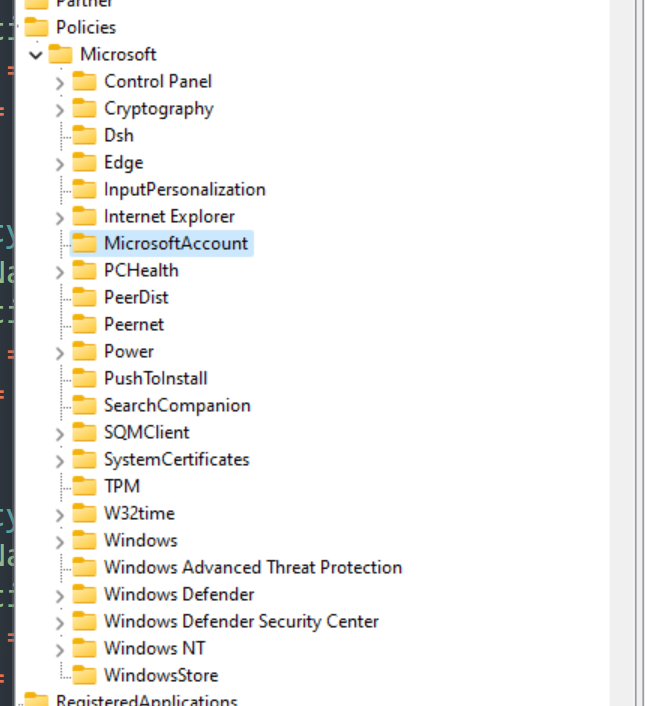
**CONCLUSION:**

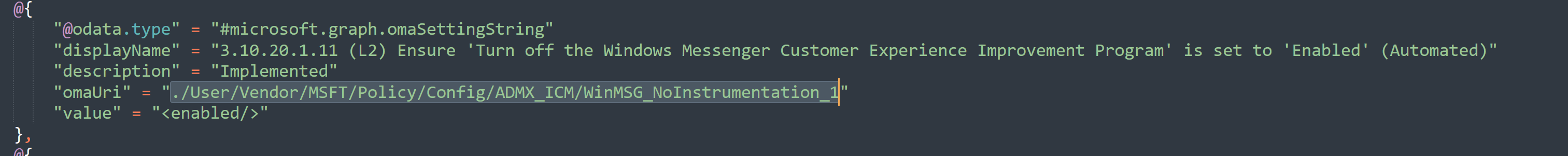
Update policy OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_ICM/WinMSG\_NoInstrumentation\_2**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Messenger\Client:CEIP is not found. The configuration is specifying the OMAURI using the ./User context. An alternative solution is to use the ./Device OMAURI with the WinMSG\_NoInstrumentation\_2 URI. The configuration will be updated to this to see if this configuration will apply.

**PROOF:**

****



**AUDIT RESULT:**

"3.10.28.5.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled': [FAILED]"

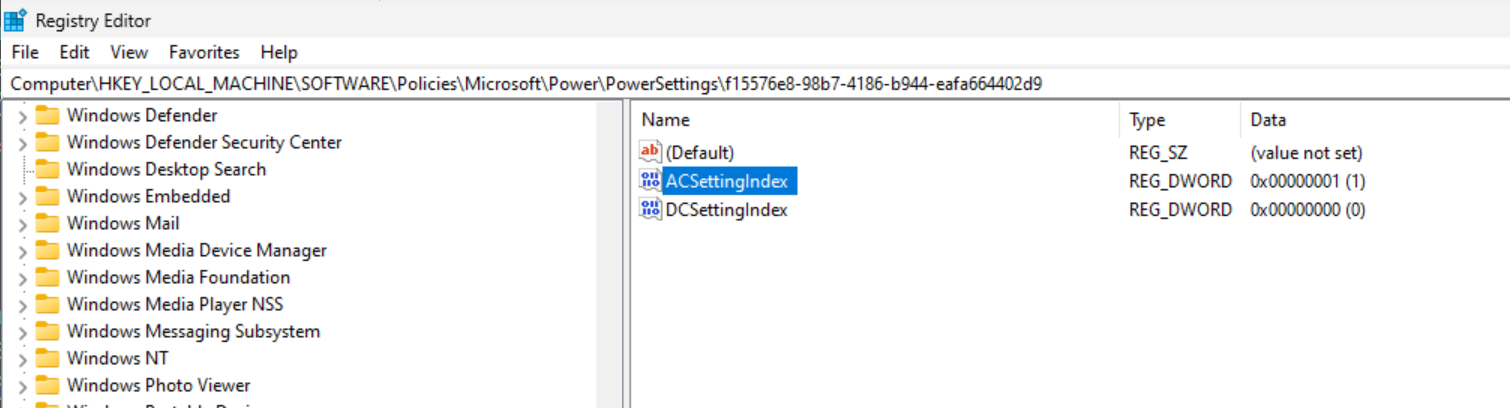
**CONCLUSION:**

No change. Policy was opposed.

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:ACSettingIndex was set to the desired setting. We opposed the CIS recommendation and set the value to enabled. No change to policy configuration is required since it is working as intended.

**PROOF:**

****

**AUDIT RESULT:**

"3.10.28.5.3 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled': [FAILED]"

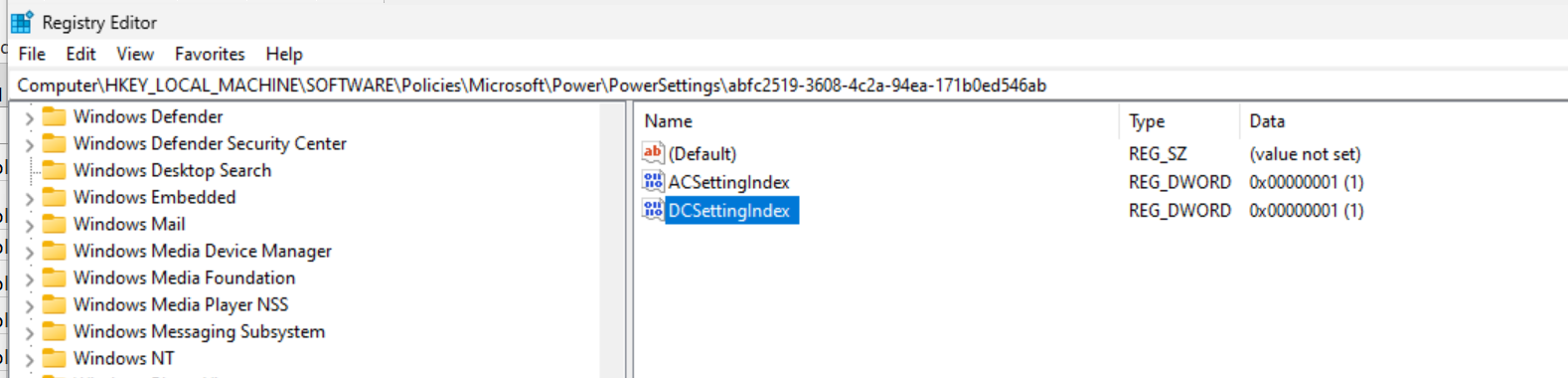
**CONCLUSION:**

No change. Policy was opposed.

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab:DCSettingIndex was set to the desired setting. We opposed the CIS recommendation and set the value to enabled. No change to policy configuration is required since it is working as intended.

**PROOF:**

****

**AUDIT RESULT:**

"3.10.28.5.4 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled': [FAILED]"

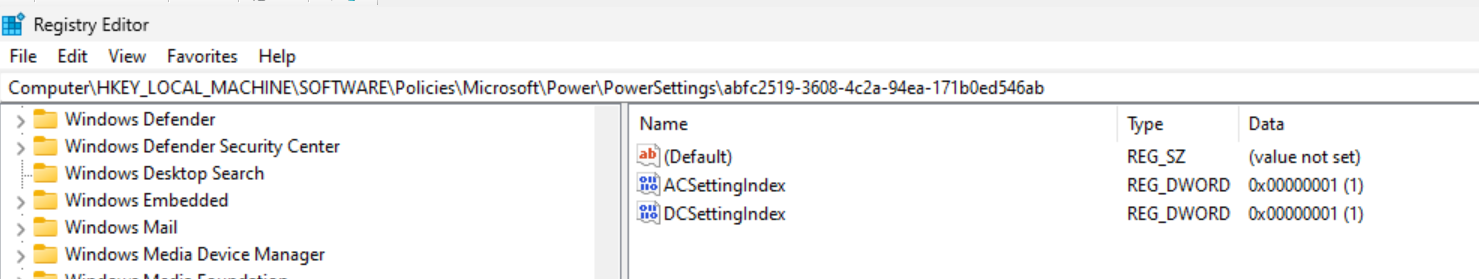
**CONCLUSION:**

No change. Policy was opposed.

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab:ACSettingIndex was set to the desired setting. We opposed the CIS recommendation and set the value to enabled. No change to policy configuration is required since it is working as intended.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.15.1.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

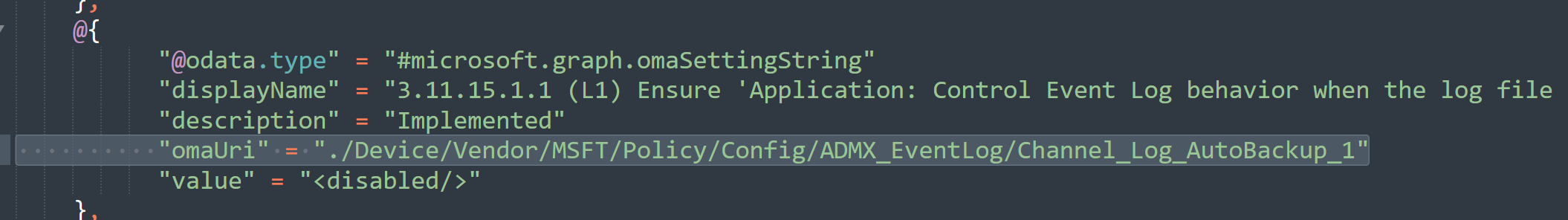
Update OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_1**

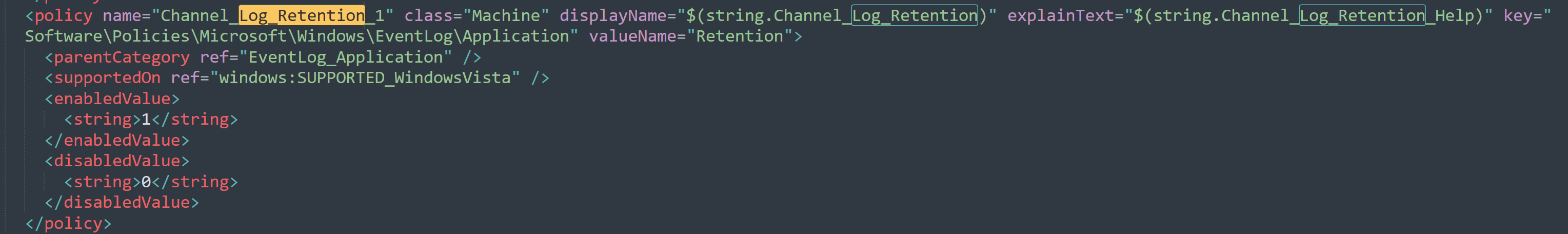
**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:Retention is not set. When altering the policy to set it to “Enabled”, the policy still did not set any registry entry. This is in contrast to what happens when altering the Group Policy setting. When altering Group Policy the “Retention” value was set to 0 when set to Enabled, 1 when it was disabled, and it was deleted when set to Not Configured.

The OMAURI ./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_1 should be used instead of the current one.

**PROOF:**

**** ****

****

**AUDIT RESULT:**

"3.11.15.2.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

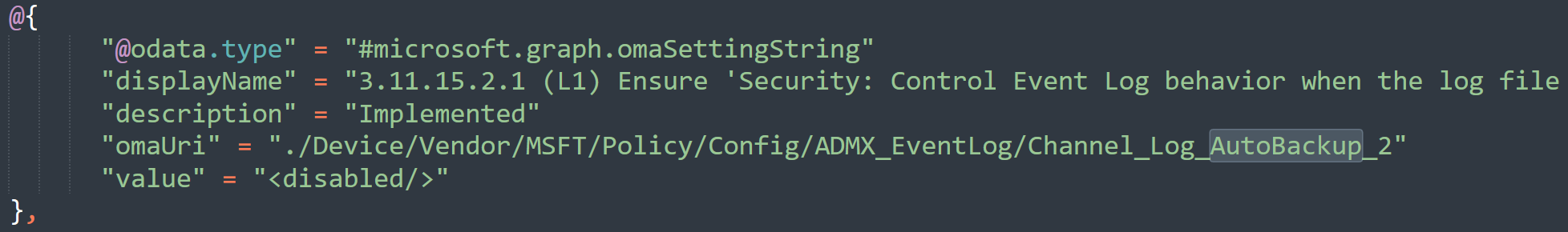
Update OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_2**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Retention is not set. When altering the policy to set it to “Enabled”, the policy still did not set any registry entry. This is in contrast to what happens when altering the Group Policy setting. When altering Group Policy the “Retention” value was set to 0 when set to Enabled, 1 when it was disabled, and it was deleted when set to Not Configured.

The OMAURI ./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_2 should be used instead of the current one.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.15.3.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

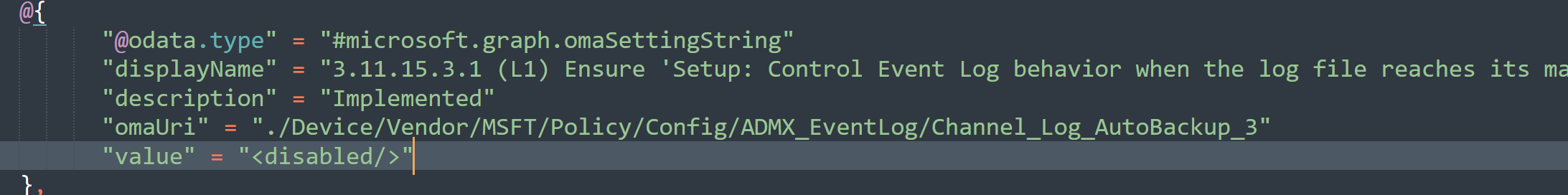
Update OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_3**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retention is not set. When altering the policy to set it to “Enabled”, the policy still did not set any registry entry. This is in contrast to what happens when altering the Group Policy setting. When altering Group Policy the “Retention” value was set to 0 when set to Enabled, 1 when it was disabled, and it was deleted when set to Not Configured.

The OMAURI ./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_3 should be used instead of the current one.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.15.4.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

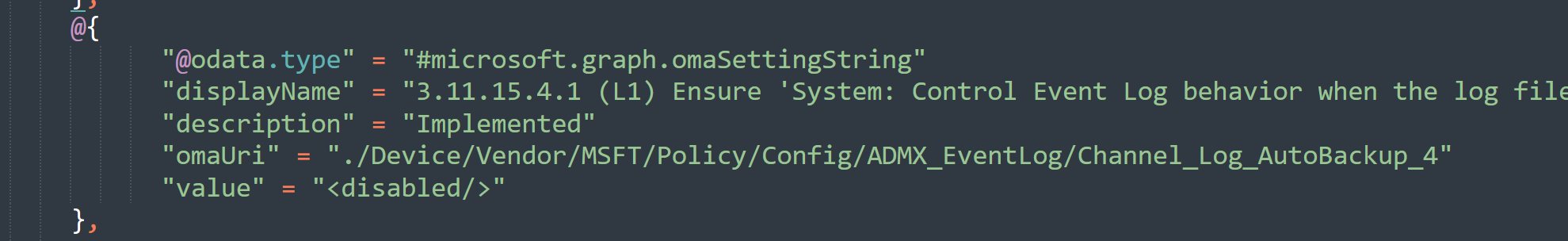
Update OMAURI to: **./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_4**

**INVESTIGATION:**

The registry value HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retention is not set. When altering the policy to set it to “Enabled”, the policy still did not set any registry entry. This is in contrast to what happens when altering the Group Policy setting. When altering Group Policy the “Retention” value was set to 0 when set to Enabled, 1 when it was disabled, and it was deleted when set to Not Configured.

The OMAURI ./Device/Vendor/MSFT/Policy/Config/ADMX\_EventLog/Channel\_Log\_Retention\_4 should be used instead of the current one.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.18.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass': [FAILED]"

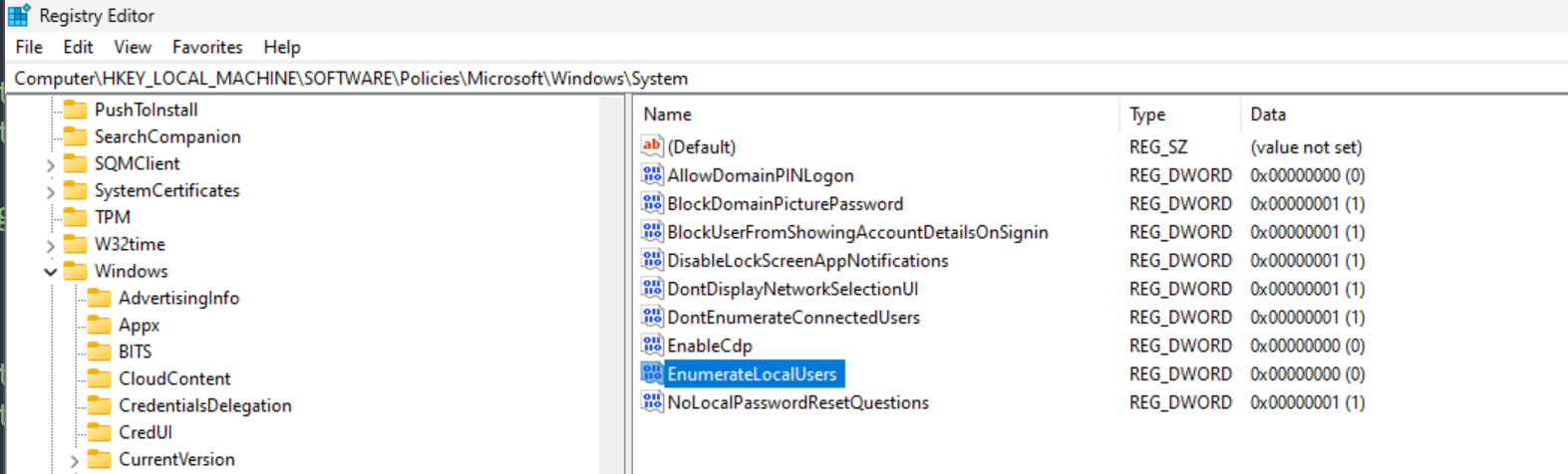
**CONCLUSION:**

Add an additional OMAURI for **./Device/Vendor/MSFT/Policy/Config/SmartScreen/PreventOverrideForFilesInShell**

**INVESTIGATION:**

The registry key was not set. While reviewing the policy, an OMAURI was set for Enable SmartScreen, but the “prevent override” was not set. The PreventOverrideForFilesInShell setting will be enabled which should remediate this issue.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.28.11 (L1) Ensure 'Turn off Microsoft Defender Antivirus' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

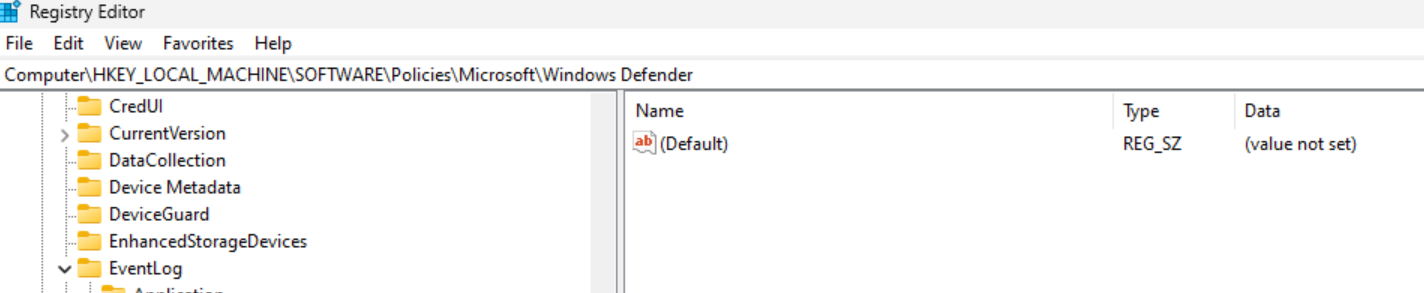
Update config with new OMAURI: **./Device/Vendor/MSFT/Policy/Config/ADMX\_MicrosoftDefenderAntivirus/DisableAntiSpywareDefender**

set to disabled

**INVESTIGATION:**

The registry key was not set and there was no OMAURI defined. One will be created for the policy.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.28.11 (L1) Ensure 'Turn off Microsoft Defender Antivirus' is set to 'Disabled': [FAILED]"

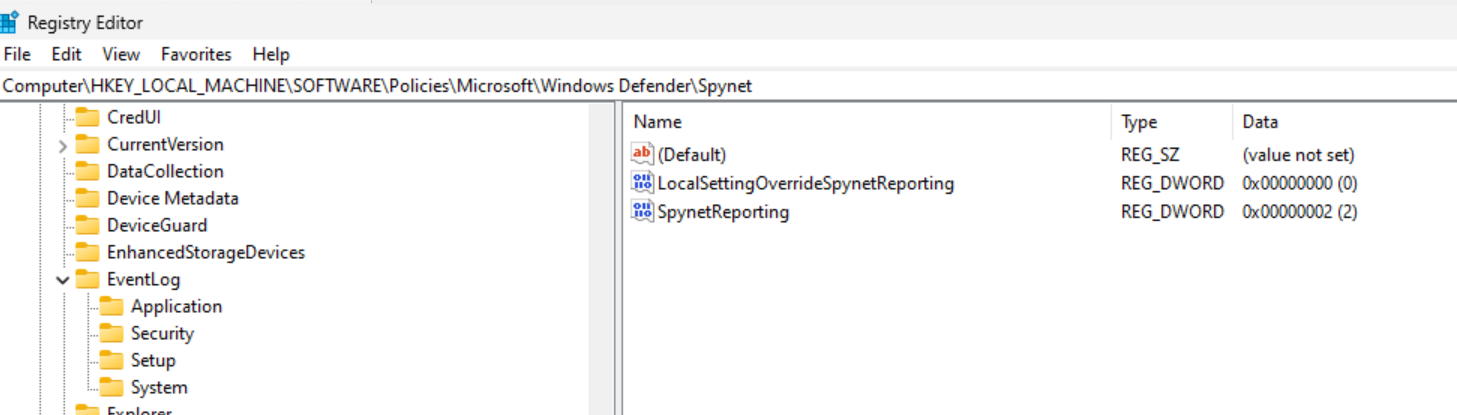
**CONCLUSION:**

No fix required. Appears to be set properly.

**INVESTIGATION:**

The registry key was set to the desired value. We opposed the CIS recommendation because the 2 value allows for better AV protection.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.36.4.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled': [FAILED]"

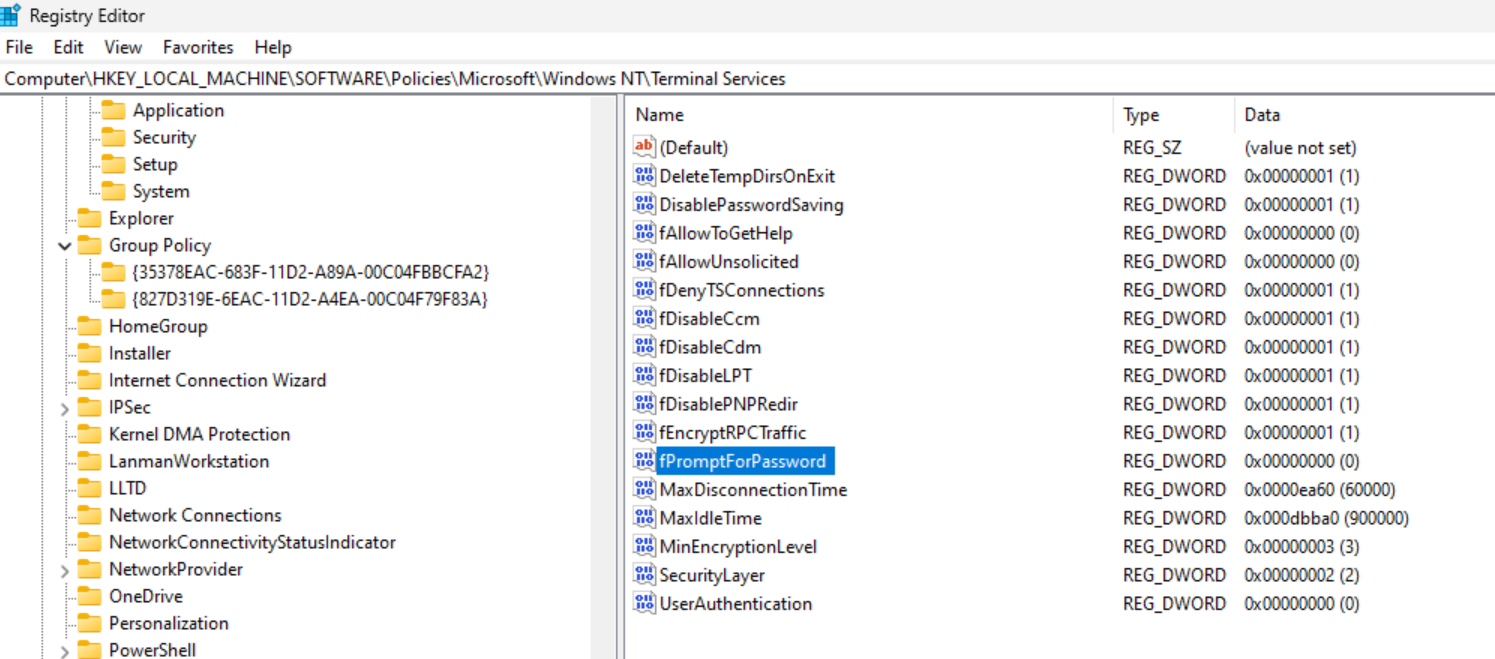
**CONCLUSION:**

Update the configuration to enabled.

**INVESTIGATION:**

The registry key is not set to the CIS recommended setting. This setting was opposed, but I will be swapping this to implemented in the next iteration.

**PROOF:**

****

**AUDIT RESULT:**

"3.11.36.4.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled': [FAILED]"

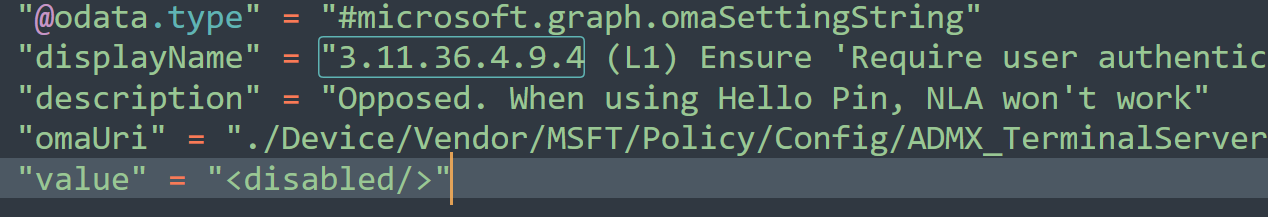
**CONCLUSION:**

No change.

**INVESTIGATION:**

This setting was opposed because NLA breaks authentication in RDP when it is enabled and a user tries to login using “azuread\username”. NOTE: RDP is already disabled by this policy so this will have no effect unless .

**PROOF:**

****

**AUDIT RESULT:**

"3.11.49.1 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

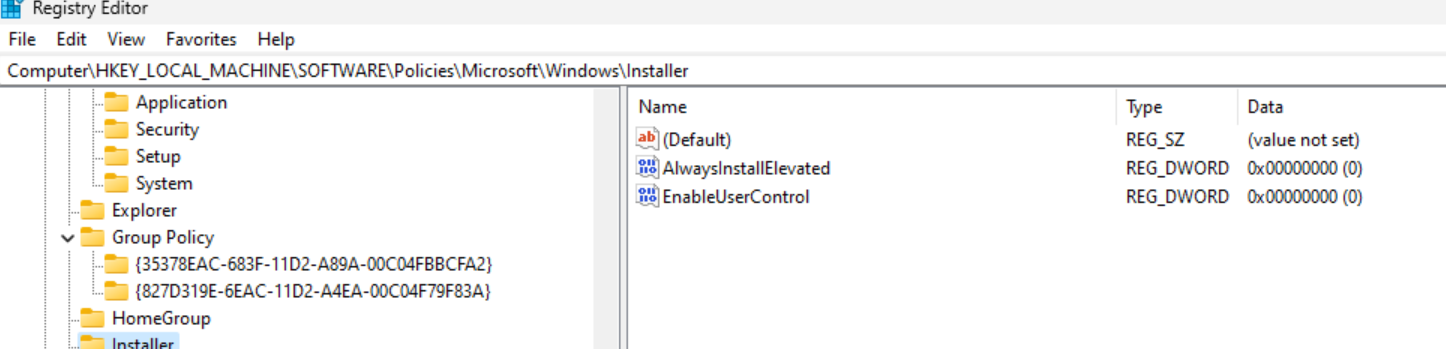
Add new omauri for **./Device/Vendor/MSFT/Policy/Config/ADMX\_MSI/SafeForScripting**

Set to disabled

**INVESTIGATION:**

This setting is missing from the policy. The OMAURI is ./Device/Vendor/MSFT/Policy/Config/ADMX\_MSI/SafeForScripting and will be added.

**PROOF:**

****

**AUDIT RESULT:**

"3.6.17.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled': [FAILED]"

**CONCLUSION:**

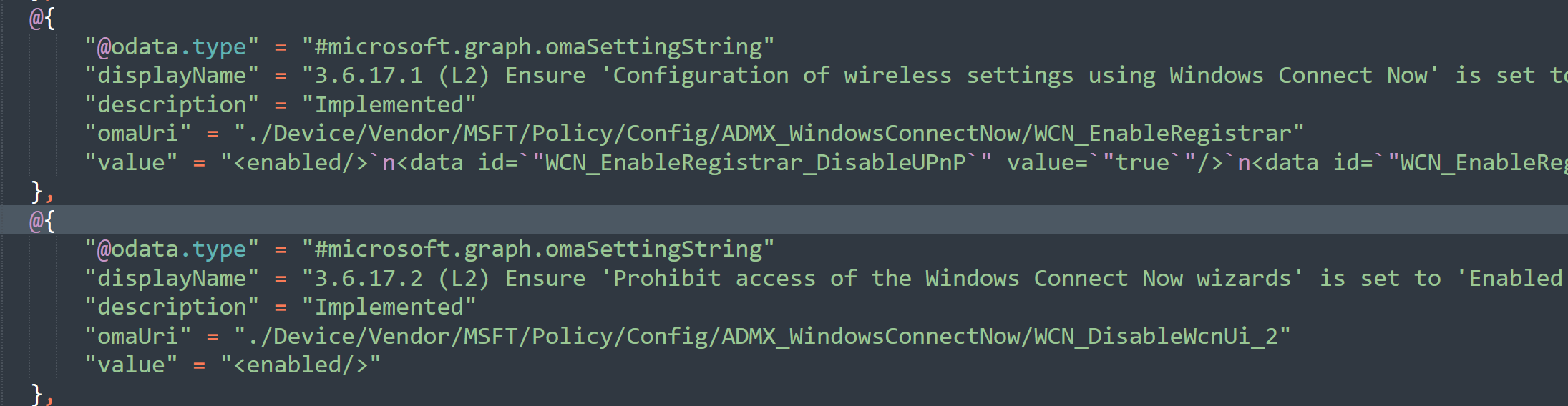
Set OMAURI to Disabled

**INVESTIGATION:**

The configuration is implemented, but it’s a little confusing. The configuration option needs to be set to “disabled” so that all registry entries are set to 0 (per CIS recommendation). When setting to disabled, it sets “DisableUPNPRegistrar” to 0 and other registry entries. This is a bit confusing, but is the recommended configuration.

The OMAURI option will be set to disabled.

**PROOF:**

****

**AUDIT RESULT:**

"3.6.19.1 (L1) Ensure 'Require PIN pairing' is set to 'Enabled': [FAILED]"

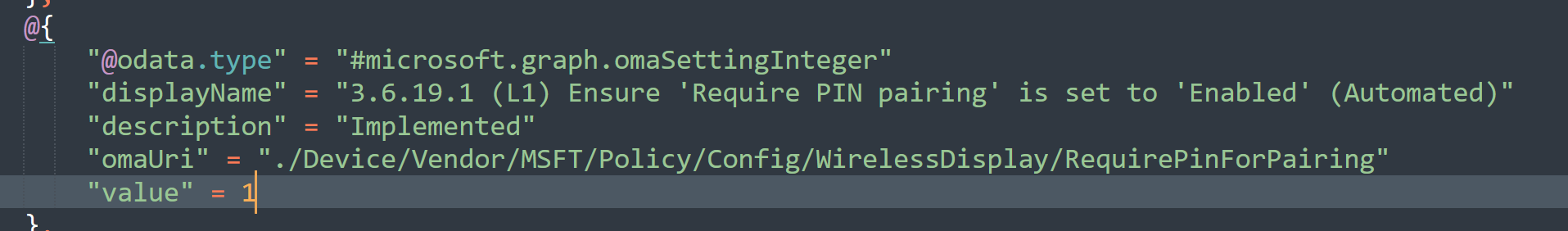
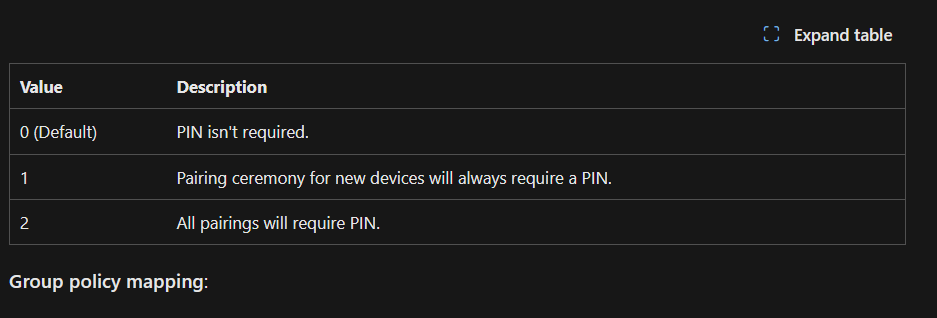
**CONCLUSION:**

Update omauri value to 2

**INVESTIGATION:**

The CIS recommendation is to always require pin pairing. It mentions that the value should be set to “Enabled”. However the OMAURI states that to make pin pairings always require password, the int value should be set to 2, instead. The config will be updated to 2

**PROOF:**

**** ****

**AUDIT RESULT:**

"3.6.9.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled': [FAILED]"

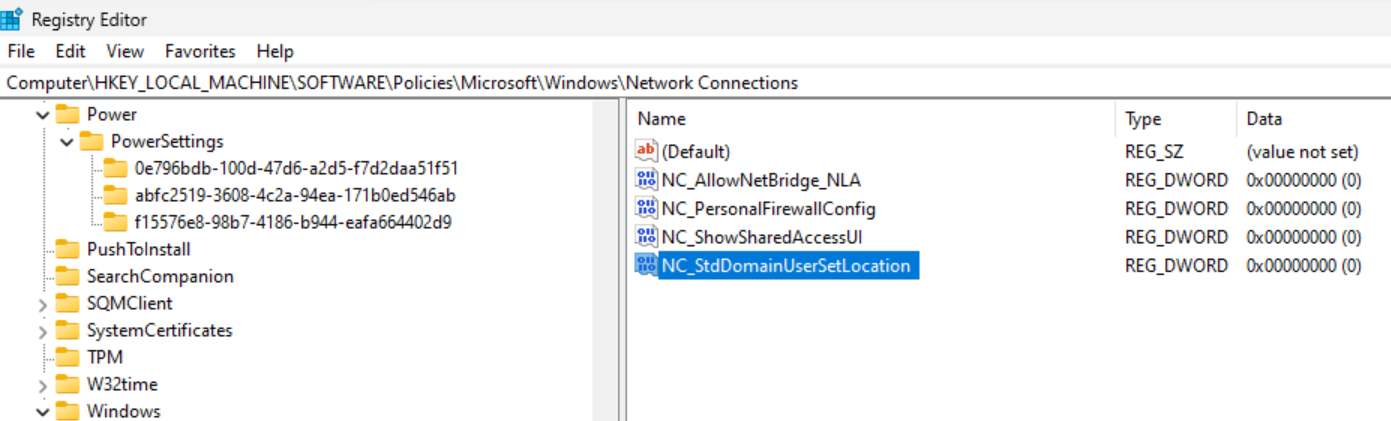
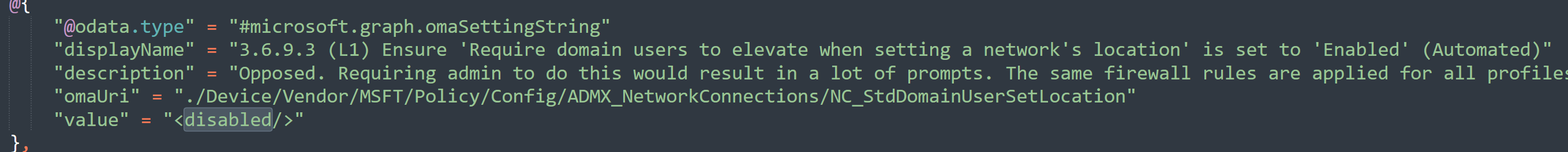
**CONCLUSION:**

Update OMAURI value to enabled

**INVESTIGATION:**

The registry value is not set correctly. The configuration was previously opposed which caused this. The configuration will be changed back to implemented for the next audit since prompting should be disabled and the original reasoning for opposing is no longer valid.

**PROOF:**

**** ****

**AUDIT RESULT:**

"30.4 (L1) Ensure 'Disable Consumer Account State Content' is set to 'Enabled': [FAILED]"

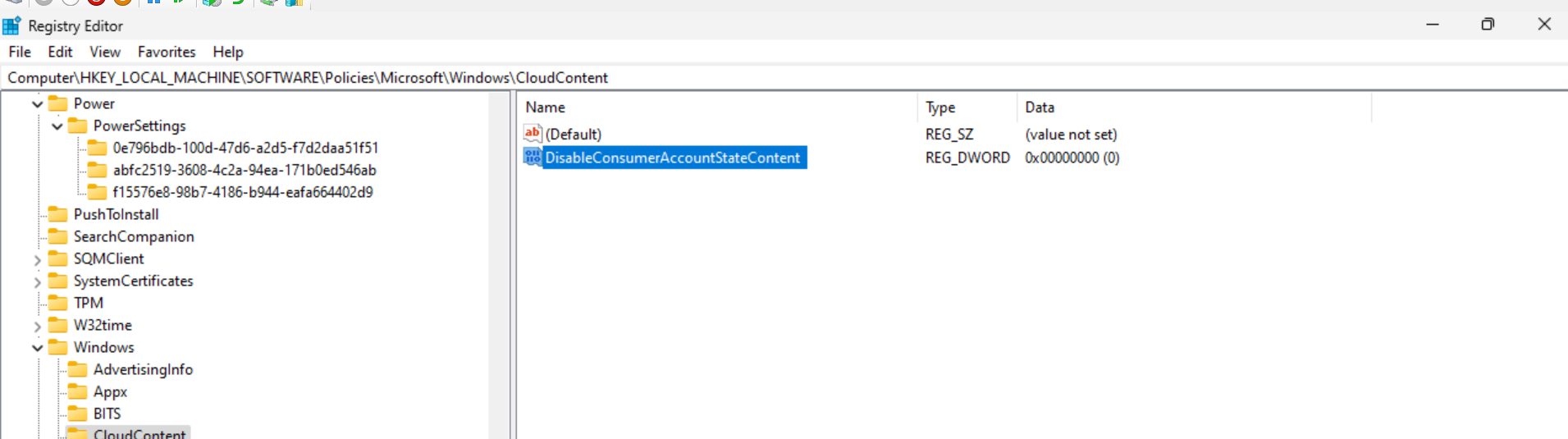
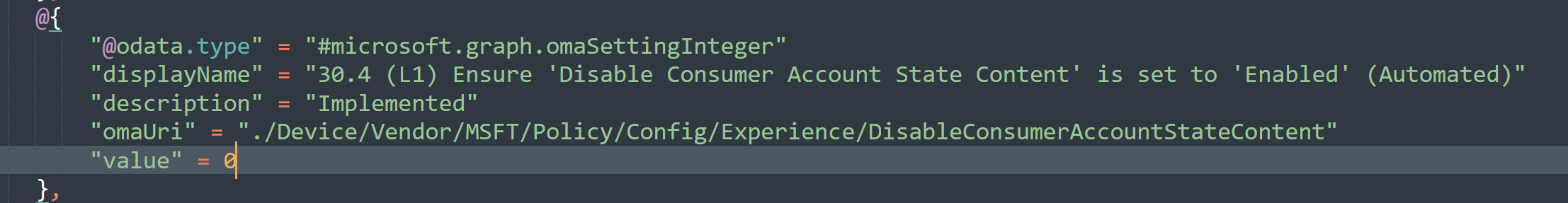
**CONCLUSION:**

Update the OMAURI value to 1.

**INVESTIGATION:**

The registry value is not set to the correct value. In the configuration, the value is set to 0. This should be set to 1.

**PROOF:**

**** ****

**AUDIT RESULT:**

"35.16 (L1) Ensure 'Enable Public Network Firewall: Allow Local Ipsec Policy Merge' is set to 'False': [FAILED]"

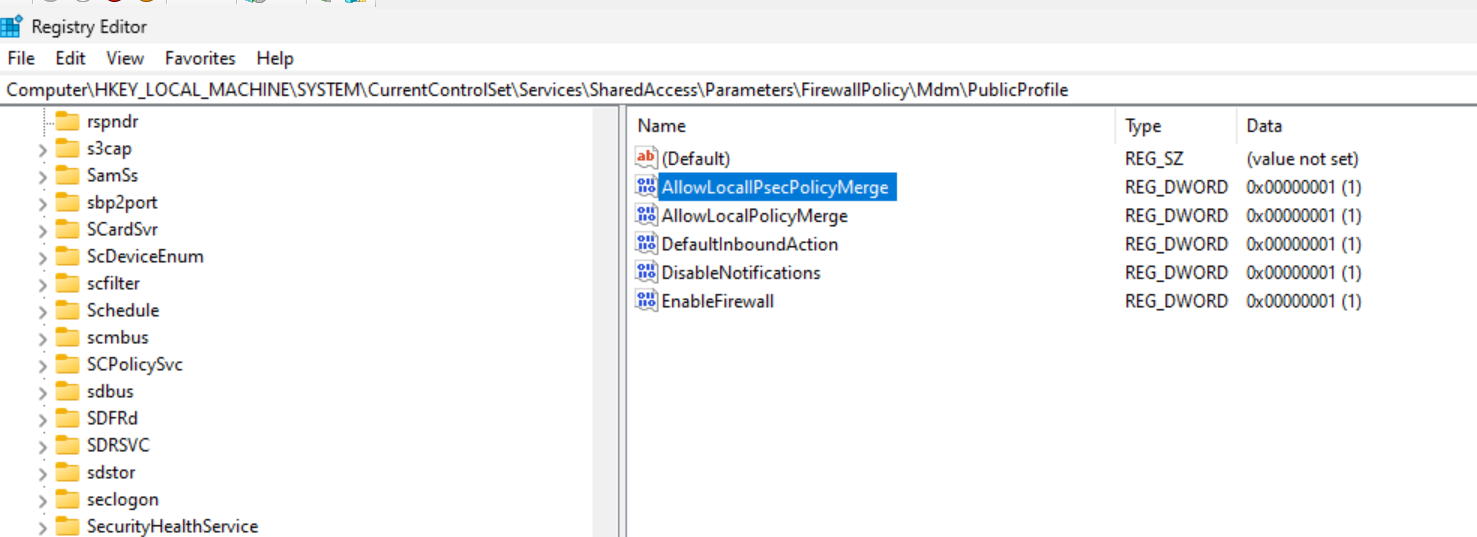
**CONCLUSION:**

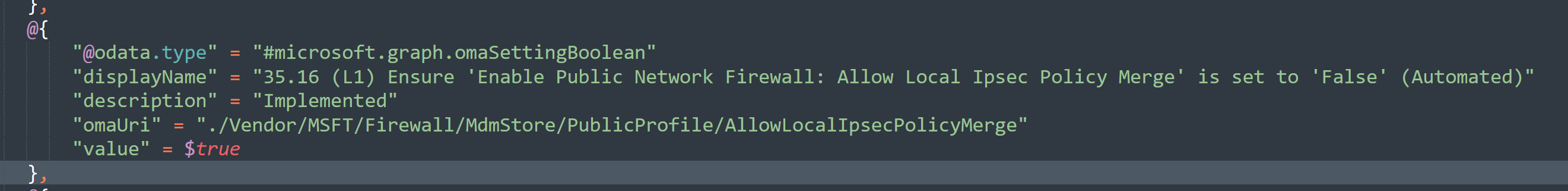
Update OMAURI value to False

**INVESTIGATION:**

The registry value is set to the wrong value. After reviewing configuration, the value is set wrong. The configuration will be updated to false.

**PROOF:**

****

****

**AUDIT RESULT:**

"35.17 (L1) Ensure 'Enable Public Network Firewall: Allow Local Policy Merge' is set to 'False': [FAILED]"

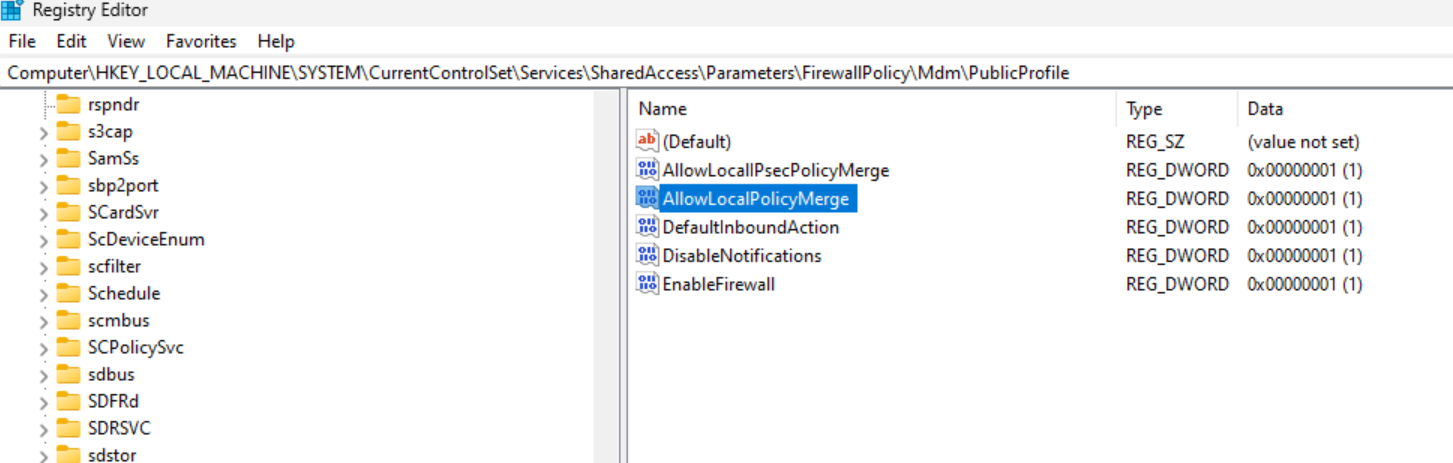
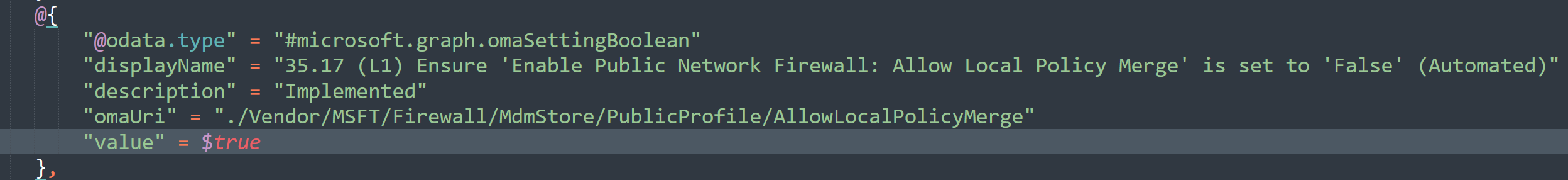
**CONCLUSION:**

Update OMAURI value to False

**INVESTIGATION:**

The registry value is set to the wrong value. After reviewing configuration, the value is set wrong. The configuration will be updated to false.

**PROOF:**

**** 

**AUDIT RESULT:**

"45.30 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests': [FAILED]"

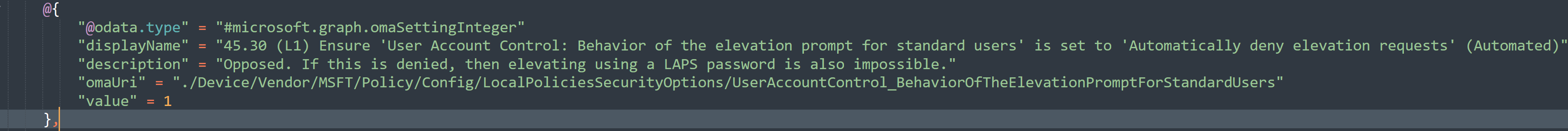
**CONCLUSION:**

No change.

**INVESTIGATION:**

This recommendation has been opposed because if it is enabled, there will be no way to elevate to an admin without logging out of the machine. We prefer that elevating by entering the admin password is allowed and this recommendation has been opposed.

**PROOF:**

****

**AUDIT RESULT:**

"45.7 (L1) Ensure 'Interactive logon: Do not display last signed-in' is set to 'Enabled': [FAILED]"

**CONCLUSION:**

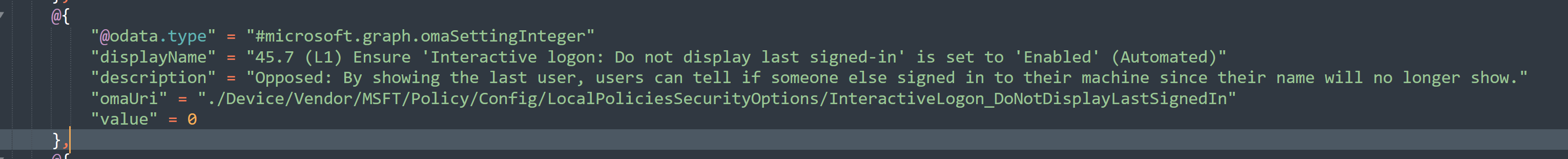
No change.

**INVESTIGATION:**

This recommendation has been opposed for a few different reasons:

1. Users sometimes don’t even know their username
2. If the computer is logged into using another username other than their own, then the username of the previous user will show and not their name, indicating to them that the machine was recently used by someone else. This can serve as a possible IOC and users may contact their admin about the occurrence.
3. Users can identify their own computer when in a large setting by looking at the login screen in case they confuse it with someone elses (prevents them from taking the wrong computer).

**PROOF:**

****

**AUDIT RESULT:**

"45.8 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled': [FAILED]"

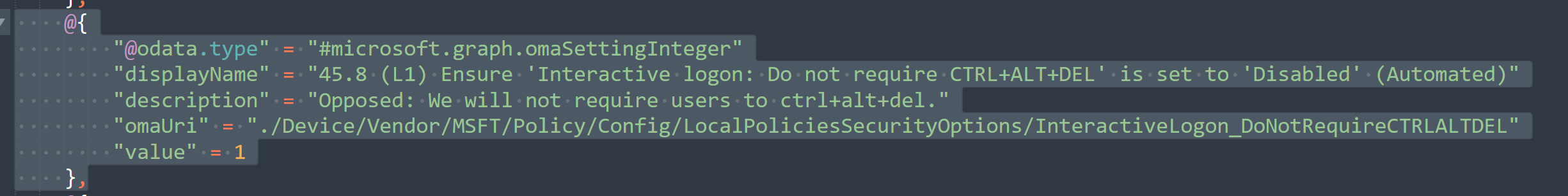
**CONCLUSION:**

No change.

**INVESTIGATION:**

This recommendation has been opposed. Trojans that hijack the login screen is not popular. Requiring ctrl+alt+del is rather annoying for users who are used to simply hitting any key to login. Furthermore, users only have user access and login via Windows Hello. If the password was stolen, it gives the attacker no additional access than they had when the trojan was running in the first place. IE: If the machine is compromised, ctrl+alt+del isn’t going to limit the exposure or allow elevation.

**PROOF:**

****

**AUDIT RESULT:**

"48.3 (L2) Ensure 'Disable Store Originated Apps' is set to 'Enabled': [FAILED]"

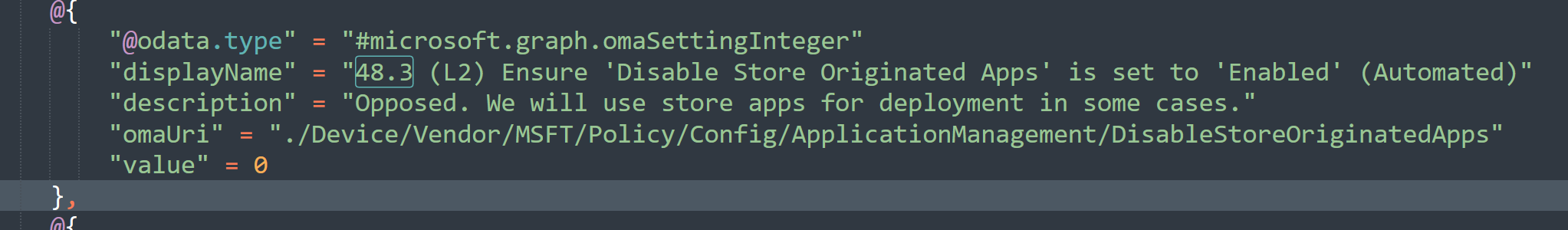
**CONCLUSION:**

No change.

**INVESTIGATION:**

This recommendation has been opposed. Windows store will be used for deployment in some cases. We have a monthly control in place that looks for unknown software installed on all machines that will actively look for malicious store apps.

**PROOF:**

****

**AUDIT RESULT:**

"48.7 (L1) Ensure 'Require Private Store Only' is set to 'Only Private store is enabled': [FAILED]"

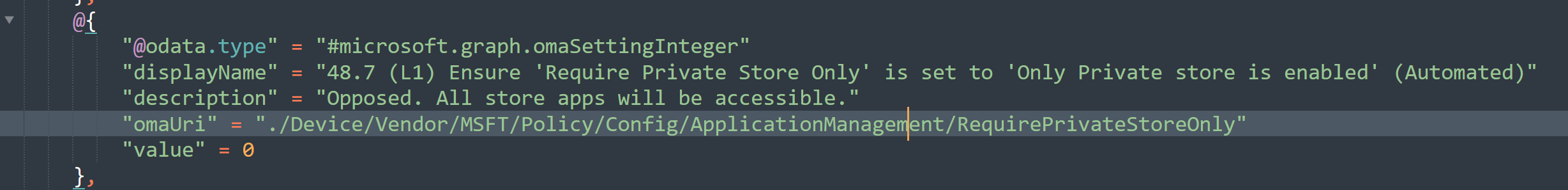
**CONCLUSION:**

No change.

**INVESTIGATION:**

This recommendation has been opposed. We will allow access to Windows Store. It is a better solution than downloading random applications from the web. We have a monthly control in place to audit installed software to ensure nothing malicious is installed.

**PROOF:**

****

**AUDIT RESULT:**

"5.1 (L1) Ensure 'Account Logon Audit Credential Validation' is set to 'Success and Failure': [FAILED]"

**CONCLUSION:**

Add setting for OMAURI: **./Device/Vendor/MSFT/Policy/Config/Audit/AccountLogon\_AuditCredentialValidation**

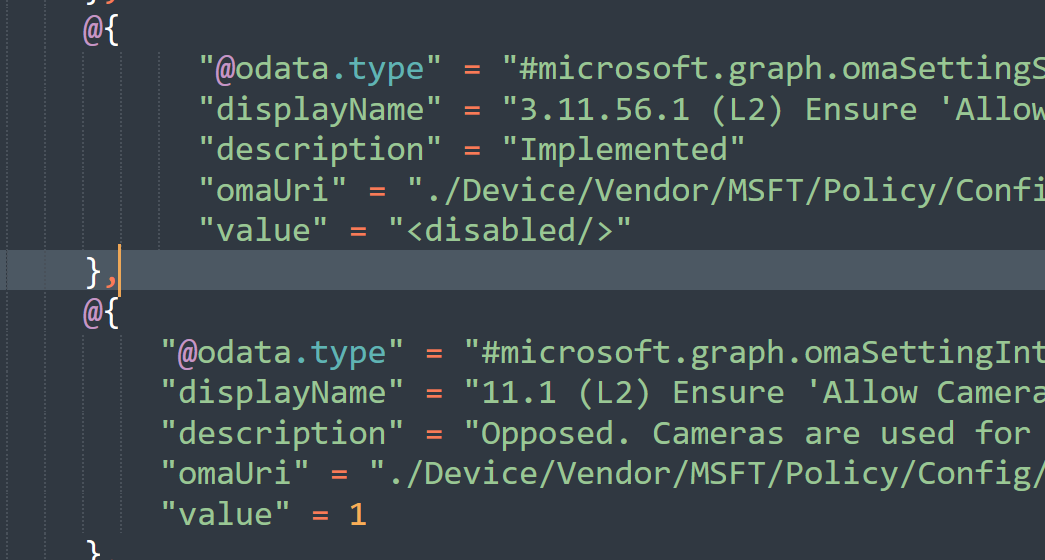
Set to 3

**INVESTIGATION:**

This recommendation was missing from the configuration. It has been added.

**PROOF:**

Nothing after 3.11.56.1

****

**AUDIT RESULT:**

"5.10 (L1) Ensure 'Audit File Share Access' is set to 'Success and Failure': [FAILED]"

**CONCLUSION:**

Add OMAURI for: **./Device/Vendor/MSFT/Policy/Config/Audit/ObjectAccess\_AuditFileShare**set to 3

**INVESTIGATION:**

This recommendation was missing from the configuration. It has been added.

**PROOF:**

See previous