Patch Tuesday Will Never Be the Same: Windows as a Service

Mark Minasi mark@minasi.com, @mminasi twitter
www.minasi.com
newsletter at www.minasi.com

Windows 10 is Different

- About every nine months, Microsoft releases a new Windows 10
- You have about a year to install it (that's a simplification), or you stop getting security patches
- Every month, you don't get patches, you get one big patch that contains patches
- Even if you haven't patched in months, you get one big patch
  - That's nice, as doing a fully patched system from an ISO is faster and easier
- Once your system sees a patch, it'll install it in 30 days whether you want it to or not
  - That's not nice, as many admins like to stop or delay particular patches
- For many people, *Windows* patching (not Office patching) might best be handled with a set of group policy settings rather than WSUS

One or Two New Win 10s a year

- Basically Microsoft will release a new version – new "feature update" -- of Windows 10 about every nine months on average
- They're like the old Service Packs with a few new features
- New one out now: "Creator's Update, "RS2" or "1703" is the fourth
- **MS will only support – provide patches for --the two latest versions**
- The third latest stops getting security patches
- You can control how quickly you must adopt a "feature update"
- Two "branches," CB and CBB exist; CBB lets you put off upgrades a little
- These are the basics – we'll get more precise later on

How Do I Get the Patches and Features?

- Like Config Manager? Keep using it, it's slowly getting more Win 10-aware, so keep up on *its* newly-sped-up pace of change
- If you use WSUS, it seems to be moving to non-Windows patches
- For the rest of us, the non-CM answer seems to be controlling the Windows Update ("WU") client via a bunch of new GPO settings
- Those GPs are collectively called "Windows Update for Business" (WUfB)

How Windows 10 Patches Work

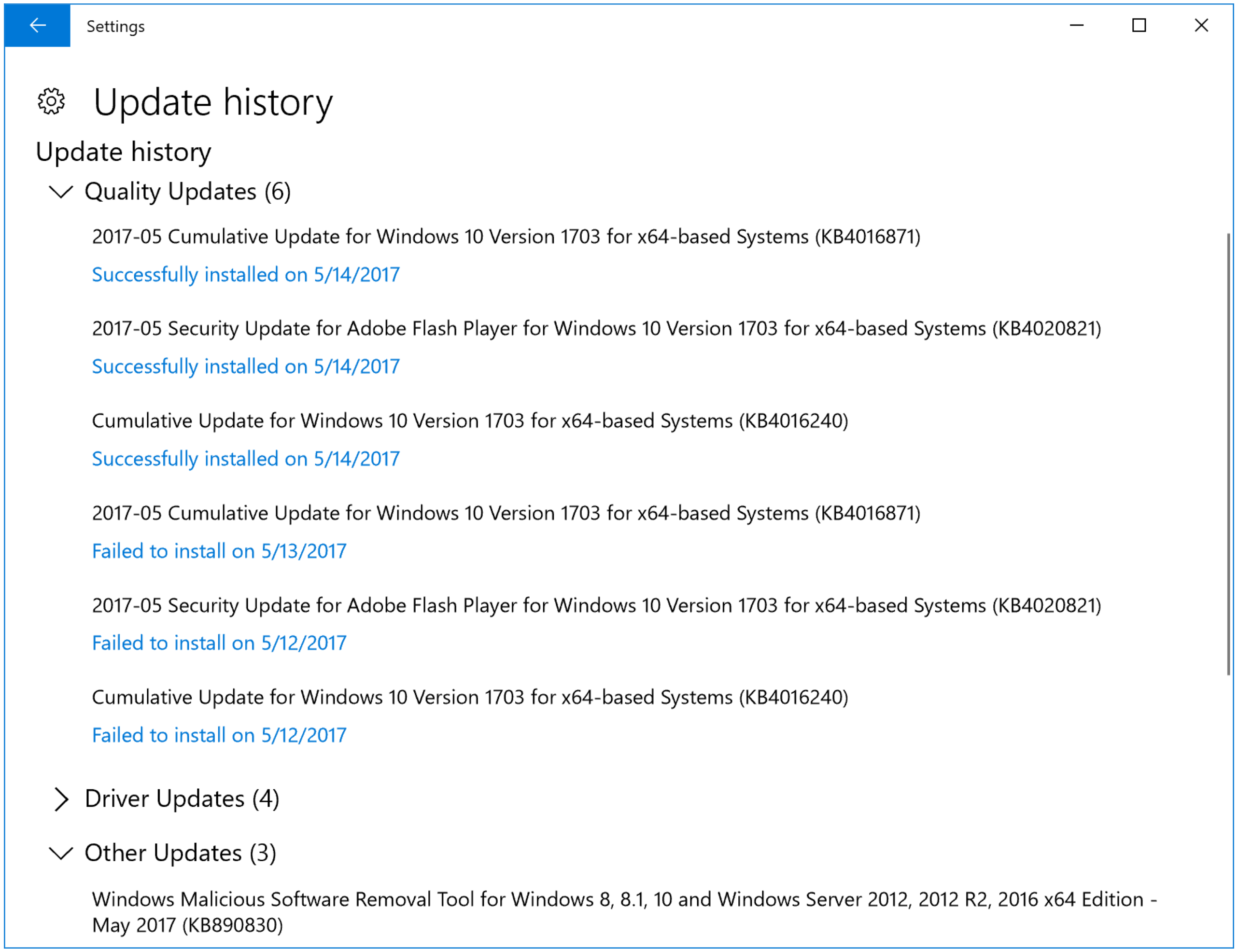
- Imagine installing a new Win 7 SP1 from the DVD/ISO, going to update it, and then getting just one big patch and one reboot
- The idea is that basically Microsoft maintains
  - The one big "Cumulative quality update," a sort of "superpatch" from the initial release of 1703 (the fourth Win 10, remember?) or whatever
  - Then when your WU client contacts the WU server for updates, the WU server creates a "delta superpatch" with all of this month's patches in it, and your system installs that
- Nice side-effect: Installing the delta each month cleans out the old junk so your C: drive doesn't grow forever

More Patches Than Just Cumulatives, though

- Not everything goes into the cumulative "superpatches"
- WU also does things like Adobe fixes or not-exactly-Windows things like the malicious software removal tool or Defender updates or drivers
- So you'll see updates classified as
  - Quality
  - Driver
  - Other

Quality updates:

- Standard security patches and bug fixes



Update history

Update history

Quality Updates (6)

2017-05 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016871)
Successfully installed on 5/14/2017

2017-05 Security Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4020821)
Successfully installed on 5/14/2017

Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016240)
Successfully installed on 5/14/2017

2017-05 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016871)
Failed to install on 5/13/2017

2017-05 Security Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4020821)
Failed to install on 5/12/2017

Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016240)
Failed to install on 5/12/2017

Driver Updates (4)

Other Updates (3)

Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - May 2017 (KB890830)

Driver updates: just what it says.

Quality updates:

- "Other:" things like Defender updates

Sidebar: Windows 7

- In the process of doing this "superpatch" thing Microsoft seems to be thinking about back-porting this to Windows 7
- In *any* case, any time you install Win 7 and are starting the painful patching, immediately install the "Updated Windows Update client for Windows 7"
- Greatly speeds up the ISO-to-done time
- Not as well as Win 10 does, but it's faster than normal Win 7 installs, and I suspect they will continue to improve the Win 7 WU client

So What Exactly is Windows as a Service?

- The notion that
  - Windows changes faster than before
  - New features appear more commonly
  - Windows is "never completed, always improved"
  - And that patching is less optional
- Are all parts of a programming notion called "agile" that tells programmers to use those ideas to constantly improve their software
- Microsoft's cloud products all have "as a Service" at the end of their names, so Windows got it even though it's not a cloud thing

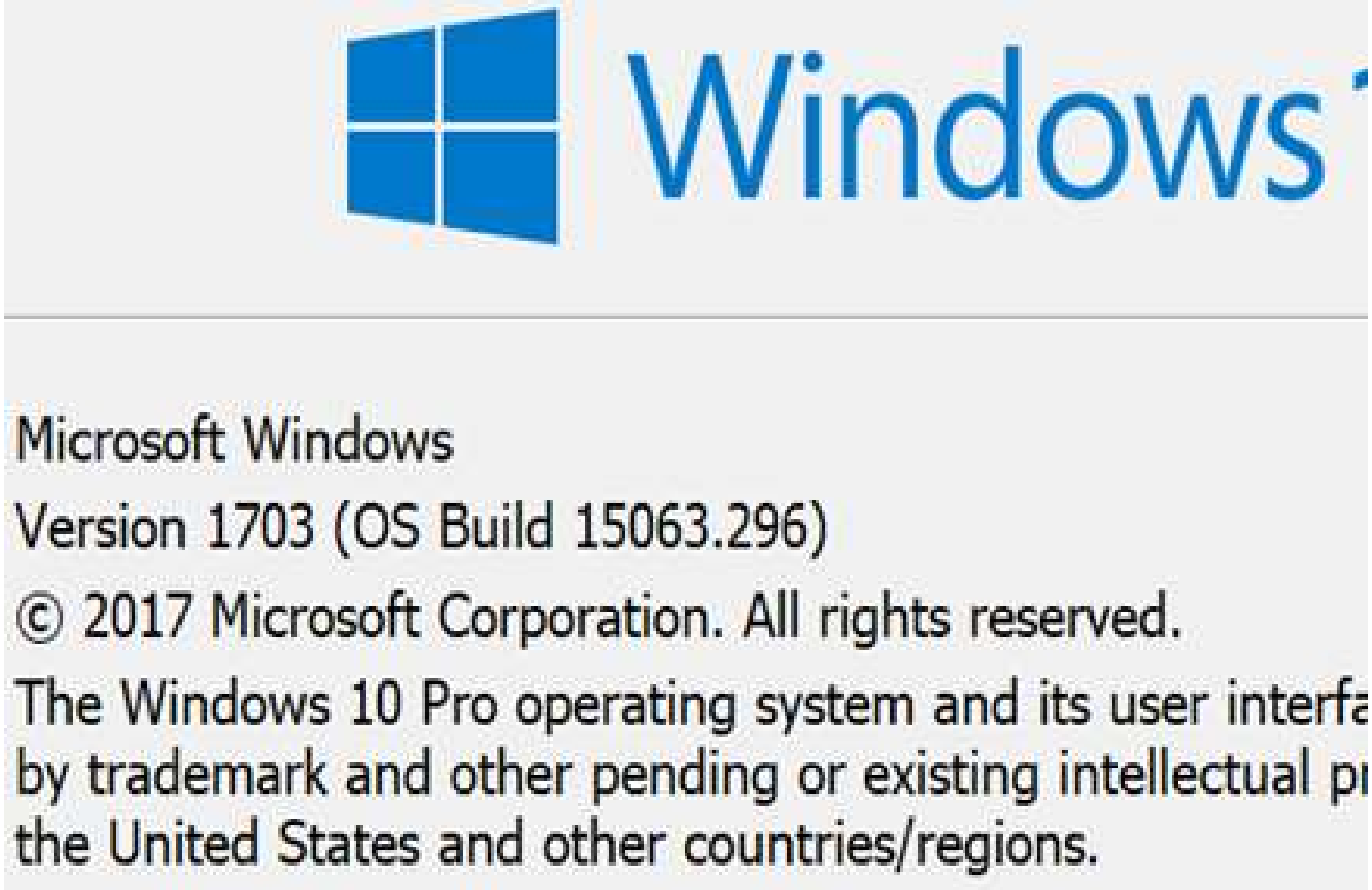
WaaS Terms

- Update: Patch or bug fix – things we just met. More recently called a "Quality Update" sometimes
- Upgrade: a new version of Windows 10, delivered via WU, like Creators Update. Also "Feature Update" in in Group Policies
- Branch: Upgrades are tested by different groups of users called "Branches." Early branches see rough, buggy code. Users like you and me see later branches, and more on this soon. You'll hear of branches named CB, CBB and LTSB.
- Ring: a subset of a branch. NB that Sometimes "branch" means "ring"
- Flight: a release of new code. In the process of creating a new "upgrade" of Windows, Microsoft releases dozens of flights that are unfinished, "test" versions before the final flight for that upgrade

"10" Means Nothing; Version and Build are What You Need

In this capture of the "Winver" command, you see first the "version" number, 1703, and then the "build" number, 15063.296

The version number is just the date that the version appeared in YYMM format – a 2017 build appearing in March, the third month, is then "1703"



Microsoft Windows

Version 1703 (OS Build 15063.296)

© 2017 Microsoft Corporation. All rights reserved.

The Windows 10 Pro operating system and its user interfa
by trademark and other pending or existing intellectual pr
the United States and other countries/regions.

People Call Releases By Different Names

Name	Version Number	Build Number	Beta name
Windows 10 RTM	1507	10240	Threshold
November Update	1511	10586.916	Threshold 2
Anniversary Edition	1607	14393.1198	Redstone
Creators Update	1703		Redstone 2

This table changes regularly in a blog; google "Windows 10 release information" to see it

The left-of-the decimal part of the build numbers shouldn't change, and the part right of the decimal *will* change with every released patch

REFERENCE: Getting the Build Number

lots of ways to do it…

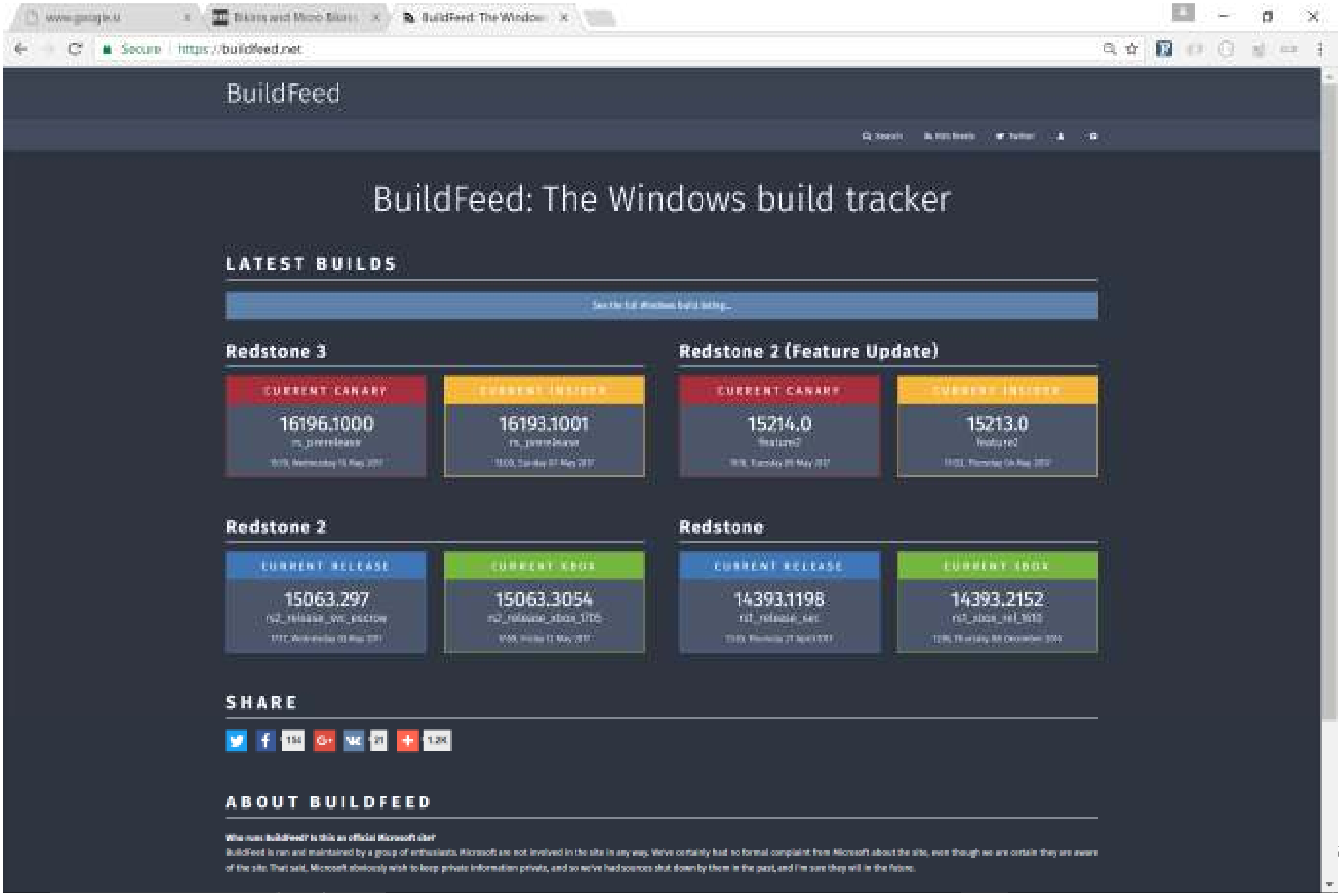
- (get-ciminstance win32_operatingSystem). version
- (gwmi win32_operatingsystem).version
- (get-itemproperty "hklm:\software\microsoft\windows nt\CurrentVersion").Currentbuildnumber
- Get-WindowsEdition -online (gets Enterprise vs Pro vs Home)
- DISM /online /get-currentedition
- ver
- Notice that getting the actual *version* number (e.g. 1511) seems a mite tougher than getting the build number in many cases

"New Windows All the Time? No, No, No!"

- Well, Windows 7 support doesn't stop until January 2020
- There is a somewhat-less-desirable version called the Long Term Servicing Branch or LTSB; I'll get to it
- In truth Microsoft hasn't really kicked anyone off the two-year-old 1507 as I write this slide in mid-2017, so maybe they're listening… we'll see

Flights And Rings: Seeing the Future

- Microsoft fixes bugs and creates new features daily on the road to something worth releasing to the world
- These daily test versions are called "builds" and there are literally thousands of them leading to each "update" release
- Most go nowhere beyond internal Microsoft testing, but some are released or leak out as "flights"
- Builds are created by "labs" with names like "th2_release"
- You can search on particular labs at buildfeed.net to see their builds
- The "flights" are designated them "low" or "high" ("medium" seems to have disappeared)
- "High" flights tend not to leave Redmond, "low" ones become more publicly-available



BuildFeed

BuildFeed: The Windows build tracker

LATEST BUILDS

See the full Windows build listing...

Redstone 3

CURRENT CANARY	CURRENT INSIDER
16196.1000 rs_prerelease 10:15, Wednesday 10 May 2017	16193.1001 rs_prerelease 13:00, Sunday 07 May 2017

Redstone 2 (Feature Update)

CURRENT CANARY	CURRENT INSIDER
15214.0 feature2 19:18, Tuesday 09 May 2017	15213.0 feature2 11:02, Thursday 04 May 2017

Redstone 2

CURRENT RELEASE	CURRENT XBOX
15063.297 rs2_release_svc_escrow 17:17, Wednesday 03 May 2017	15063.3054 rs2_release_xbox_1705 9:59, Friday 12 May 2017

Redstone

CURRENT RELEASE	CURRENT XBOX
14393.1198 rs1_release_sec 13:09, Thursday 27 April 2017	14393.2152 rs1_xbox_rel_1610 12:16, Thursday 08 December 2016

SHARE

ABOUT BUILDFEED

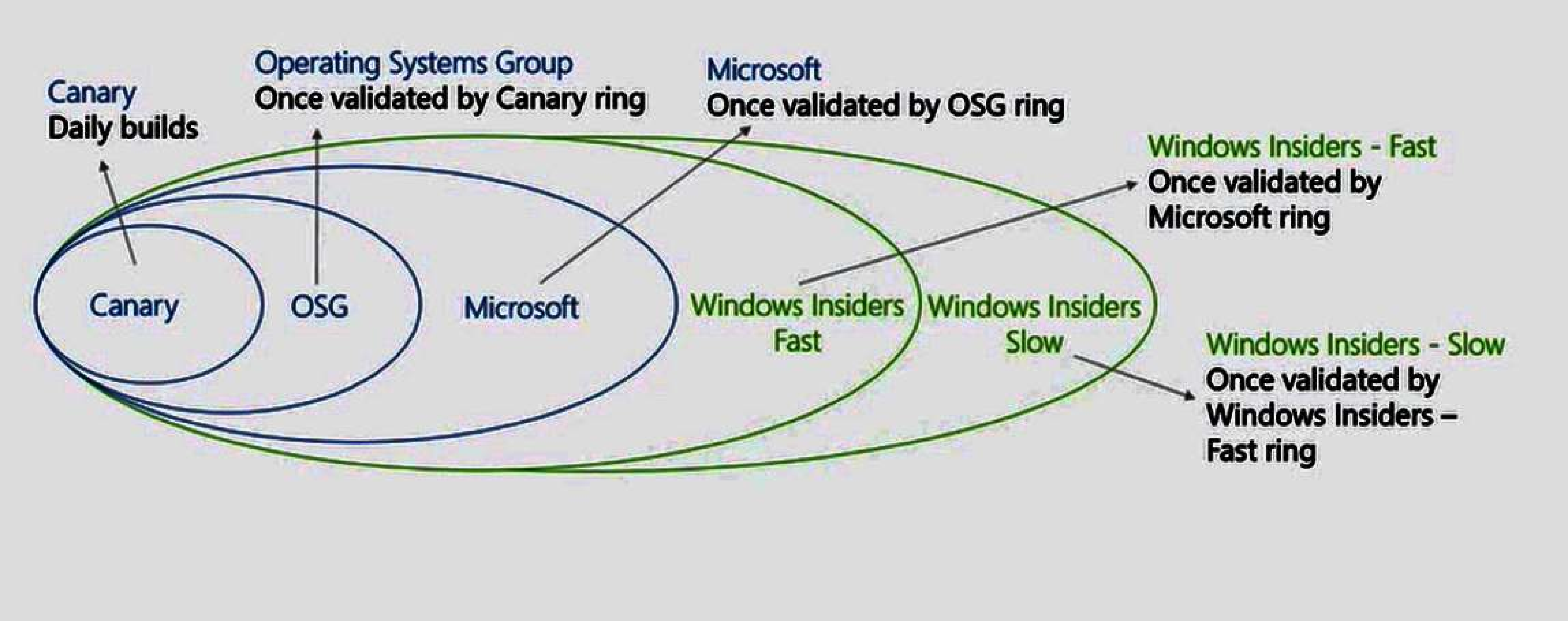
Who runs BuildFeed? Is this an official Microsoft site?

BuildFeed is ran and maintained by a group of enthusiasts. Microsoft are not involved in the site in any way. We've certainly had no formal complaint from Microsoft about the site, even though we are certain they are aware of the site. That said, Microsoft obviously wish to keep private information private, and so we've had sources shut down by them in the past, and I'm sure they will in the future.

From Idea to Product: Branches and Rings

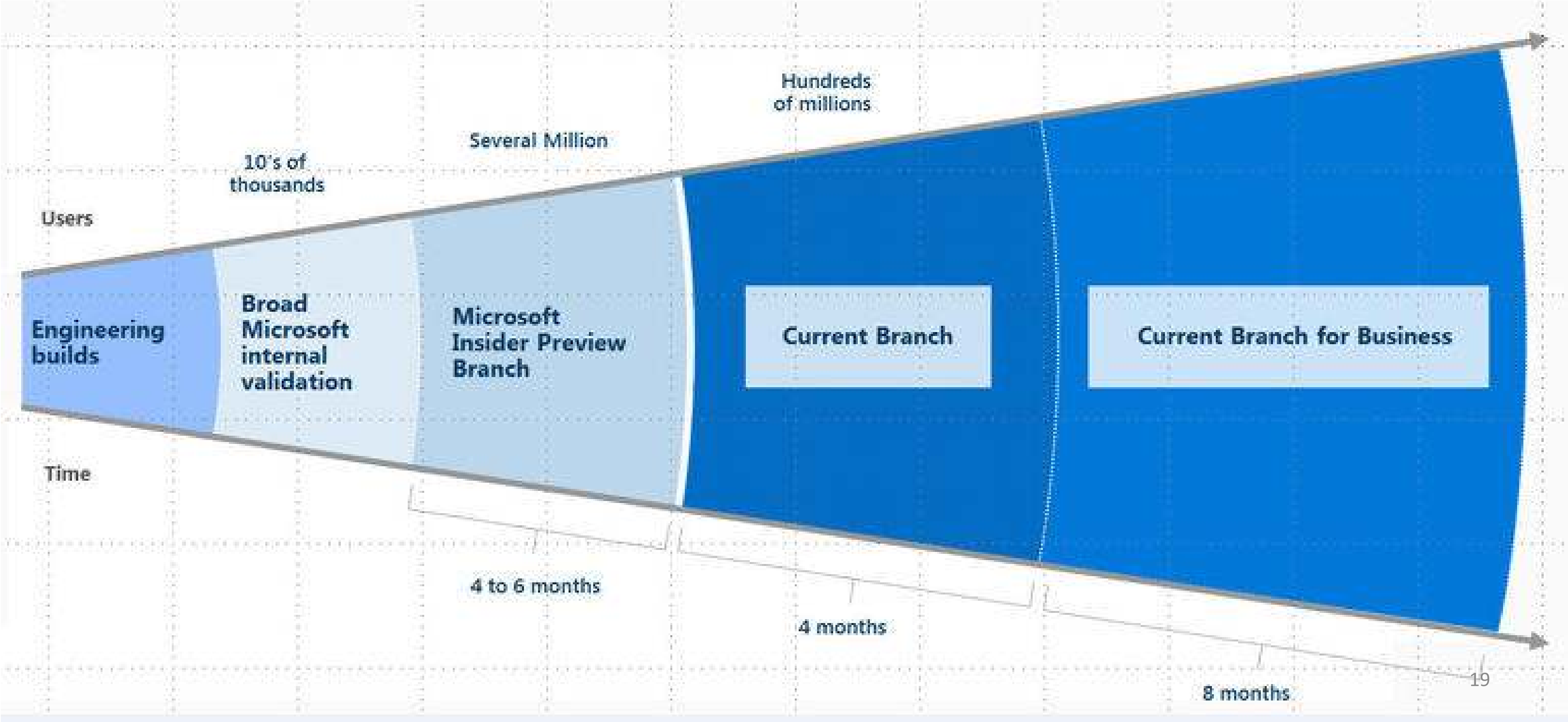
- In its earliest days, a build is seen only by the "canary" group in Microsoft. "Canary" is an example of a branch.
- A build filters through many branches before non-Microsoft folks see that build
  - First non-MSFT people to see a release are the "Insiders" branch, which any brave soul may join, as you'll see
  - All Windows 10 systems enter the first "non-enthusiast" public branch out of the box, the "Current Branch" or CB
  - Folks who don't want to get near scary new code opt to be in the "Current Branch for Business" or CBB, which ships four to six months after CB
  - Users of Windows Home have no choice, they're in CB, but Pro and Enterprise users can opt to move to CBB

Branches and Rings



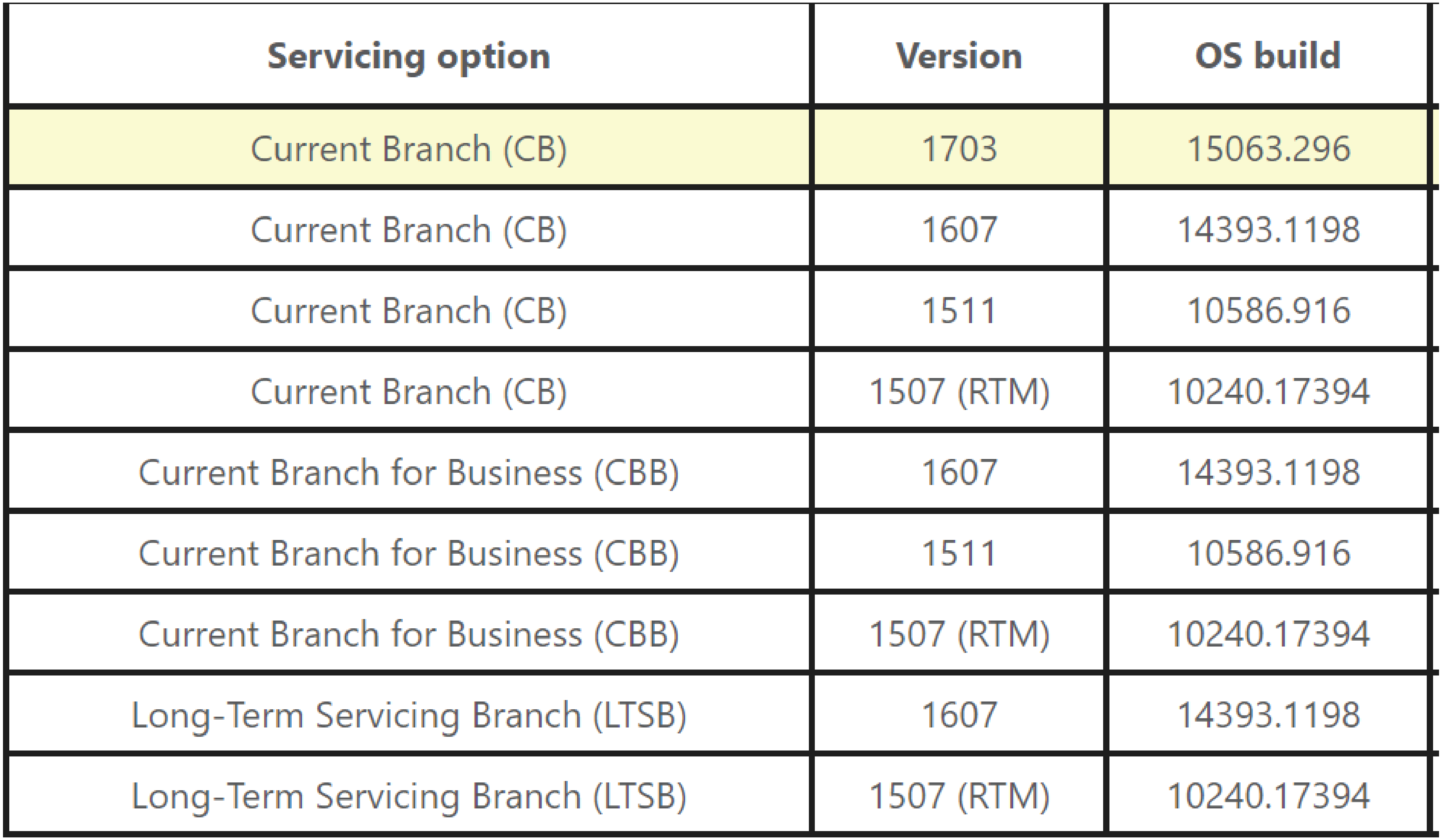
Branch/ring example: "Windows Insiders" is a branch. Three rings inside it: Fast, Slow and Release Preview

Branch Timings



Here's the "You Must Upgrade" Part

- Let's say you're on CBB and adopt 1511 (win 10 v 2)
- Now let's say CBB gets 1703 (win 10 v 4) in July 2917
- 1703 is two updates after 1511
- CBB people should in theory get 60 days' more grace to September 2017
- Then CBB 1511 people will stop getting new updates (patches)
- Again, this is all in theory, as there's been no die-offs yet



Servicing option	Version	OS build
Current Branch (CB)	1703	15063.296
Current Branch (CB)	1607	14393.1198
Current Branch (CB)	1511	10586.916
Current Branch (CB)	1507 (RTM)	10240.17394
Current Branch for Business (CBB)	1607	14393.1198
Current Branch for Business (CBB)	1511	10586.916
Current Branch for Business (CBB)	1507 (RTM)	10240.17394
Long-Term Servicing Branch (LTSB)	1607	14393.1198
Long-Term Servicing Branch (LTSB)	1507 (RTM)	10240.17394

On to the Details… What Can I Do and How Can I Do It?

- Ignore features for up to six months by with a GPO setting
- Ignore patches **for up to 30 days**
- Pause all updates for up to 60 days
- Join Insider Hub
- Restrict the hours that Windows is allowed to reboot to install new features via "Active Hours"
- Enable/disable peer-to-peer update/upgrade sharing
- Configure peer-to-peer upgrade sharing
- Control level of information sent to Microsoft

Sounds Like the CBB Is the Way to Go

- CBB gets an extra four months' worth of testing before release
- Anyone with Pro, Enterprise or Education can join the CBB via a Settings check box or with at group policy setting
- Windows Home users… no way to get to CBB
- You can join the CBB either through the UI (through 1607) or group policies (even on 1703)
- If this "one year" thing is freaking you out, I've got an option later

Not an Early Adopter? Ignore for 180 Days

- The "you must be on one of the two latest builds in your branch" rule never changes
- But you don't want Windows Update nagging you immediately
- So there's a group policy that tells Windows Update not to offer an upgrade for up to 180 days

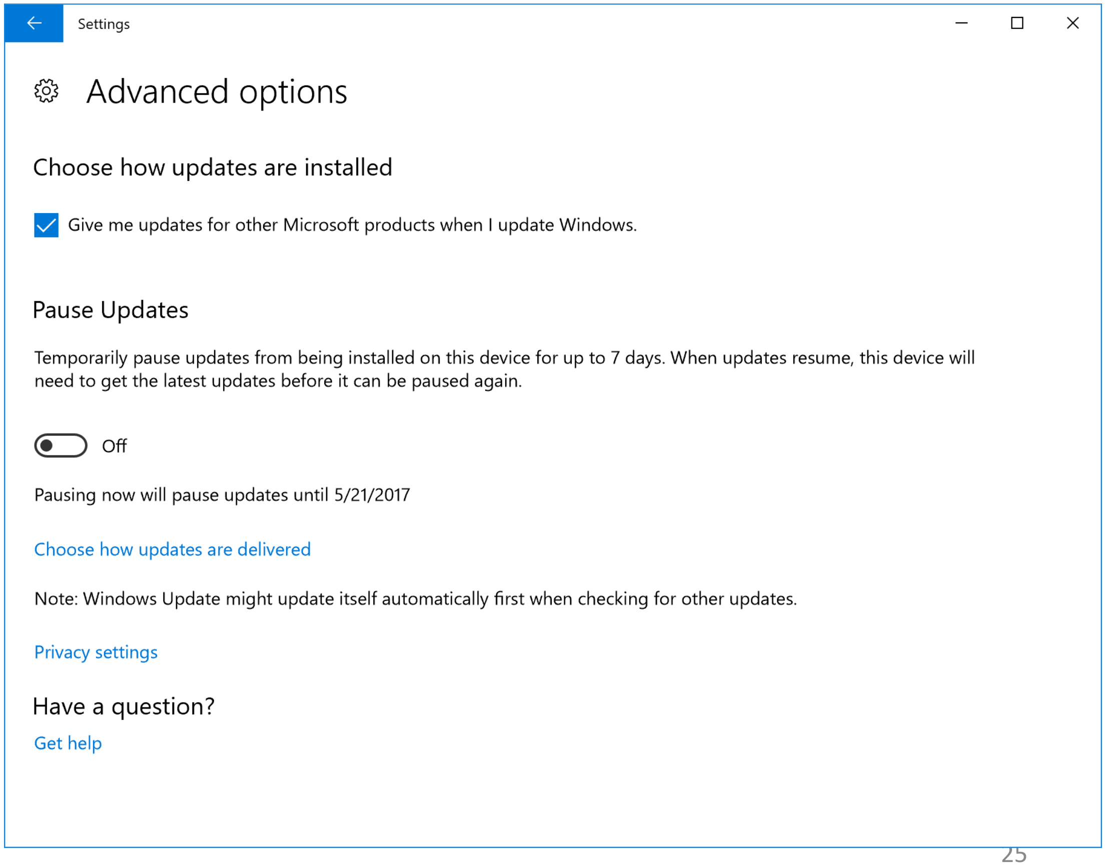
Joining the CBB in Settings

Settings / Update and Security / Advanced Options

Prior to 1703 you could choose CBB here; now it's just group policies.

It *does* offer a "pause for seven days" switch – GPs allow up to 60

None of this is in Home



Advanced options

Choose how updates are installed

☑ Give me updates for other Microsoft products when I update Windows.

Pause Updates

Temporarily pause updates from being installed on this device for up to 7 days. When updates resume, this device will need to get the latest updates before it can be paused again.

Off

Pausing now will pause updates until 5/21/2017

Choose how updates are delivered

Note: Windows Update might update itself automatically first when checking for other updates.

Privacy settings

Have a question?

Get help

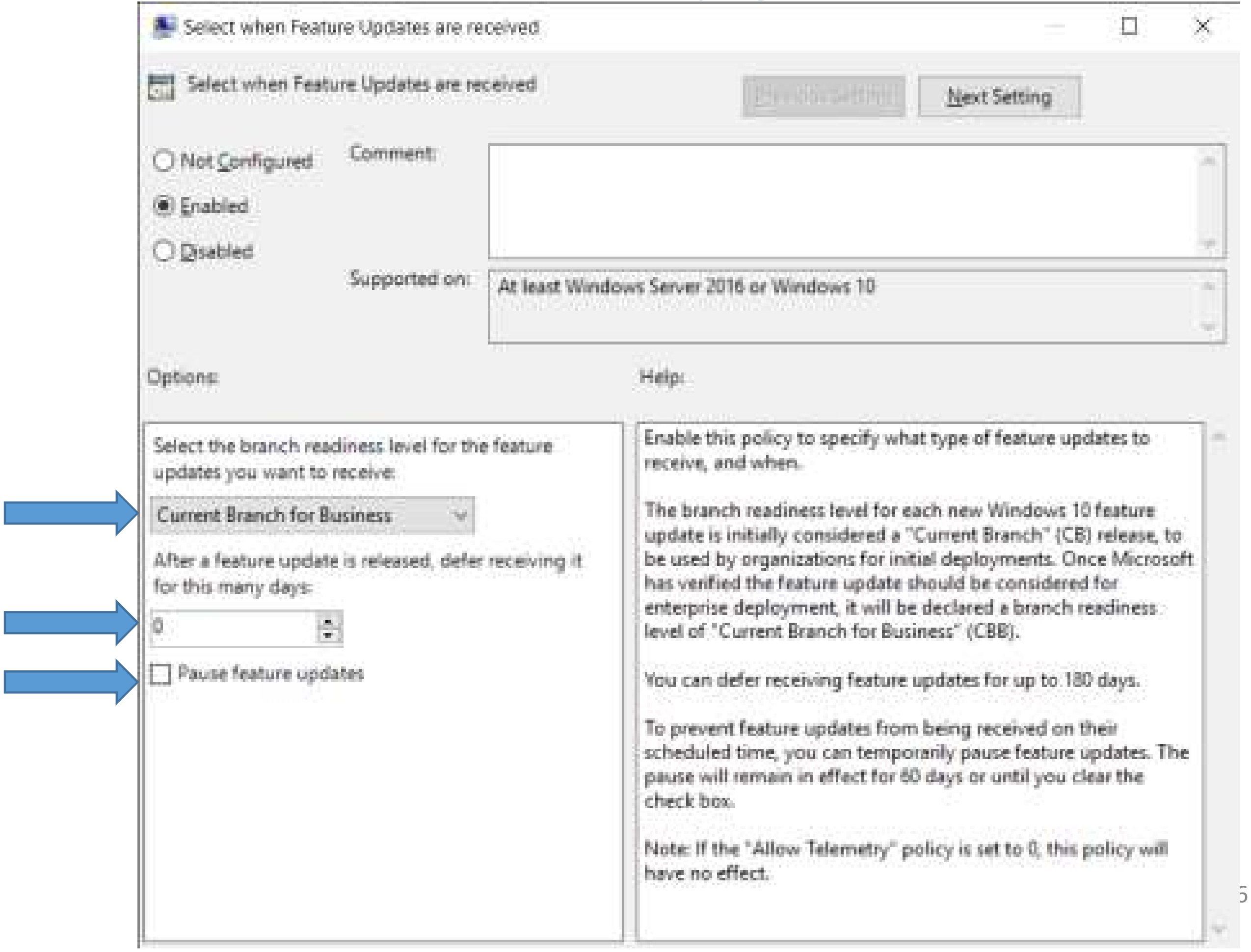
GPO Settings: Join CBB, Defer Upgrades

Admin Templates / Windows Components / Windows Update / Defer Windows Updates

Enable the policy, choose "Common Branch" or "Common Branch for Business"

Then dial in how many days

This says, "we're in the middle of something, skip the updates for up to 60 days." It is *not* the 60-day grace period



Select when Feature Updates are received
Select when Feature Updates are received
Previous Setting
Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016 or Windows 10

Options:

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:

0

□ Pause feature updates

Help:

Enable this policy to specify what type of feature updates to receive, and when.

The branch readiness level for each new Windows 10 feature update is initially considered a "Current Branch" (CB) release, to be used by organizations for initial deployments. Once Microsoft has verified the feature update should be considered for enterprise deployment, it will be declared a branch readiness level of "Current Branch for Business" (CBB).

You can defer receiving feature updates for up to 180 days.

To prevent feature updates from being received on their scheduled time, you can temporarily pause feature updates. The pause will remain in effect for 60 days or until you clear the check box.

Note: If the "Allow Telemetry" policy is set to 0, this policy will have no effect.

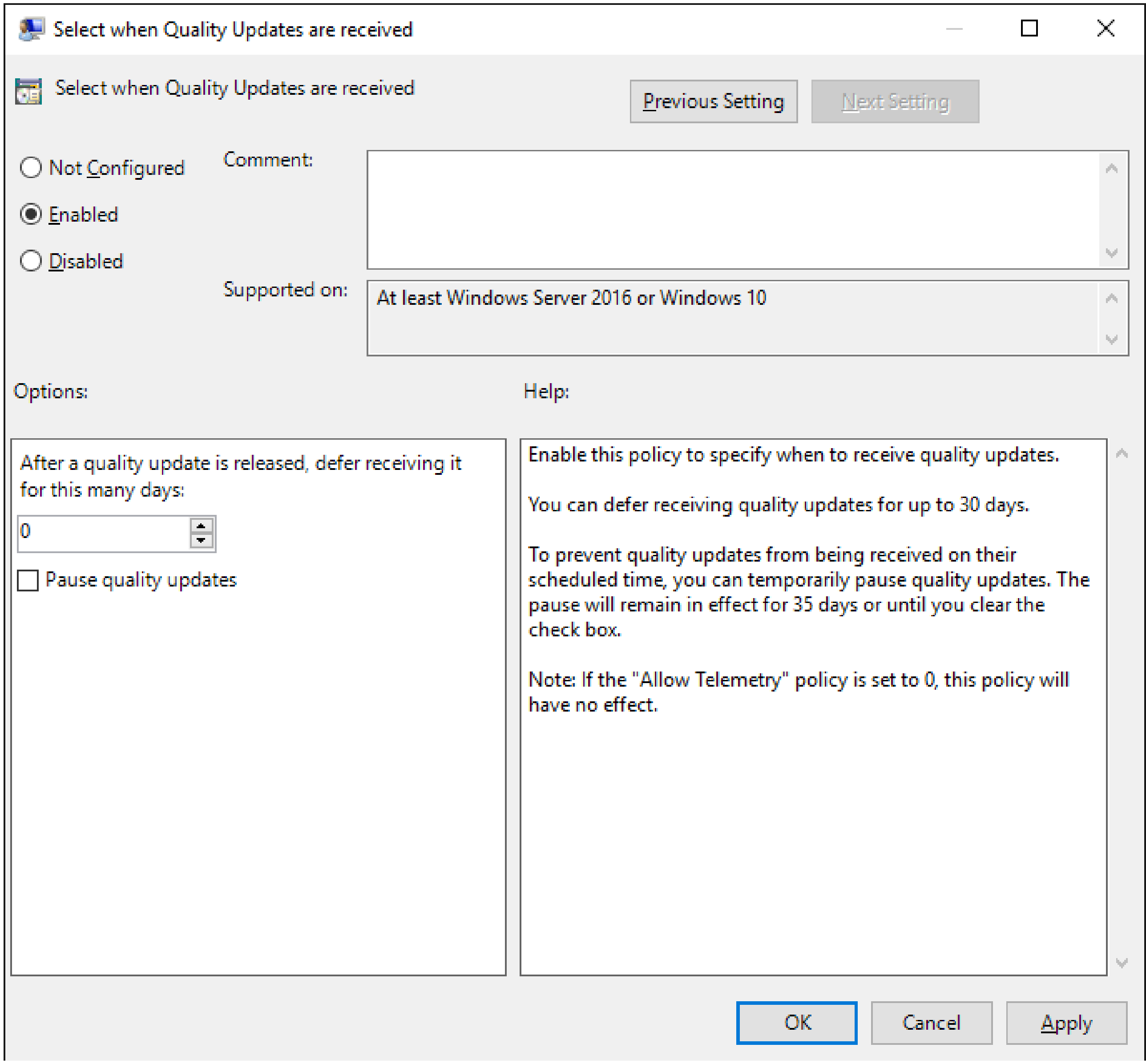
Controlling Updates (Patches) with WUB

- Again, WSUS can control updates to a certain extent, but for some reason WSUS hasn't really gotten Win 10-smart
- You can push off updates – patches – for only up to four weeks
- I can't see a way in the UI to do it, but there's a group policy
- WUB and WSUS: if you use WUB settings and have WSUS, WUfB takes over but only for the Windows updates, not the Office updates or whatever else WSUS handles (this was a new 1607 – win 10 v 3-- feature)

Same location as the previous setting.

Defer Patches – note no branch here

Cannot defer a patch more than 30 days



Select when Quality Updates are received

Select when Quality Updates are received

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016 or Windows 10

Options:

After a quality update is released, defer receiving it for this many days:

0

□ Pause quality updates

Help:

Enable this policy to specify when to receive quality updates.

You can defer receiving quality updates for up to 30 days.

To prevent quality updates from being received on their scheduled time, you can temporarily pause quality updates. The pause will remain in effect for 35 days or until you clear the check box.

Note: If the "Allow Telemetry" policy is set to 0, this policy will have no effect.

Create Your Own Rings

- So you see that you can delay new features by zero to six months and patches by zero to four weeks
- As these are group policies, you can thus have different GPOs with different delay lengths, attached to different groups of PCs
- This is how you create your own rings
- But don't stop there… think about joining a few boxes to Windows Insider

Block Drivers in Updates

- Windows 10 has been delivering drivers with updates and essentially forcing them on systems
- An Anniversary setting in Windows Components / Windows Update is "Do not include drivers with Windows Updates"
- It's just an enable/disable setting

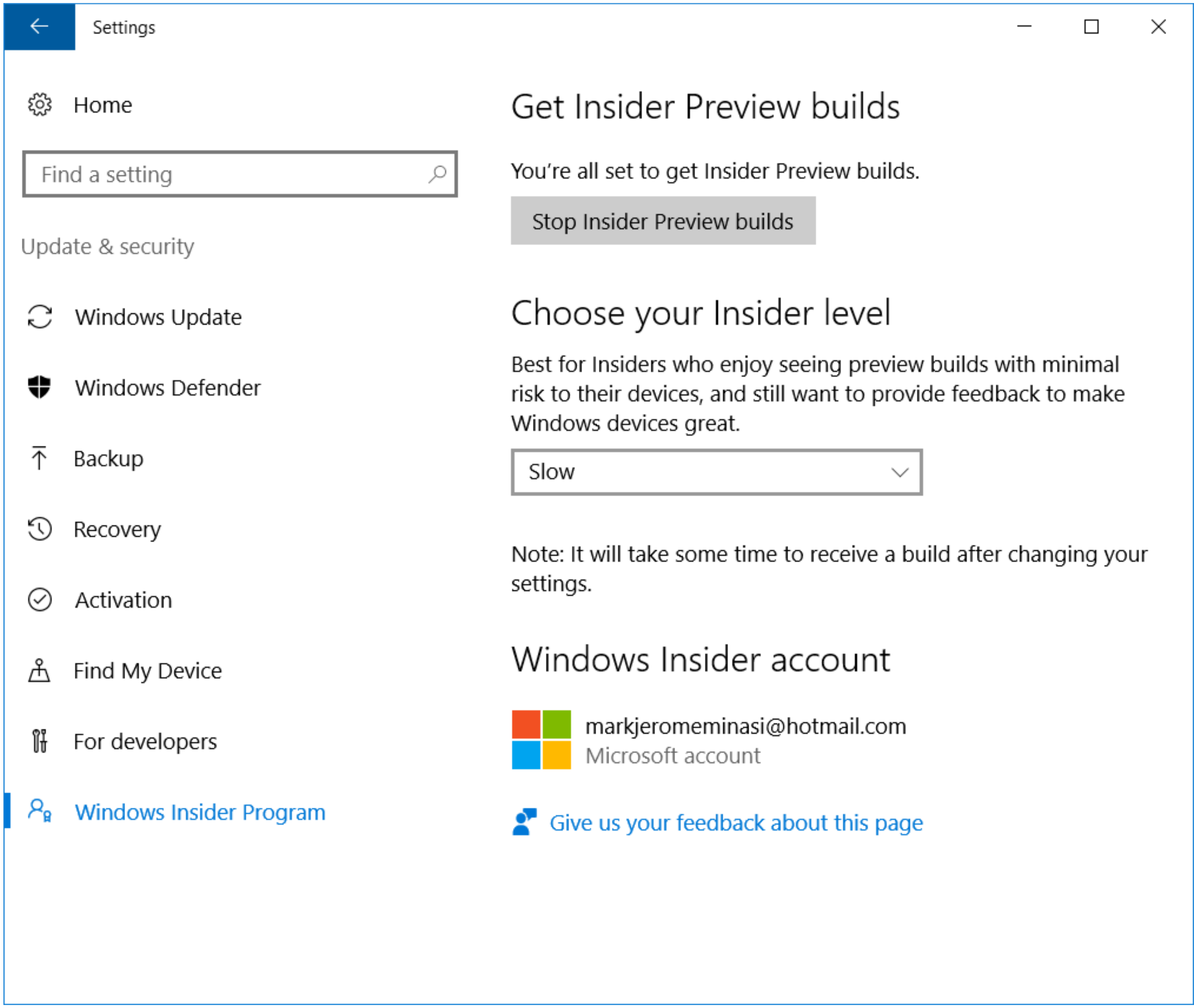
Windows Insider

- No GPO setting, just a Settings UI check and slider
- Settings / Update and Security / Windows Insider Program
- There are three rings in Insider:
  - Fast – more risky, some irritating things may fail, but in my experience nothing that stopped me from doing my work. Main irritant is that there are more of these than in Slow
  - Slow – filters through Fast for a bit, much more stable
  - Release Preview: you get new upgrades a few weeks before CB
- I strongly recommend that you have a few boxes on WIP
- But if Fast, nothing mission-critical!

Settings page for Windows Insiders

Note that this can be a kind of one-way switch, as in some cases Microsoft says you may have to wipe and rebuild to turn it off.

There is a group policy that *blocks* users from joining Insiders, but that's all



Settings

Home

Find a setting

Update & security

Windows Update

Windows Defender

Backup

Recovery

Activation

Find My Device

For developers

Windows Insider Program

Get Insider Preview builds

You're all set to get Insider Preview builds.

Stop Insider Preview builds

Choose your Insider level

Best for Insiders who enjoy seeing preview builds with minimal risk to their devices, and still want to provide feedback to make Windows devices great.

Slow

Note: It will take some time to receive a build after changing your settings.

Windows Insider account

markjeromeminasi@hotmail.com
Microsoft account

Give us your feedback about this page

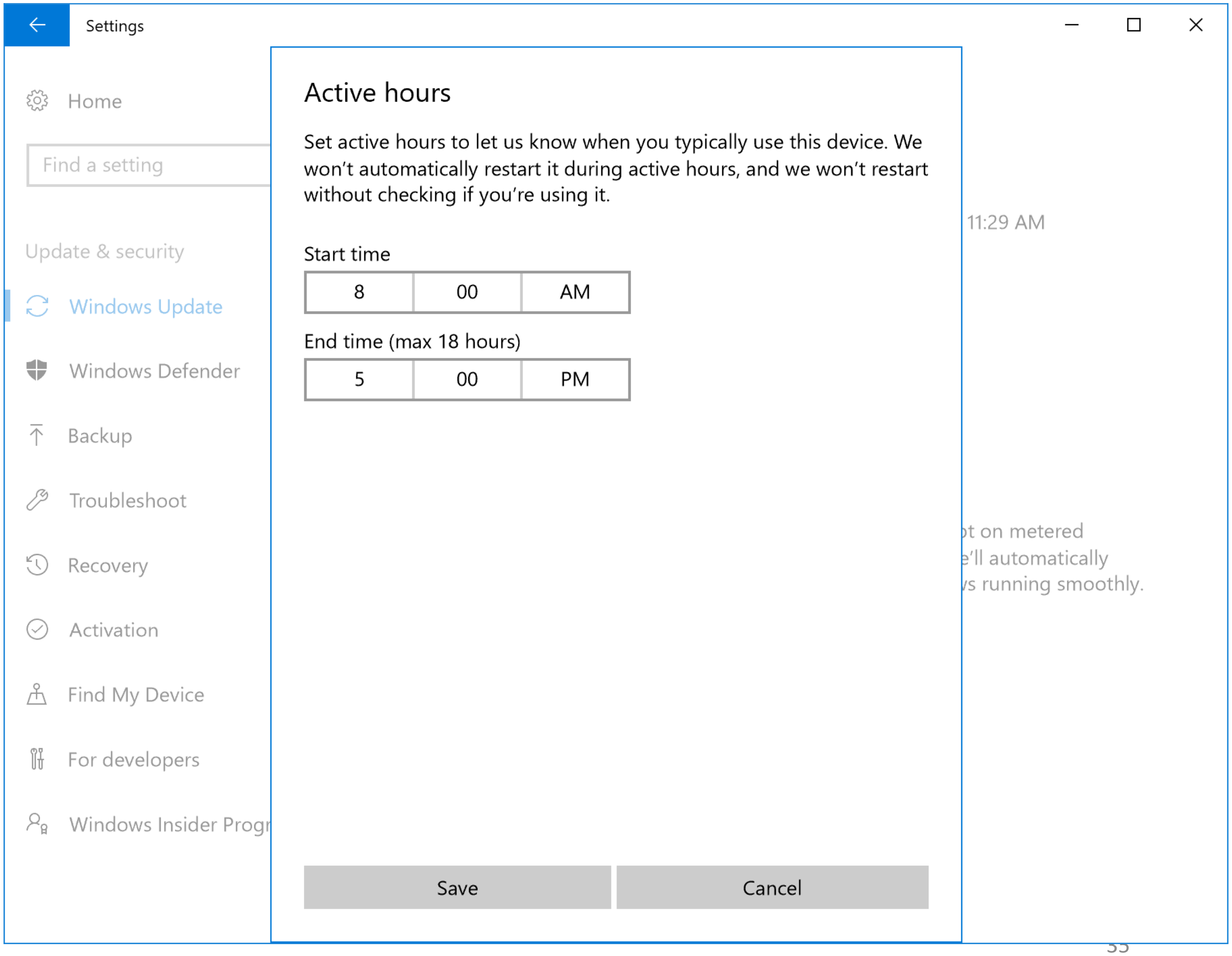
The Worst Part of Upgrades (IMHO)

- If you leave your computer on (as I do), it's irritating to find that your computer has rebooted and lost anything you hadn't saved, or that now some Office app isn't sure what version of a file to save
- And then there's the dread "Hello" page when you try to log on
- It's hard to say to Win 10, "don't reboot until I let you!," but you have *some* control
- From Settings / Update and Security, there is "Change Active Hours" and "Restart Options"

Pushing Off Reboots

- "Restart options" really only lets you set a preferred day and time for the reboot; it's really only useful if you see the upgrade coming
- "Active hours" lets you define a 12-hour window in the day – yes, it can't be more than 12 hours – where Windows should never reboot to get some upgrade working
- (1703 increases that to 18 hours)
- It seems to be pre-built with an 8AM-5PM set of active hours
- "No auto-restart with logged on users for scheduled automatic updates installations" in the Windows Update GP settings may defeat this whole thing … we'll know when the first post-Anniversary updates appear

Active Hours in Settings



Active hours

Set active hours to let us know when you typically use this device. We won't automatically restart it during active hours, and we won't restart without checking if you're using it.

Start time

8	00	AM

End time (max 18 hours)

5	00	PM

Group Policy Settings for Auto-Reboots

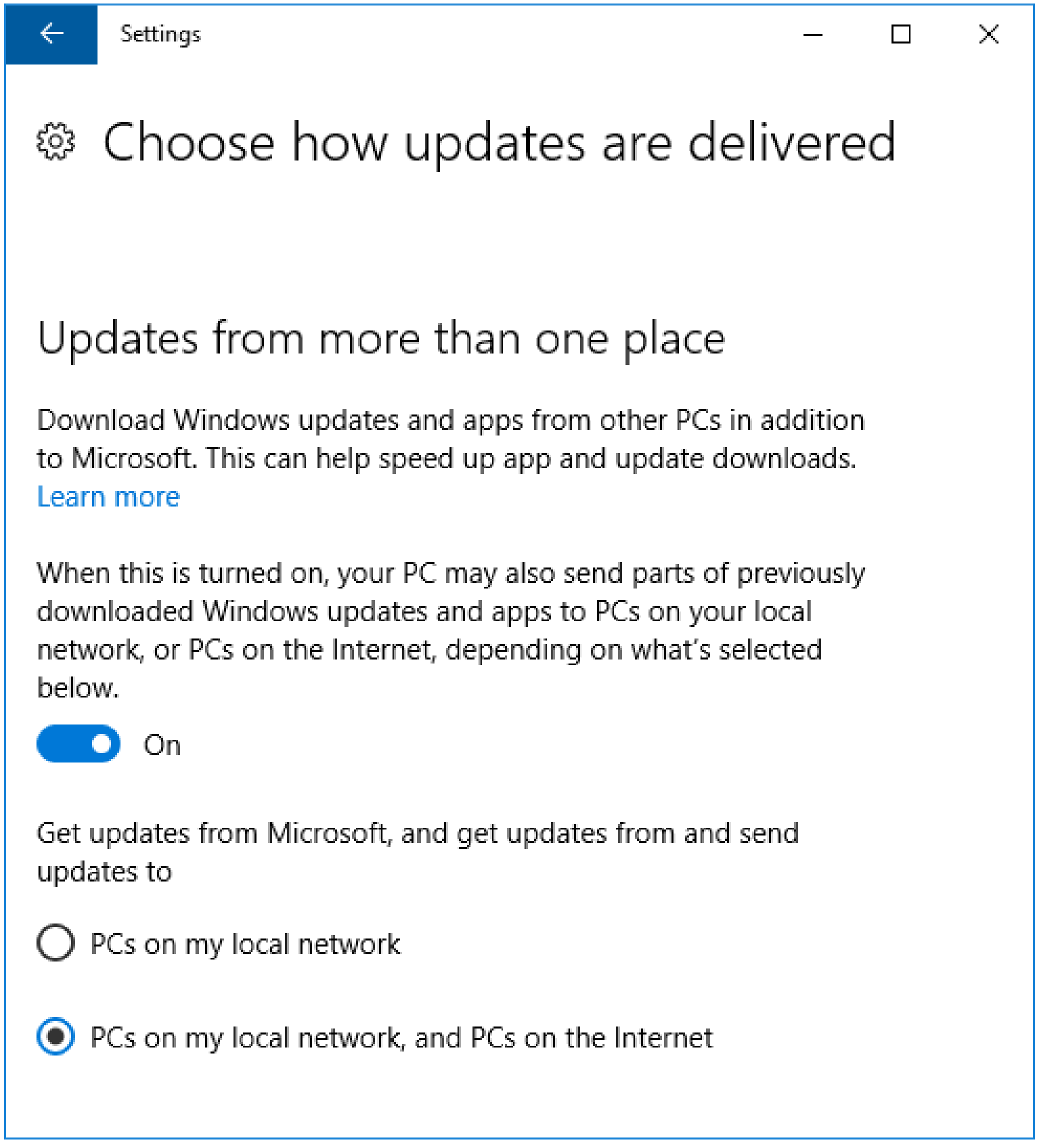
- It is in the "Windows Components / Windows Update" part of GP settings unlike the others, which have their own "Defer Windows Updates" folder
- "Turn off auto-restart for updates during active hours"
- You specify two values: Start and End, *but* if End is more than 12 hours after Start, Windows just adds 12 hours and calls that the End of active hours
- Change the "12's" to "18's" when you adopt 1703, Win 10 v4

Patches Via Torrents: WUDO

- "Windows Update Delivery Optimization"
- Upgrades can be *big*… gigabytes big… and so Windows Update can use a BranchCache-like, bit torrent-like delivery system
- One system in the building gets an update, it caches it and other systems can ask, "does anyone have this update?"
- This does *not* happen over metered connections
- Lots of group policy settings to tweak it
- Windows Components / Delivery Optimization
- And there are settings in Settings / Update & Security / Windows Update / Advanced Options / Choose how updates are delivered

Two main things: the on/off switch (on by default) and whether to only accept updates from local systems or anyone on the Internet.

There are a number of other knobs and switches, but you need to go to Group Policies to see them.



Settings

Choose how updates are delivered

Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads.
Learn more

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network, or PCs on the Internet, depending on what's selected below.

On

Get updates from Microsoft, and get updates from and send updates to

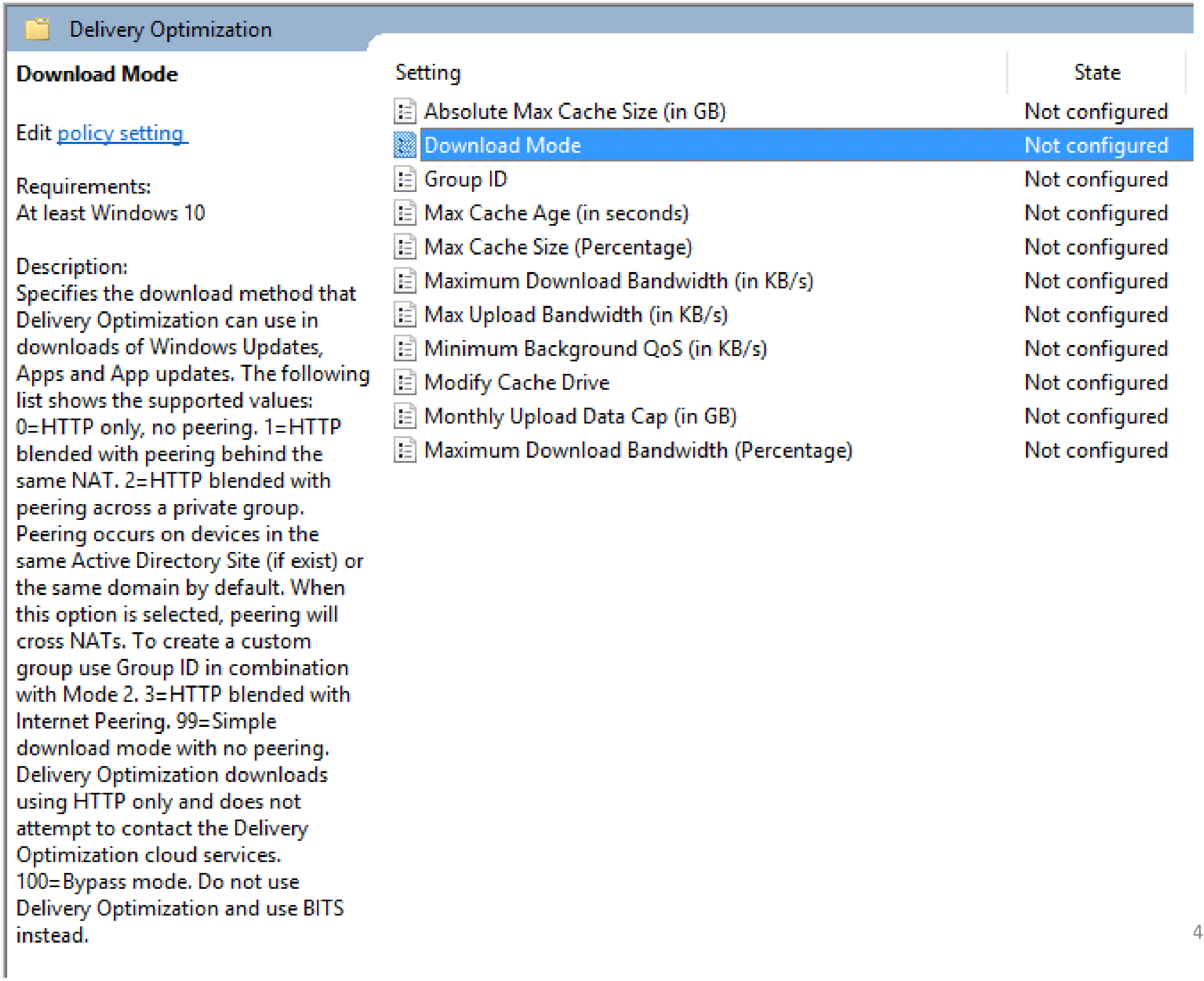
○ PCs on my local network

● PCs on my local network, and PCs on the Internet

WUDO GP Settings

- Group policies let you control
  - Peer-to-peer distribution
  - Max size, drive to place the updates cache, max cache age
  - Bandwidth for transfer of updates/upgrades
  - Monthly bandwidth cap
  - Can create "sharing groups via GUIDs
- These are all part of Windows Update for Business

WUDO Options



Delivery Optimization

Download Mode

Edit policy setting

Requirements:
At least Windows 10

Description:
Specifies the download method that Delivery Optimization can use in downloads of Windows Updates, Apps and App updates. The following list shows the supported values: 0=HTTP only, no peering. 1=HTTP blended with peering behind the same NAT. 2=HTTP blended with peering across a private group. Peering occurs on devices in the same Active Directory Site (if exist) or the same domain by default. When this option is selected, peering will cross NATs. To create a custom group use Group ID in combination with Mode 2. 3=HTTP blended with Internet Peering. 99=Simple download mode with no peering. Delivery Optimization downloads using HTTP only and does not attempt to contact the Delivery Optimization cloud services. 100=Bypass mode. Do not use Delivery Optimization and use BITS instead.

Setting	State
Absolute Max Cache Size (in GB)	Not configured
Download Mode	Not configured
Group ID	Not configured
Max Cache Age (in seconds)	Not configured
Max Cache Size (Percentage)	Not configured
Maximum Download Bandwidth (in KB/s)	Not configured
Max Upload Bandwidth (in KB/s)	Not configured
Minimum Background QoS (in KB/s)	Not configured
Modify Cache Drive	Not configured
Monthly Upload Data Cap (in GB)	Not configured
Maximum Download Bandwidth (Percentage)	Not configured

WUDO Notes

- Windows Update actually keeps track of what systems sit behind a given NAT router so it knows where to direct systems to get torrent-ed updates/upgrades from
- Same with location in general for the part that says, "accept updates/upgrades from any system on the Internet"

And One More Setting…

- Pretty much all of the WUB settings are nullified if you dial down the "telemetry" between a PC and Microsoft to its absolute minimum
- Look in Windows Components / Data Collection and Preview Builds under a setting called "Allow Telemetry"
- "0" is minimum, "1" is "Basic," which is default
- If you set it to 0, all of the WUB settings are ignored
- And this is only Enterprise… set Pro to 0 and it automatically becomes "1"

Another Alternative: LTSB

- "Long Term Servicing Branch," an alternate Enterprise SKU
- You are not offered any upgrades, just updates
- Microsoft delivers patches for any given build for ten years and no more
- After that, you must move to a newer build via an in-place upgrade (or flatten and rebuild) just as you would in going (for example) from 7 to 10
- Microsoft does *not* offer LTSB releases for every upgrade version

Some Things Aren't in LTSB

- Because basically nothing is supposed to change in LTSB, Microsoft leaves some things out of LTSB
  - Edge browser
  - Cortana
  - Modern apps

Thank You!

- I enjoy making Windows 10 easier to understand, and I hope I succeeded for you
- Ask questions now or I'm at mark@minasi.com
- Or contact me via twitter @mminasi, or sign up for my newsletter or join my new-and-improved forum at newforum.minasi.com
- Please fill out an evaluation