Keeping Windows 10 devices up to date with Microsoft Intune and Windows Update for Business

The release of Windows 10 introduced Windows as a service and a new approach to servicing Windows and deploying updates. Windows 10 features a continuous update delivery model with a faster update release cadence. Rather than waiting years between version releases, Microsoft now spreads new features and the latest security defenses into a continual update process. To streamline update management and eliminate the need for on-premises infrastructure to deploy updates, Microsoft Core Services Engineering and Operations (CSEO) recently implemented Windows Update for Business (WUfB), a publicly available, cloud-based Windows update service that simplifies update management for Windows 10 devices.

Windows was traditionally serviced with major version releases every few years, service packs, and monthly updates. We had to approach almost every major update release as a complicated, long-term project. It was time consuming, costly, and often disruptive for the business. For Windows 10, an operational approach to deploying major updates was needed—an approach that allowed processes to be continually refined with each release, reducing cost and complexity over time.

With Windows 10, our updates are smaller and more frequent. They come in two flavors:

- **Feature updates.** Released twice a year, feature updates include new operating system features, functionality, and bug fixes.
- **Quality updates.** Released every month, quality updates include security and reliability fixes.

WUfB helps us keep Windows 10 devices at Microsoft up to date by connecting them directly to the Windows Update service. With WUfB, we can control how and when our employees' and vendors' Windows 10 devices are updated, including update deferments. We can also restart enforcement using group policy for domain-joined devices, and Microsoft Intune policies for cloud domain-joined or Azure AD-joined devices. It also provides centralized management and can be configured without requiring any on-premises infrastructure.

Using co-management strategies to get to modern management

At Microsoft, there are currently 210,000 Active Directory domain-joined Windows 10 devices managed through System Center Configuration Manager and 30,000 Azure AD Windows 10 devices managed through Intune. In our environment, we use co-management strategies while moving all devices toward modern management with Intune and Azure AD-joined.

Most employee and vendor devices are still AD-joined and managed with Configuration Manager. To simplify IT administration, we're making modern management with Intune and Azure AD the default experience for new devices. As illustrated in Figure 1, WUfB has made it possible to shift our update-management workload to the cloud and introduce consistency in how we deploy updates to both domain-joined and managed devices.

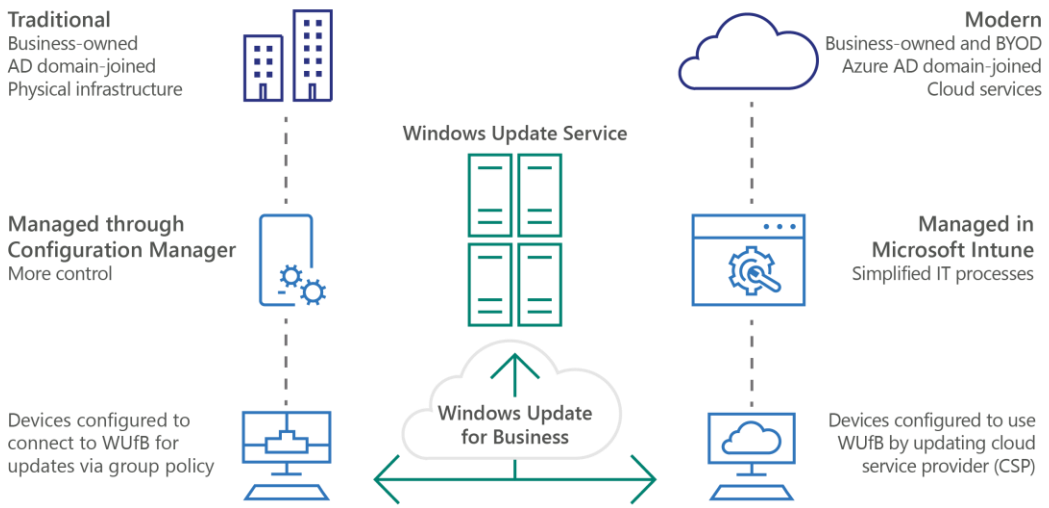


Figure 1. WUfB manages updates for both traditionally and modernly managed Windows 10 devices at Microsoft

Implementing Windows Update for Business

We began moving all of our Windows 10 update servicing into WUfB after the release of Windows 10 version 1803, also known as the Windows 10 April 2018 Update. It offered new features that improved control and visibility of WUfB, and it helped us better manage, secure, and target deployments. Specifically, this version provided the following benefits:

- **Greater control over update deployment.** Now, we can remotely pause and uninstall problematic updates. If an anomaly is recognized, we can easily roll back feature and quality updates using Intune.
- **Greater visibility into device update health.** Windows Analytics and Desktop Analytics provide extensive data about the state of devices to help manage Windows deployments. Enhancements in Windows Analytics and Desktop Analytics have increased visibility into deployment activities and delivery optimization. Now, we can more confidently manage and monitor deployments.

Since the release of Windows 10 version 1803, several new features and configuration options have been introduced that we've deployed through our early adoption program as well as our broad deployment. The new WUfB features and configuration options include:

- **The ability to configure separate restart policies for quality and feature updates.** This allows us to provide users with flexible installation experiences while keeping the company secure.
- **The ability to disable pause functionality.** We can now prevent users from blocking quality updates via group policy in Windows 10 to ensure they don't keep delaying quality updates that often include important security updates.
- **The ability to configure compliance-deadline policies for quality and feature updates.** This builds upon the existing IT pro and user experience by providing a grace-period setting after the configured-enterprise deadline to get the device updated.

For our Active Directory domain-joined devices, we created group policies that directed Windows 10 devices to get their updates from WUfB. These group policies configure devices to install updates and restart devices within the timelines we configured for security and compliance. After these group policies were applied to employee and vendor devices, we removed them from our Configuration Manager patch collection for quality updates.

To view our update policy configurations, including the new settings in Windows 10 1909, see Appendix A: Windows Update for Business and restart group policies.

For Intune-managed devices, we configured their settings using configuration service providers (CSPs) to provide an equivalent experience to the devices managed via group policy. Refer to Appendix B: Windows Update for Business and MDM policies to see how we configured our Intune-managed devices.

Using servicing channels and deployment groups to create deployment waves

To align with our continuous-update delivery model, Windows 10 now has two servicing channels. Each servicing channel provides different levels of flexibility over when feature updates are delivered to client computers after they are released:

- **Semi-Annual Channel (SAC).** Receives released feature updates twice a year. Feature updates will be made available on this channel once they are ready for broad deployment for consumers as well as enterprise customers. Semi-Annual Channel for 1809 and earlier, and Semi-Annual Channel (Targeted) for 1809 and earlier, have been deprecated and are applicable only to 1809 and earlier. Any deployment-deferral settings that had been made by Windows Update for Business users will stay in effect. When Microsoft is confident that the quality is good enough for enterprises, it releases the update to the SAC channel after making it available on the insider rings and newly announced release-preview ring.
- **Long-Term Servicing Channel.** Used primarily for specialized devices—for example, automated teller machines (ATMs) and computers that control medical devices. Typically, these devices aren't used for anything beyond their primary function and don't run Microsoft Office. They receive feature updates only every few years.

The introduction of servicing channels brings with it the concept of *deployment rings*, which is a way to categorize the combination of a deployment group and a servicing channel to group devices for successive deployment waves. For more information about developing a deployment strategy using servicing channels and deployment rings, see Plan servicing strategy for Windows 10 updates.

We configured feature updates in five waves for domain-joined devices to optimize bandwidth utilization, avoid overloading support resources, and mitigate risks. All Intune users are configured to have feature updates deployed in a single wave. As the number of Intune devices grows in our environment, we'll likely segment that group into multiple waves.

We've also added a group of roughly 1,000 devices to our Windows Insider prerelease channel to validate prerelease feature updates. This group of early adopters provides valuable feedback to the product group that helps prepare feature updates for their release.

Configuring feature-update policies

Previously referred to as *upgrades*, feature updates are released every six months. They include security and quality revisions, as well as significant feature additions and changes. At Microsoft, we broadly deploy every feature update as soon as it's publicly released by the Windows product group.

Most of our Windows devices are configured to update twice a year on our Semi-Annual Channel. For most enterprise customers, we recommend using Insider Release Preview for early adoption and targeted validation for a subset of devices, and then using SAC for broad update deployment.

> ***Note:*** *While enterprise customers can defer or skip an update, Microsoft recommends you deploy all feature updates.*

WUfB has eliminated the need for update-package creation, as well as the need for a physical infrastructure to host update packages. When we were using Configuration Manager to deploy feature updates, we needed to create and package a task sequence for the update and then test the package. After successful testing, we replicated the package to all Configuration Manager distribution points globally and published the packages for deployment. For packaging, replication, and publishing activities, we're saving 120 hours of work per deployment, with an additional 90 hours of savings in testing because we don't need to validate our installation packages.

We also have improved coverage. We were creating only 10 packages, one for each of the five most used languages, in 64-bit and 32-bit versions. WUfB supports all 34 base operating-system languages in our environment, in 64-bit and 32-bit versions, expanding update service coverage while saving us resources, time, and overhead.

These WUfB improvements have saved us time without hurting us on compliance—we've been able to maintain the initial target compliance rate of 95 percent within 10 weeks of a feature update release.

Configuring quality update policies

Quality updates are traditional operating system updates typically released the second Tuesday of each month. They can include security, critical, and driver updates. Quality updates are cumulative, meaning that the latest quality update includes all the available fixes released for a specific Windows 10 feature. Additionally, you can configure devices to receive non-Windows Updates (such as those for Microsoft Office or Visual Studio) as quality updates. These non-Windows Updates are known as Microsoft Updates and devices can be configured to receive them along with the Windows Updates. We use WUfB to deliver both Windows and Microsoft updates. Third-party updates are still managed through Configuration Manager.

To meet security and compliance requirements, we defined a target compliance rate and use restart policies for enforcement. As soon as a quality update is offered on devices, it downloads and installs. If a reboot is required, the device is put into a "pending restart" stage. The enforcement of the reboot policy is set for five days.

In Windows 10 1803 and earlier versions, the first two days after a patch is installed, the device tries to restart outside of device active hours. (Default active hours are 8 AM to 5 PM, unless specifically set via Group Policy/Intune CSPs.) If the device isn't restarted successfully within the first two days, the user will start receiving prompts to schedule the restart, with options to snooze or dismiss the notification. Users can schedule the restart, but they can push it out only until the IT pro-configured deadline day [Auto restart (two days) + Snooze (two days) + deadline (three days)]. This means they're able to snooze for two days. If a user hasn't scheduled a restart, the machine will force-restart on the deadline day after two notifications (one notification two hours before the restart and the other 15 minutes before).

In Windows 10 1809, we can have Windows 10 devices go directly into engaged restart after an update is downloaded and installed. Rather than the device trying to auto-restart outside of business for the first two days after an update is installed, with WUfB configured for engaged restart, users are notified of the pending restart right away, and they have the option to restart immediately or schedule the restart at a more convenient time. They can still snooze for two days, and they have five days to schedule their restart.

Beginning with Windows 10 1903, the compliance-deadline policy was introduced and broadly utilized within Microsoft. This lets the IT pro set the deadline in number of days, and a grace period for the devices. This policy starts the countdown for the update-installation deadline from the moment the update is published, instead of starting with the "restart pending" state as the older policies did. The policy also includes a configurable grace period to allow, for example, users who have been away to have extra time before being forced to restart their devices. Further, the policy includes the option to opt out of automatic restarts until the deadline is reached, by presenting the "engaged restart experience" until the deadline has expired. At this point the device will automatically schedule a restart regardless of active hours.

We broadly rolled out WUfB for quality updates in September 2018. One month later, at our next big patch Tuesday, we achieved our target adoption rate of 95 percent in a record-setting 10 days. Since then, we've seen more improvements—for example, we've already had a 50 percent reduction in the work related to applying Windows quality updates in our environment.

Improving bandwidth utilization through update delivery optimization

Because bandwidth for downloading new updates is a common concern, Microsoft uses delivery optimization to share the workload of downloading update packages between multiple devices in the environment. This sharing is done through a self-organizing distributed cache that allows clients to download update packages from alternate sources (such as other peers on the network) in addition to the traditional Internet-based Windows Update servers. This is configured through group policy and in Intune. To make this work, we changed some delivery optimization settings:

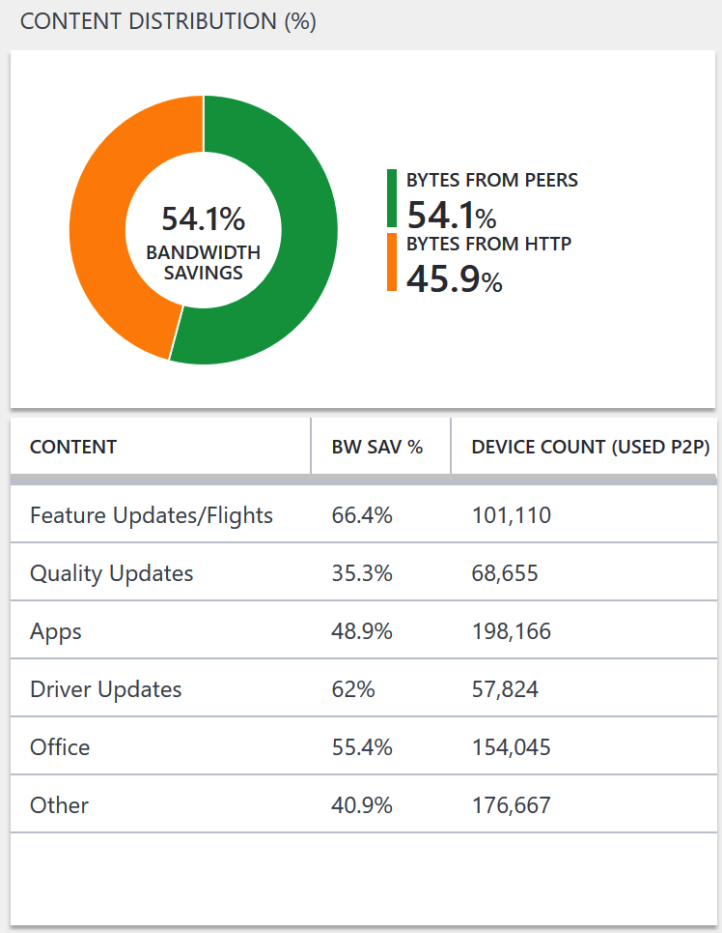
- **Allow uploads while the device is on battery.** We configure this setting so that it works only when the battery level is above 60 percent to minimize the impact on the device.
- **Download mode.** We use download mode two, which allows devices in the same domain or Active Directory site to be peers and share content.
- **Max cache age in seconds.** We set the max cache age to seven days (604,800 seconds) to increase the amount of time content is cached on devices, making it more likely that devices will be able to get their update content from peers.
- **Minimum peer caching content file size (in MB).** We set this option to 10 MB so that devices will peer only if they have a significant amount of content to share.

Note: *More details about these enabled configurations are included in Appendix A: Windows Update for Business and restart group policies.*

Monitoring update compliance using analytics

For Active Directory domain-joined devices, monitoring update installation compliance levels after moving the update service out of Configuration Manager can pose a challenge for organizations that haven't adopted Windows Analytics or Desktop Analytics to monitor their Windows 10 devices. The traditional method for monitoring update installations with Configuration Manager doesn't work because Configuration Manager can't see updates that have been installed through WUfB. Organizations that are considering using WUfB also should invest in Windows Analytics or Desktop Analytics to gain visibility and actionable insight into their environment, including update compliance.

Analytics solutions use diagnostic data to provide reporting and insights into an organization's Windows 10 devices. We have been effectively using Windows Analytics and Desktop Analytics to determine what has been installed on which devices. We use that information to monitor update installation and restarts.



CONTENT	BW SAV %	DEVICE COUNT (USED P2P)
Feature Updates/Flights	66.4%	101,110
Quality Updates	35.3%	68,655
Apps	48.9%	198,166
Driver Updates	62%	57,824
Office	55.4%	154,045
Other	40.9%	176,667

Figure 2. Windows Analytics displays bandwidth savings

Update compliance is a new Windows Analytics solution that enables organizations to monitor Windows 10 security, quality, and feature updates. It uses Windows 10 and Windows Defender Antivirus diagnostic data for all of its reporting. It collects system data—including update deployment progress, WUfB configuration data, Windows Defender Antivirus data, and delivery optimization usage data—and sends it to a secure cloud to be stored for analysis and usage in Azure Log Analytics.

For more information, see Monitor Windows Updates using update compliance.

Lessons learned

- **WUfB now takes advantage of update offer blocks.** If there is a known issue with an update on a specific device, the Windows update service might decide not to offer the update. Beginning with 1903, WUfB-configured devices have started taking advantage of these offer blocks. When known issues exist with an update for specific devices, they don't get the latest release offered, devices are checked for compatibility issues. If an issue is detected after an initial check, the user will see a notification in Windows Update that their device is temporarily blocked from getting the update (offer block). If the device successfully downloaded the update, there will be a second check to see if there is an issue. If there is, setup will be blocked from continuing, and the user will see a notification that mentions a hardware-compatibility issue (setup block). We also communicate these to our enterprise users via broad email to let them know if they don't get the update offered, one of the reasons may be offer or setup block, and users will get the update as soon as the issue is resolved. Missed-restart notifications can be inconvenient or cause data loss. The auto-restart feature in Windows 10 provides users with the most seamless update experience possible. During the Windows 10 1809 deployment, many users communicated that they were satisfied with the update experience because they didn't even notice it happened. However, some

users have expressed concerns about the potential for lost work as a result of unexpected restarts. New policies in Windows 10 1809 and 1903 have addressed this concern by going directly into the engaged restart experience that notifies users and allows them to schedule the update.

- **It isn't possible to configure devices to use WUfB for just quality or feature updates.** If a device is configured for one type of update, it will use WUfB for both. It is important to configure individual deferral policies for both quality and feature updates to avoid unexpected updates.
- **WUfB doesn't use a task sequence to run scripts before or after the setup like Configuration Manager-based deployments.** The task sequence is a common method that enterprises use to address compatibility issues. The task-sequence functionality was useful when updating devices to Windows 10, but we found with each Windows 10 release we relied less on these scripts and got to the point they were not required. If required, similar functionality can be implemented with WUfB using custom actions as part of the feature-update setup process.

Benefits

Windows Update for Business plays a key role in supporting the company's Windows as a service continuous-update delivery model. It helps us in CSEO keep devices secure with the latest updates and helps our users take advantage of the latest Windows features. Updating devices and keeping them up to date are key pillars in keeping business information secure, particularly in an ever-evolving threat landscape. We don't need to wait for large version releases and then plan the full upgrade deployments to roll out new and improved operating system and security features to our employees and vendors using Windows 10.

Modern management strategies, like moving operating system update servicing to the cloud and being able to manage updates for both domain-joined and managed devices with a single service, are simplifying and improving how we manage devices. After we configure our update policies for WUfB, we have confidence that it will just work. In the rare event that an update breaks something in the environment, it can be rolled back.

WUfB is providing better, more centralized control of update deployments, simplifying management, and enabling more efficient delivery of updates. Overall, we're seeing improved user satisfaction with the update experience and better adoption velocity for updates. The feature improvements in Windows 10 1809 included additional flexibility and more end-user control, which will help us provide an even better update and restart experience moving forward.

Are you ready to learn more about deploying Windows 10 or Windows as a Service, or using Windows Update for Business in your organization?

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Onboarding to Windows Update for Business in Windows 10

Appendix A: Windows Update for Business and restart group policies

Policy	<1809	1809	1903 and greater	Notes
Remove access to Pause Updates feature	N/A	Enabled	Enabled	Our security team requires pause functionality to be disabled on devices. This policy is new in 1809.
Specify Engaged Restart transition and notification schedule for updates	Enabled Transition (days) = 2 Snooze (days) = 2 Deadline (days) = 17	Enabled Quality updates: • Transition (days) = 0 • Snooze (days) = 2 • Deadline (days) = 5 Feature updates: • Transition (days) = 0 • Snooze (days) = 2 • Deadline (days) = 12	Compliance deadline policy is configured instead of this policy	The ability to configure separate restart settings for feature and quality updates is new in 1809. Devices not running 1809 were temporarily configured with a longer restart deadline to give users more time to install the 1809 update.
Specify deadlines for automatic updates and restarts	N/A	N/A	Enabled Quality update deadline in days = 7 Feature update deadline in days = 7 Grace period = 2	This feature will override the "Specify engaged restart transition and notification schedule for updates" policy. Until the deadline is reached, the devices will get the inbuilt toast notifications to update their

				devices to the latest release. Once the grace period is reached, pop-up notifications will show up 2 days and 12 hours before the device is forced to restart to apply the installed update.
Select when preview builds and feature updates are received	Enabled Readiness level = Semi-Annual Channel (Targeted) Deferral (days) = [value depends on deployment wave] Pause builds starting = 2017-01-01	Enabled Readiness level = Semi-Annual Channel (Targeted) Deferral (days) = [value depends on deployment wave]	Enabled Readiness level = Semi-Annual Channel Deferral (days) = [value depends on deployment wave]	We started broad deployment across the company with devices configured for the Semi-Annual Channel (Targeted) servicing channel for 1909 update. The deferrals are still honored. It will need to be changed to Semi-Annual Channel going forward. The number of deferral days depends on the deployment wave in which the device is placed. We configured the Pause Builds setting with a date of 2017-01-01 to disable the

						pause functionality. This decision was a workaround until the policy was delivered in 1809 to disable the functionality.
Select when quality updates are received		Deferral (days) = 0		Deferral (days) = 0	Deferral (days) = 0	We want devices to install quality updates as soon as they're available, so we configure all devices with a deferral period of 0 days.
Configure auto-restart warning notifications schedule for updates		Enabled Reminder (hours) = 2 Warning (mins) = 60		Enabled Reminder (hours) = 2 Warning (mins) = 60	Enabled Reminder (hours) = 2 Warning (mins) = 60	We configure this policy so that users receive a restart reminder notification 2 hours before the restart and a warning 60 minutes before a forced restart.
Configure auto-restart required notification for updates		Enabled Notification dismissal method = 2 – User Action		Enabled Notification dismissal method = 2 – User Action	Enabled Notification dismissal method = 2 – User Action	The default behavior is for restart notifications to be dismissed automatically after 25 seconds. We configure this policy to require users to dismiss the notification so that they don't miss the notification.
Do not connect to any Windows Update Internet locations	Disabled	Disabled	Disabled	Although this is the default Windows behavior, we		

				configure this policy to prevent conflicts with local policies set by Configuration Manager.		
Do not allow update deferral policies to cause scans against Windows Update		Disabled		Disabled	Disabled	Although this is the default Windows behavior, we configure this policy to prevent conflicts with local policies set by Configuration Manager.
Configure automatic updates		Enabled Configure automatic updating = 4 – Auto-download and schedule the install Install during automatic maintenance = enabled Scheduled install day = 0 – Every day Updated every week = enabled Install updates for other Microsoft products = enabled		Enabled Configure automatic updating = 4 – Auto-download and schedule the install Install during automatic maintenance = enabled Scheduled install day = 0 – Every day Updated every week = enabled Install updates for other Microsoft products = enabled	Enabled Configure automatic updating = 4 – Auto-download and schedule the install Install during automatic maintenance = enabled Scheduled install day = 0 – Every day Updated every week = enabled Install updates for other Microsoft products = enabled	The automatic-update settings are configured so that the device will download automatically and install updates every day at 11 a.m. We also select the option to get updates for other Microsoft products, to ensure we get all the available updates applied to devices.
Delivery Optimization – Allow uploads while the device is on battery while under Set Battery Level (Percentage)		60		Enabled	Enabled	We configure this policy to minimize the impact on

				devices running on battery.
Delivery Optimization – Download Mode	Group (2)	Enabled	Enabled	We use Download Mode 2 to allow devices in the same domain or AD site to be peers and share content.
Delivery Optimization – Maximum cache age in seconds	604800	Enabled	Enabled	We set the maximum cache age to seven days to increase the amount of time content is cached on devices.
Minimum Peer Caching Content File Size (in MB)	10	Enabled	Enabled	We set this policy to 10 MB so that devices will peer only if they have a significant amount of content to share.

Appendix B: Windows Update for Business and MDM policies

The following table lists the MDM policies configured on devices to provide an equivalent experience to the devices managed via group policy.

Policy	Setting
DeliveryOptimization\DODownloadmode	2
DeliveryOptimization\DOMinBatteryPercentageAllowedToUpload	60
DeliveryOptimization\DOMinFileSizeToCache	10
DeliveryOptimization\DOMaxCacheAge	604800
Update\EngagedRestartTransitionSchedule	2
Update\AutoRestartRequiredNotificationDismissal	2

Update\DeferFeatureUpdatePeriodInDays	0
Update\ScheduleImminentRestartWarning	15
Update\BranchReadinessLevel	16
Update\EngagedRestartDeadline	17
Update\ScheduleRestartWarning	2
Update\EngagedRestartSnoozeSchedule	2
Update\AllowAutoUpdate	6
Update\DeferQualityUpdatePeriodInDays	0
Update\AllowMUUpdateService	1

Compliance-deadline settings with grace periods are still being validated on Intune, so we are using engaged restart policies for Azure AD-joined devices.