s

Troubleshooting Steps

Client-Side Script

**Remove** the affected devices from the WSUS MMC console. On each affected system, run once from an elevated (Run as administrator) prompt:

**PowerShell**

Stop-Service -Name BITS, wuauserv -Force

Remove-ItemProperty -Name AccountDomainSid, PingID, SusClientId, SusClientIDValidation -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\ -ErrorAction SilentlyContinue

Remove-Item "$env:SystemRoot\SoftwareDistribution\" -Recurse -Force -ErrorAction SilentlyContinue

Start-Service -Name BITS, wuauserv

wuauclt /resetauthorization /detectnow

(New-Object -ComObject Microsoft.Update.AutoUpdate).DetectNow()

**Command Prompt**

Wait 24-48 hours after running the client-side script to see if the issues have gone away. Normally it is noticeable within an hour, but sometimes it takes longer.

Long Explanation: What is this Doing? Should I be Afraid of Running this?

Background: What is SusClientId and What Symptoms Does Having Duplicate SusClientId Entries have?

Why Should I Remove Affected Devices from the WSUS MMC Console?

****

**Are your WSUS ports open? Is IIS running properly?**

WSUS by default will run on ports 8530/8531 (2012+) and ports 80/443 (2008 and lower). The best thing to do would be to test the connections from an affected client system.

Try to download the WSUS iuident CAB file from the client machine.

http://server.domain.local:8530/selfupdate/iuident.cab  
https://server.domain.local:8531/selfupdate/iuident.cab (if SSL is enabled)

**Then try to browse to:**

http://server.domain.local:8530/ClientWebService/client.asmx  
https://server.domain.local:8531/ClientWebService/client.asmx (if SSL is enabled)

If you can download the cab file and browse to the Client Web Service URL ([using both URLs if you’re using SSL](https://www.ajtek.ca/wsus/client-machines-not-reporting-to-wsus-properly/#Non-SSL-Blocked)), then your ports are open and IIS is functioning properly; continue troubleshooting. If you can’t download the cab file and browse to the Client Web Service URL, check firewall settings (Microsoft and 3rd party firewalls) and port settings.

Z

**Group Policies: Are your policies pointing to the correct place?**

Is the client actually receiving the correct GPO and the correct policies? From an elevated (Run as administrator) Command or PowerShell prompt on an affected client, run the following:

gpresult /h gpo.htm

Open the newly created gpo.htm file (created in the current folder) and verify it’s location URLs (all 3 as noted in [part 4 of my part blog series on How to Setup, Manage, and Maintain WSUS](https://www.ajtek.ca/wsus/how-to-setup-manage-and-maintain-wsus-part-4-creating-your-gpos-for-an-inheritance-setup/).) If the GPOs are pointing to the correct place at the client; continue troubleshooting.



**Is the Windows Firewall enabled?**

Is the Windows Firewall enabled on client? As [noted by Microsoft](https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/windows-update-issues-troubleshooting#issues-related-to-firewall-configuration), some of the errors that you might see in Windows Update logs:

DownloadManager Error 0x800706d9 occurred while downloading update; notifying dependent calls.

Or

[DownloadManager] BITS job {A4AC06DD-D6E6-4420-8720-7407734FDAF2} hit a transient error, updateId = {D053C08A-6250-4C43-A111-56C5198FE142}.200 <NULL>, error = 0x800706D9

Or

DownloadManager [0]12F4.1FE8::09/29/2017-13:45:08.530 [agent]DO job {C6E2F6DC-5B78-4608-B6F1-0678C23614BD} hit a transient error, updateId = 5537BD35-BB74-40B2-A8C3-B696D3C97CBA.201 <NULL>, error = 0x80D0000A

Go to Services.msc and ensure that Windows Firewall Service is enabled. Stopping the service associated with Windows Firewall with Advanced Security isn’t supported by Microsoft. For more information, see [I need to disable Windows Firewall](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc766337(v=ws.10)).

**⎝**

**Is it DNS?**

Especially if you’re using a generic FQDN like wsus.domain.com, you’ll want to make sure your systems are actually resolving the name to the actual IP of the server you’re trying to get the clients to communicate with. Even if it is the FQDN of a specific server, just verify DNS is working from the client side.

From PowerShell:

Resolve-DnsName wsus.domain.local  
Resolve-DnsName server.domain.local

**From Command Prompt:**



Are you using a DNS Alias?

Are you using a DNS CNAME/A record that is not the WSUS fully qualified domain name (FQDN)? An example would be:  
**wsus.domain.com** when the FQDN is **WSUS-01-SEA.domain.local**.

In these instances, you will need to configure the correct SPN records. Microsoft Docs: [Service Principal Names](https://docs.microsoft.com/en-us/windows/win32/ad/service-principal-names)

To see if it is related to the SPN:

setspn -Q HTTP/WSUSServerName.domainame.local

If you find that it has a bad SPN record, you’ll want to delete the bad record. To do that:

setspn -D HTTP/WSUSServerName.domainame.local

To list all of the SPNs for a specific hostname:

setspn -L [Hostname]

If you are using a CNAME for your WSUS SSL Certificate, you must add the appropriate HTTP/CNAME record:

setspn -S HTTP/CNAME.domain.com [Hostname]

setspn -S HOST/CNAME.domain.com [Hostname]

r

**Is the Non-SSL Port Blocked?**

When SSL is enabled on a WSUS system, the port switches to port 8531 (2012+) or port 443 (2008 and lower). Many administrators assume that because WSUS is now responding on the SSL port, that they can now cut the non-SSL port out of the equation and block the HTTP port (8530/80). Unfortunately, that causes problems as WSUS using SSL still will use the HTTP channel for data. Both ports are required to be open when you are using SSL.

s

**Is IPv6 Disabled?**

Many IT administrators like to try to disable things that they don’t use. One of the protocols they disable is IPv6 because they don’t have IPv6 setup on their network and only use IPv4. This is a mistake because ever since Windows 7, IPv6 has been enabled by Microsoft and is used by the client systems to communicate with itself and other services on the system. [Stop hurting yourself by disabling IPv6](https://blogs.technet.microsoft.com/yongrhee/2018/02/28/stop-hurting-yourself-by-disabling-ipv6-why-do-you-really-do-it-2/)!

****

**Do you have any Remote Monitoring & Managing (RMM) Software on your systems?**

If you have RMM software installed, such as SolarWinds RMM, they monitor and solidify the the Windows Update registry keys so that alternative applications cannot change the settings (the RMM software will almost immediately change it back). If you have any of these RMM softwares, disable or uninstall them to verify that they are not the cause of your issues.

**→**

**Verify The Registry**

Verify that: HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer is set to 1.

Use the following PowerShell to pull all the properties and values from the WindowsUpdate registry key and AU key.

Get-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows\WindowsUpdate'

Get-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows\WindowsUpdate\AU'

Use the output to not only inspect the UseWUServer value and make sure it’s set to 1, but also to check for any errors in the URL (which CANNOT HAVE a trailing slash on it).



**Are the GPO Templates Updated?**

As noted in [Part 3 of How to Setup, Manage, and Maintain WSUS](https://www.ajtek.ca/wsus/how-to-setup-manage-and-maintain-wsus-part-3-windows-as-a-service-waas-and-group-policy-administrative-templates/), you will want to get the latest Administrative Templates (.admx/.adml) for Windows which are located at:

<https://docs.microsoft.com/en-US/troubleshoot/windows-client/group-policy/create-and-manage-central-store>

Get the latest one, even if it’s not for the OS you are installing. These are backwards compatible and cumulative meaning that the latest one will have all the updates from each of the preceding admx files. Install these Administrative Templates in your Central PolicyDefinitions folder on your Domain Controller.

This flows into the next point about Scan Sources – you will want to make sure you are specifying the scan source policy.

**ϒ**

**What is the Scan Source of the Windows Update Agent?**

Is WSUS The Default Automatic Update Service? What is the scan source of the Windows Update services? Use the PowerShell below to find out.

$(New-Object -ComObject "Microsoft.Update.ServiceManager").Services | Select-Object Name, IsDefaultAUService

If Windows Server Update Services is not set to True, and your GPOs have the proper settings, you have a dual scan scenario happening. This again flows into the next step.



**Are You Specifying WUfB Policies?**

Are you specifying Windows Update for Business (WUfB) policies?

If you are using WSUS:

DON’T SPECIFY ANY WUFB POLICIES!!!!

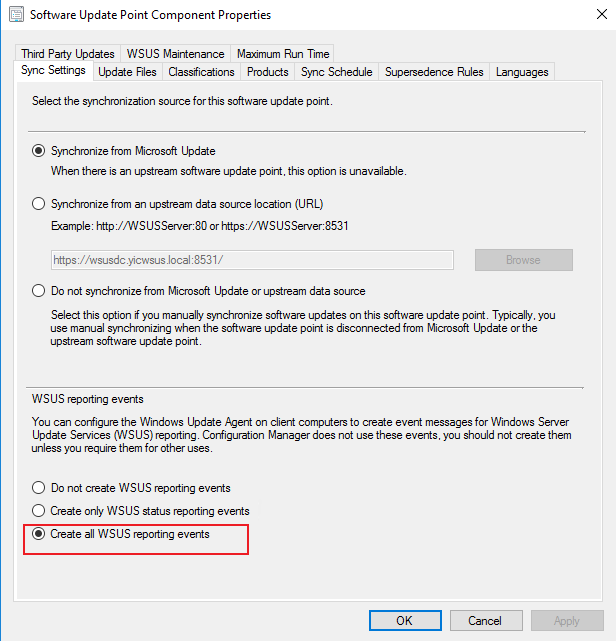
If you have any of them specified, set them all to ‘Not Configured’.

More information is in the article [Dual Scan – Making Sense of Why So Many Admins Have Issues](https://www.ajtek.ca/wsus/dual-scan-making-sense-of-why-so-many-admins-have-issues/).

Do not mistake the Policy “Do not allow update deferral policies to cause scans against Windows Update” (or the associated registry key HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\DisableDualScan) as a fix for this – this too is a WUfB policy.

Are you using Configuration Manager?

Ensure that your Software Update Point Component Properties have it set to “Create all WSUS reporting events”.

[](https://www.ajtek.ca/wp-content/uploads/2021/06/SUP_Properties.png)

****

Is WSUS in a Healthy State?

The easiest way to check if WSUS is in a healthy state is by using Microsoft’s utility to check the health of your WSUS server and then review the event viewer Application Event logs to confirm everything is healthy.  
& "$env:ProgramFiles\Update Services\Tools\WsusUtil.exe" checkhealth  
If it is not in a healthy state, you should investigate and fix these isssues. If in the Application Event Log there is an error from Windows Server Update Services, event ID 12002, saying *“The Reporting Web Service is not working.”*, you may need to restart the WSUS Administration site in IIS and verify again that *“The Reporting Web Service is working correctly.”* Sometimes even a restart of the server is not enough.



Is the WSUS server missing required files?

The easiest way to fix this (you can’t easily tell without doing wireshark captures) is to run a WsusUtil Reset which will go through all files, confirm they are not corrupted and missing, and ONLY download or re-download missing or corrupted files from Microsoft.  
& "$env:ProgramFiles\Update Services\Tools\WsusUtil.exe" Reset  
Unfortunately, you can’t tell how much progress has been completed, or what has been done, or when this is finished. It is best to assume it is going to take a full 24 hours (longer if it has to download a lot of data and you have a slow connection).

It’s my WSUS server!

It may be your WSUS server that’s the problem. Clients request updates and cause the WSUS server to communicate back and forth and compare the updates that are already installed on the client system with what updates are available within WSUS. The available updates include all of the updates excluding declined updates that the server knows about. When you’re not doing the proper maintenance on the WSUS server, the comparative lists grow big and can time out the server’s connection. Due to this timeout, reporting back to the server can be affected. By performing the proper maintenance on the WSUS server, you effectively reduce the amount of data that needs to be compared against thereby making the time shorter and the client able to respond to the request. [Part 8 of my blog series on How to Setup, Manage, and Maintain WSUS](https://www.ajtek.ca/wsus/how-to-setup-manage-and-maintain-wsus-part-8-wsus-server-maintenance/) explains what should be done on a regular basis to maintain your WSUS instance. Alternatively, you can simply [WAM your server](https://www.ajtek.ca/wam/features/) ® and you won’t need to worry about WSUS maintenance anymore.