HOW TO MANAGE DEVICES

#htmdcommunity

@htmdcommunity

HTMD Community Conference - 2024

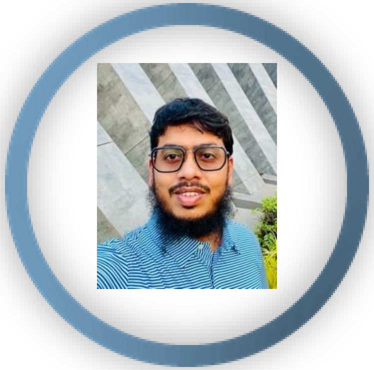
Microsoft

PATCH MY PC

ZERO TOUCH

nerdio

Speakers



Umair Khan

Worked as Support Engineer, Support Escalation Engineer,
Technical Advisor, Beta Engineer roles in Microsoft for ConfigMgr.

@umairMSFT

@TheFrankUK

Vishwas Makkar

Worked as Support Engineer, Support Escalation Engineer,
in Microsoft for ConfigMgr.

Demystifying Windows Update Scan source policies with ConfigMgr

Agenda

- History of the Dual Scan issue (10 mins)
- Introduction of the Windows Scan source policies (5 mins)
- History of the Windows Scan source policies (10 mins)
- Observations in Windows 10 and 11 (10 mins)
- The new Design in 2409 (5 mins)
- Questions (5 mins)

History of the Dual Scan issue

Scenario

You have WSUS or SCCM configured to manage Windows Update in the environment, but you observe that Windows 10 machines are reaching online to get updates including system updates.

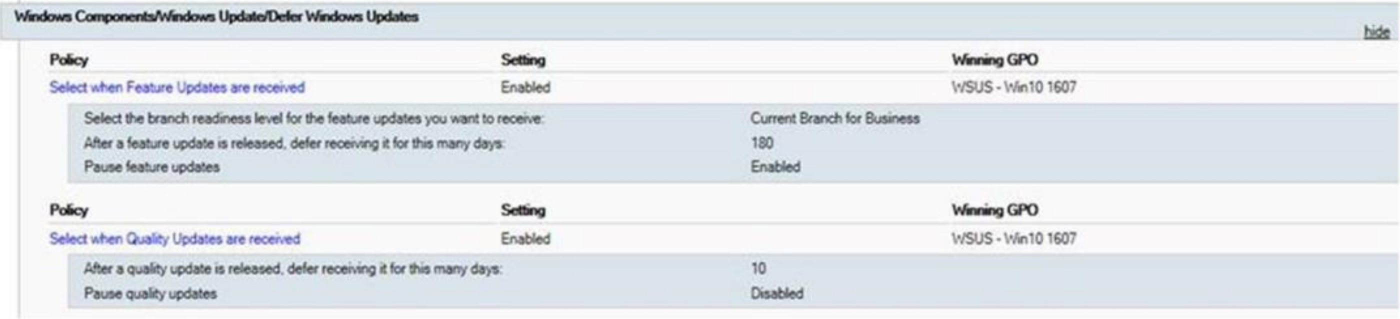
```
[Agent] WSUS server: https://wsus.contoso.com

[Agent] WSUS status server: https://wsus.contoso.com

[DownloadManager] Download manager restoring 0 downloads

[SLS] Making request with URL HTTPS://sls.update.microsoft.com/SLS/{9482F4B4-E343-43B6-B170-9A65BC822C77}/x64/10.0.14393.0/0?CH=448&L=en-US&P=&PT=0x4&WUA=10.0.14393.351
```

Point to note: If you didn't try to scan it against Microsoft Online manually, then why did it try to establish connection with *.update.microsoft.com although WSUS endpoint is in place.

History of the Dual Scan issue

What you need to check

Check the Windows Update Group policies and ensure that none of these policies are configured (Enabled or Disabled).



Windows Components/Windows Update/Defer Windows Updates

hide

Policy	Setting	Winning GPO
Select when Feature Updates are received	Enabled	WSUS - Win10 1607
Select the branch readiness level for the feature updates you want to receive:	Current Branch for Business	
After a feature update is released, defer receiving it for this many days:	180	
Pause feature updates	Enabled	

Policy	Setting	Winning GPO
Select when Quality Updates are received	Enabled	WSUS - Win10 1607
After a quality update is released, defer receiving it for this many days:	10	
Pause quality updates	Disabled	

Ensure that the registry HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate doesn't reflect any of these values.

DeferFeatureUpdate

DeferFeatureUpdatePeriodInDays

DeferQualityUpdate

DeferQualityUpdatePeriodInDays

PauseFeatureUpdate

PauseQualityUpdate

DeferUpgrade

ExcludeWUDriversInQualityUpdate

History of the Dual Scan issue

What just happened here? Aren’t these update or upgrade deferral policies?

Not in a managed environment. These policies are meant for Windows Update for Business (WUfB). Learn more about Windows Update for Business.

Windows Update for Business aka WUfB enables information technology administrators to keep the Windows 10 devices in their organization always up to date with the latest security defenses and Windows features by directly connecting these systems to Windows Update service.

If you are already using an on-prem solution to manage Windows updates/upgrades, using the new WUfB settings will enable your clients to also reach out to Microsoft Update online to fetch update bypassing your WSUS/SCCM end-point.

To manage updates, you have two solutions:

- Use WSUS (or SCCM) and manage how and when you want to deploy updates and upgrades to Windows 10 computers in your environment (in your intranet).

- Use the new WUfB settings to manage how and when you want to deploy updates and upgrades to Windows 10 computers in your environment directly connecting to Windows Update.

So, the moment any one of these policies are configured, even if these are set to be “disabled”, a new behavior known as Dual Scan is invoked in the Windows Update agent.

History of the Dual Scan issue

Older Workaround to prevent Dual Scan to let systems reach the internet:

When Dual Scan is engaged, the following change in client behavior occur:

Whenever Automatic Updates scans for updates against the WSUS or SCCM server, it also scans against Windows Update, or against Microsoft Update if the machine is configured to use Microsoft Update instead of Windows Update. It processes any updates it finds, subject to the deferral/pausing policies mentioned above.

Some Windows Update GPOs that can be configured to better manage the Windows Update agent. I recommend you test them in your environment.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
“DoNotConnectToWindowsUpdateInternetLocations”=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
“NoAutoUpdate”=dword:00000001
“UseWUServer”=dword:00000001
```

In GPO

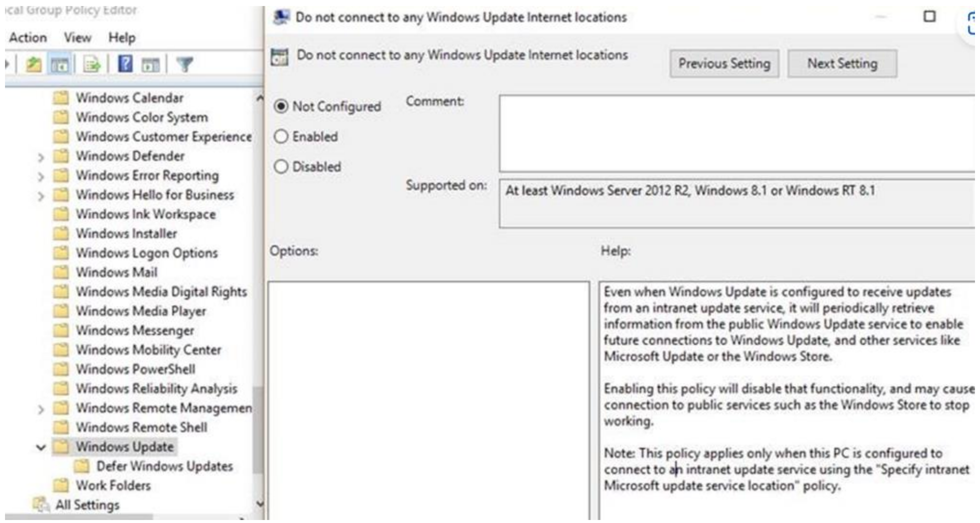
Windows Components/Windows Update

Configure Automatic Updates: Disabled

Do not connect to any Windows Update Internet locations: Enabled

Specify intranet Microsoft update service location: Enabled

WSUS Endpoints



Do not connect to any Windows Update Internet locations

Do not connect to any Windows Update Internet locations

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Options:

Help:

Even when Windows Update is configured to receive updates from an intranet update service, it will periodically retrieve information from the public Windows Update service to enable future connections to Windows Update, and other services like Microsoft Update or the Windows Store.

Enabling this policy will disable that functionality, and may cause connection to public services such as the Windows Store to stop working.

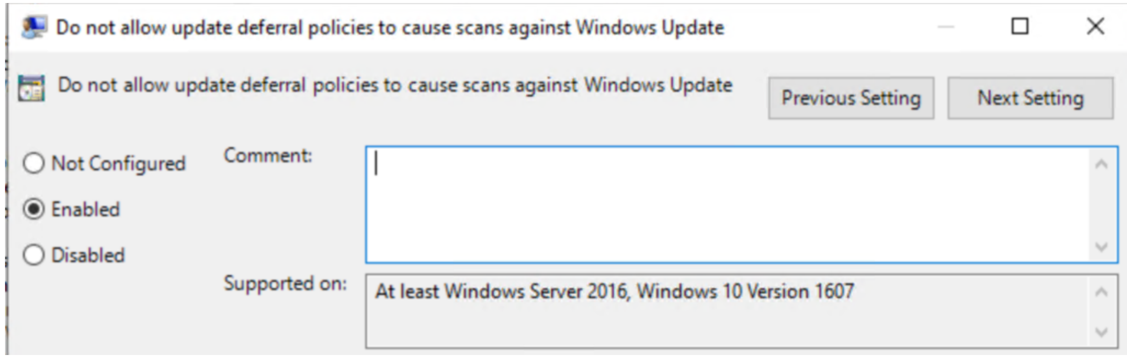
Note: This policy applies only when this PC is configured to connect to an intranet update service using the "Specify intranet Microsoft update service location" policy.

History of the Dual Scan issue

Later Workaround to prevent Dual Scan to let systems reach the internet:

The new policy, "Do not allow update deferral policies to cause scans against Windows Update" , when enabled, will disable Dual Scan. This allows enterprises that wish to configure deferral policies, the ability to do so without being concerned that Dual Scan will override administrator intent.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
“DisableDualScan”=dword:00000001
```



Do not allow update deferral policies to cause scans against Windows Update

Do not allow update deferral policies to cause scans against Windows Update

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10 Version 1607

In GPO

Windows Components/Windows Update

"Do not allow update deferral policies to cause scans against Windows Update“

ConfigMgr started to set this policy to Disable Dual scan when WUFB was disabled or the Software updates were managed by ConfigMgr

Introduction of Windows Scan source policies

- Introduced from Windows 10 2004 and Windows 11 onwards.
- The reason for introduction was simply to give more control in terms of selection of different types of updates from WSUS or Windows Update instead of the binary Dual Scan option with no much control.
- The specify scan source policy enables you to specify whether your device gets the following Windows update types form WSUS or from Windows Update:

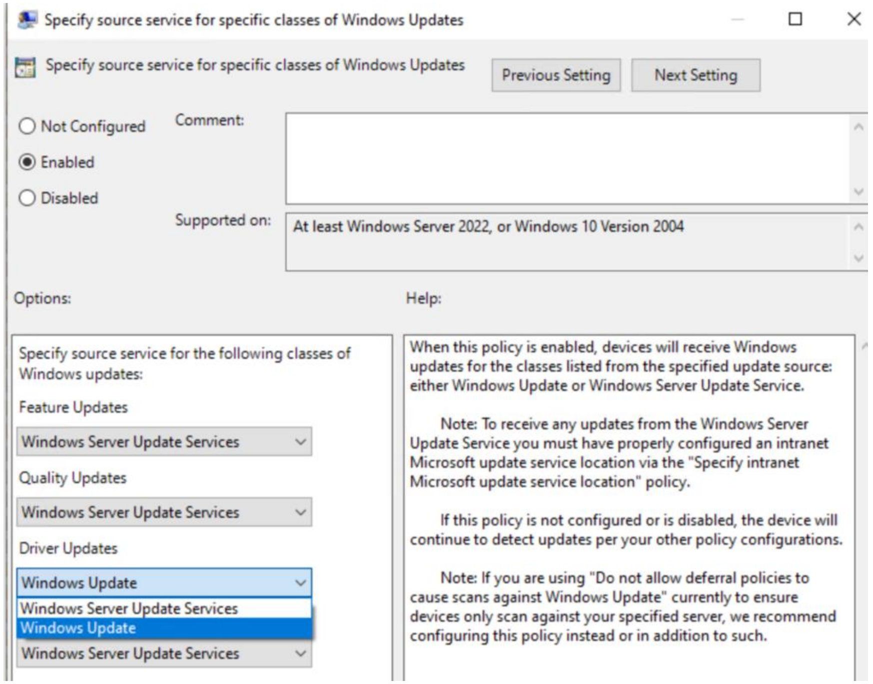
  Quality Updates – Monthly cumulative updates, Defender Platform updates

  Feature Updates – Operating System Upgrades

  Driver Updates - Drivers

  Other Updates – Defender Definition updates, other non-OS updates

- ConfigMgr started setting all these 4 settings to WSUS when the machines where managed by ConfigMgr for Software Updates and started to set it to Windows Update when it found that WuFB was enabled.
- There is a twist to this as to whether these actually applied as we missed to make one more change which actually made these settings to apply. Will see it in the coming slides.



Specify source service for specific classes of Windows Updates

Specify source service for specific classes of Windows Updates

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2022, or Windows 10 Version 2004

Options:

Specify source service for the following classes of Windows updates:

Feature Updates: Windows Server Update Services

Quality Updates: Windows Server Update Services

Driver Updates: Windows Update

Windows Server Update Services

Help:

When this policy is enabled, devices will receive Windows updates for the classes listed from the specified update source: either Windows Update or Windows Server Update Service.

Note: To receive any updates from the Windows Server Update Service you must have properly configured an intranet Microsoft update service location via the "Specify intranet Microsoft update service location" policy.

If this policy is not configured or is disabled, the device will continue to detect updates per your other policy configurations.

Note: If you are using "Do not allow deferral policies to cause scans against Windows Update" currently to ensure devices only scan against your specified server, we recommend configuring this policy instead or in addition to such.

Introduction of Windows Scan source policies

Registries configured by the scan source policies

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

SetPolicyDrivenUpdateSourceForDriverUpdates

SetPolicyDrivenUpdateSourceForFeatureUpdates

SetPolicyDrivenUpdateSourceForOtherUpdates

SetPolicyDrivenUpdateSourceForQualityUpdates
```

Values

1= WSUS

0 = Windows Update (WUMU)

Only applies if

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\UseUpdateClassPolicySource = 1
```

History of Windows Scan source policies – ConfigMgr versions

ConfigMgr 2111 set the SetPolicyDrivenUpdateSourceXXX settings but…

- UseUpdateClassPolicySource was not configured
- Setting were present but had no effect
- Updates, Features on Demand, etc behaved just as they always did. Meaning the user behavior when they clicked to Check for updates online, Installing Feature on Demand from Settings would go to internet as they considered the user's intentional intent.

Configuration Manager 2303 with hotfix KB 25073607

Sets UseUpdateClassPolicySource=1

Effects

- Updates are taken from WSUS only after applying the hotfix.
- Problems Installing Windows Features from internet sources
  - Features on Demand
  - Optional Features
  - Language Packs
- Defender Updates won't install from internet sources

History of Windows Scan source policies – ConfigMgr versions

Configuration Manager 2403 with Hotfix KB28458746

Changes Client Behavior

- Stops setting the policy source registry values
- Values are not removed by CCMEXEC (Client)

Admins can now remove and set the Scan source policy as needed and the settings will 'stick'. Meaning ConfigMgr no longer forcefully configures these Scan source policies.

- Group Policy Objects (GPOs)
- Scripts
- Other methods

Flaws

- This still was not the complete fix as we should not be configuring these policies altogether and the ConfigMgr versions will leave these values to 1 which meant there was a manual fix from above methods needed.
- Looking into other scenarios like getting Third Party Updates from WSUS when WUFB is enabled for all other updates.

Windows 10, Disable Dual Scan and Windows Scan source policies behaviour

- If you set WSUS and no other policies you update from WSUS.
- If you set WSUS and WUfB Deferrals you update from Windows Update. (Dual Scan)
- If you set WSUS + Scan Source Policies + Do not configure disable dual scan policy --> You get updates from whatever scan source is configured to (noting FODs count as Quality Updates)

Example Scenario to illustrate : **A User clicks on the settings to get Optional apps (FOD) in Windows.**

1. WSUS configured + DisableDualScan is 1 + Scan source policy for Quality Updates = WU -> Result failed to get the FOD.
2. WSUS configured + DisableDualScan not configured + Scan source policy for Quality Updates = WU -> Able to get the FOD from WU.
3. WSUS configured + DisableDualScan not configured + Scan source policy for Quality Updates = WSUS -> Failed to get FOD as FODs are not present in WSUS.
4. WSUS configured + DisableDualScan = 0 + Scan source policy for Quality Updates = WSUS -> Failed to get FOD as FOD as not present in WSUS.

Conclusion: Dual Scan is the required switch that controls if Scan source policies work for getting updates from WU in Windows 10.

Summary or Takeaway:

WSUS configured + DisableDualScan is (0/1/not configured) + Scan source policy (not configured) + Repair policy for Windows components (set to Windows Update) -> Able to get the FOD from WU.

Windows 11, Disable Dual Scan and Windows Scan source policies behaviour

- Disable Dual Scan is not applicable to Windows 11. So that simplifies a lot of equation as we only have Scan source policies.

- Disable dual scan is deprecated (no effect)
- If you set only WSUS Policies (UseWUServer , WUServer) -> You will update from WSUS.
- If you set WSUS Policies (UseWUServer , WUServer) and WUfB policies also present (E.g Deferrals) -> You update from WU
- If you set WSUS + Set Scan Source Policies -> You get updates from whatever scan source is configured to.

Million Dollar Question – Simple Solution – ConfigMgr 2409 behavior

WufB disabled (Update Workload managed by ConfigMgr)

WufB disabled (false) ccmexec will

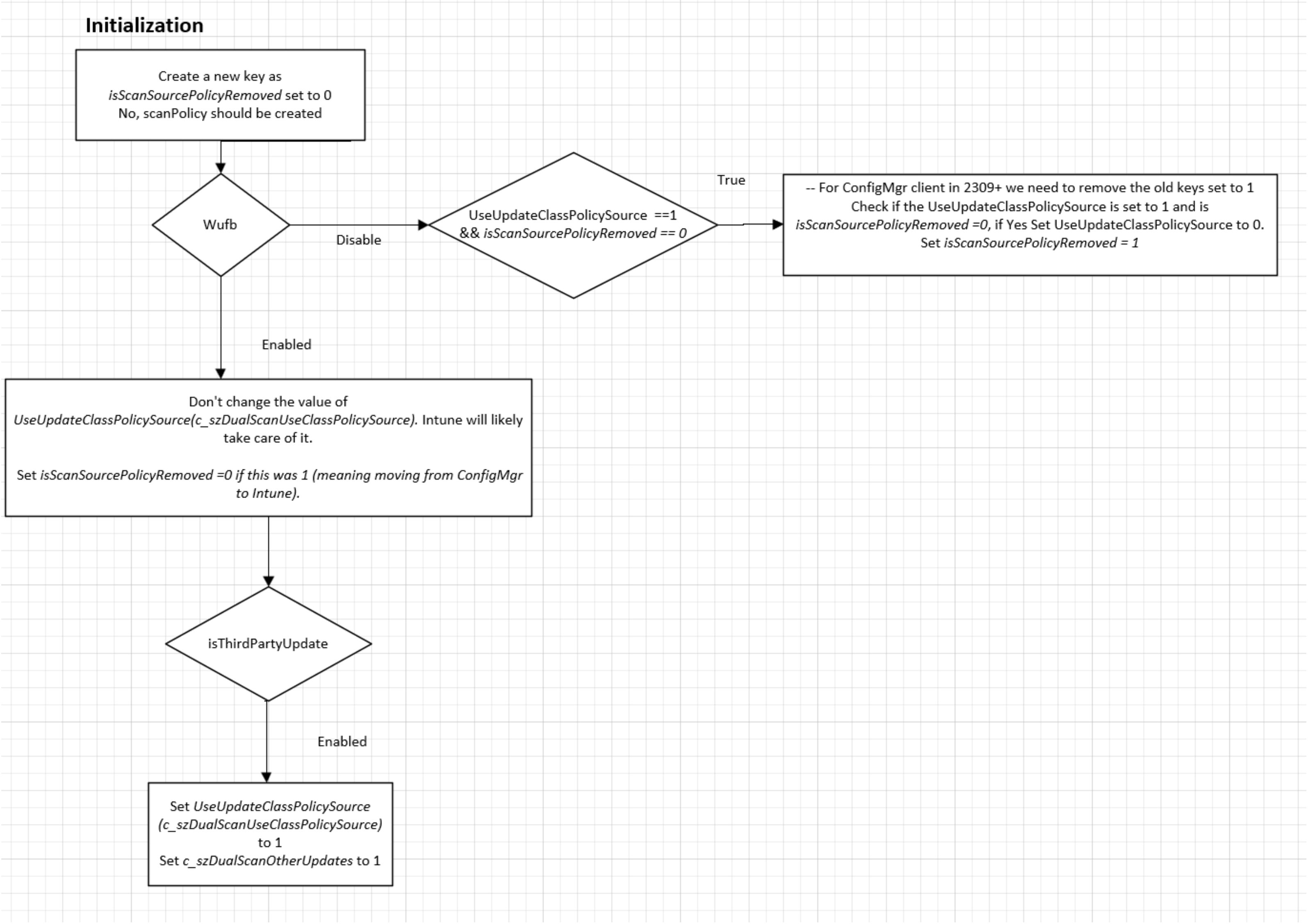
- Set UseUpdateClassPolicySource = 0 once to disable scan source settings
- Set Software\Microsoft\CCM\SoftwareUpdates\isScanSourcePolicyRemoved = 1
- isScanSourcePolicyRemoved stops ccmexec from resetting UseUpdateClassPolicySource each time it starts
- Does not remove the SetPolicyDrivenUpdateSourceForXXX values

WufB enabled (Update Workload managed by Intune)

When WufB is enabled ccmexec will

- Set Software\Microsoft\CCM\SoftwareUpdates\isScanSourcePolicyRemoved = 0
- Check Third-Party Updates status
    - ROOT\CCM\Policy\ActualConfig \CCM_SoftwareUpdatesClientConfig.EnableThirdPartyUpdates
- If Third-Party updates are enabled
    - Set UseUpdateClassPolicySource to 1
    - Set SetPolicyDrivenUpdateSourceForOtherUpdates to 1
- Does not remove the SetPolicyDrivenUpdateSourceForXXX values

Million Dollar Question – Simple Solution – ConfigMgr 2409 behavior



Initialization

Create a new key as *isScanSourcePolicyRemoved* set to 0
No, scanPolicy should be created

Wufb

Disable

UseUpdateClassPolicySource ==1 && *isScanSourcePolicyRemoved == 0*

True

-- For ConfigMgr client in 2309+ we need to remove the old keys set to 1
Check if the UseUpdateClassPolicySource is set to 1 and is *isScanSourcePolicyRemoved =0,* if Yes Set UseUpdateClassPolicySource to 0.
Set *isScanSourcePolicyRemoved = 1*

Enabled

Don't change the value of *UseUpdateClassPolicySource(c_szDualScanUseClassPolicySource).* Intune will likely take care of it.

Set *isScanSourcePolicyRemoved =0 if this was 1 (meaning moving from ConfigMgr to Intune).*

isThirdPartyUpdate

Enabled

Set *UseUpdateClassPolicySource (c_szDualScanUseClassPolicySource)* to 1
Set *c_szDualScanOtherUpdates* to 1

Questions