

# Getting to Windows 10: Microsoft's new options for upgrading and onboarding

WHITE PAPER

## Table of Contents

<b>New security and management options in Windows 10</b> .....	1
<b>Keeping Windows 10 up to date</b> .....	2
<b>Upgrading existing devices</b> .....	3
<b>Enrolling new Windows 10 devices</b> ....	3

Windows 10 has a variety of new features, and many of them are similar to what we usually find in mobile devices. These enable new experiences for users, and for IT they provide new management choices and make Windows 10 more secure than previous versions.

Microsoft wants to make it as easy as possible for IT to embrace Windows 10, so they are providing new options to upgrade, onboard, and update devices.

## New security and management options in Windows 10

Windows 10 can be managed with mobile device management APIs, so that an MDM server can be used to configure basic settings like Wi-Fi, VPN access, email, and password policies, as well as push apps. But more important than what MDM can configure is how it happens—MDM is designed for devices that are mobile and not always on corporate networks. Management actions, policy enforcement, and remediation can all take place remotely and in real time. Modern MDM (like that which is included in Windows 10) also has awareness of and respect for the fact that devices can be used for both work and personal purposes at the same time.

SPONSORED BY



There are many new security features, but some of the most significant ones include Device Guard, a set of hardware and virtualization-based controls that ensure only trusted apps can run; and Enterprise Data Protection, a new form of work and personal-aware DLP.

Even though Windows 10 has all these new mobile-style features, it's important to know that they've all been implemented in ways that are still compatible with existing enterprise processes, experience, and user expectations:

First, Windows 10 retains compatibility for all applications from Windows 7, 8, and 8.1.

Windows 10 also has all of the familiar user interface elements needed for traditional laptops and desktops. The Start menu is still present, and touch-screen friendly elements only appear on devices that actually have touch screens. New Universal Windows Apps can be used on desktops and laptops, and they can appear in free-floating resizable windows (just like classic desktop applications) instead of taking up the whole screen.

While MDM is an option now, all of the previous Active Directory and agent-based client management techniques still apply, and customers can have a mix of both types of management in their environment. (In many cases MDM will likely be limited to a subset of devices.) The new MDM APIs are also usable even without a separate MDM platform—agent-based client management tools (such as Microsoft Configuration Manager) can access them via the WMI bridge.

Finally, these new features aren't limited to just tablets and other touchscreen devices—any Windows 10 device can take advantage of them.

The end result is that all of the new mobile and security elements of Windows 10 are useful and accessible in diverse scenarios.

## Keeping Windows 10 up to date

Windows 10 will further take on the mobile model by providing frequent updates—Microsoft refers to this as Windows as a Service (not to be confused with desktops as a service, the cloud-based VDI concept). Instead of monolithic, disruptive updates every few years, updates will be smaller and more frequent.

Most IT shops prefer to wait a while for updates to get their kinks worked out, and for this reason Microsoft will distribute updates to different constituencies at different times. They will go out to consumers first, where features can be validated at scale; this is known as the Current Branch for Consumers. After a few months, updates will be passed on to the Current Branch for Business. Even then, IT will still be able to manage exactly when devices are updated.

For mission critical devices, Microsoft is providing the Long Term Servicing Branch. This branch doesn't get new features; it just gets security patches. New versions with new features will be made available every one to three years.

Since Windows 10 will be updated regularly and relatively often, the corresponding management tools will have to be updated at the same pace. This isn't a problem for cloud-based MDM platforms—most vendors (including Microsoft Intune) are already used to updating many diverse APIs on a constant basis. However, this will be a challenge for traditional on-premises client management tools. To address this, Microsoft will also provide continuous and more frequent updates to the next version of Configuration Manager, corresponding to Windows 10 updates.

## Upgrading existing devices

Of course to take advantage of all these new features, companies need to get on Windows 10 in the first place. Many will move gradually, adopting Windows 10 as hardware is replaced. Windows 7 support doesn't end until 2020, so there's not a time crunch—even with a three or four-year replacement cycle, companies will be fine.

However, with all the new aspects of Windows 10—especially the security elements and Windows as a Service updates—Microsoft believes that companies will want to move at a faster pace.

One big problem with migration is that the last time many companies did it—going from Windows XP to 7—it was a huge amount of work. Since many companies skipped Windows Vista, IT departments weren't familiar with new changes like User Account Control or version 2 profiles. Companies had to find ways to analyze all of their applications and either rewrite problem apps or use compatibility shims from third-party vendors.

This just won't be the case going from Windows 7 to 10. There can always be exceptions, but generally older applications should be completely compatible. IT will have an easier time, so migrations will go much faster.

For the actual upgrade process, Microsoft is advocating in-place upgrades. These are faster and much less intrusive than a full refresh, and users' apps, configurations, and data all stay in place. The only thing that changes is that all of the sudden users have a new operating system with more features and better security.

This model will certainly be a departure for many companies that have typically done a full refresh and used it as an opportunity to do some housekeeping. Microsoft is helping this process by updating Configuration Manager to fully support all aspects of in-place upgrades from Windows 7, 8, and 8.1 to Windows 10.

Naturally it's still possible to do a full wipe and reinstall Windows 10 from scratch. This is also needed for more complex changes like switching languages, moving to 64 bit Windows, and changing administrator accounts.

## Enrolling new Windows 10 devices

For companies that are enrolling new devices instead of upgrading existing ones, there are several options.

In certain situations, (especially BYOD) Windows 10 devices will be candidates for MDM instead of traditional agent-based client management.

Conceptually, enrolling a Windows 10 device in MDM is just like any other mobile device. In return for submitting devices to management and security policies, users receive access to enterprise data. Windows 10 MDM also supports separation between work and personal data and apps. If a user chooses to unenroll their device or if the device is out of compliance, all access to enterprise data will be removed. Conversely, it's also possible for IT to remotely wipe enterprise data without deleting users' personal content. (MDM for Windows 10 will be covered in depth elsewhere in this series.)

Another way to onboard Windows 10 devices is through the new provisioning package concept. Instead of completely wiping and imaging a brand new device, a provisioning package can take a device with Windows 10 already installed and make all the changes necessary to turn it into an enterprise device.

Provisioning packages can configure settings, install applications, install documents and other data, customize the wallpaper and Start menu, and more. They can also automatically enroll a device in MDM or join it to a domain.

Provisioning packages can be distributed on USB drives or SD cards, sent via email, or downloaded from a network share. The provisioning process can take place outside of corporate networks or even without any internet connection at all.

Again, it's still possible to fully image new computers, but Microsoft is promoting provisioning packages as a faster, easier way to set up enterprise devices. Provisioning packages can also cover a wider variety of use cases. They can quickly make off the shelf computers into enterprise machines out in the field or they can be used for employee-owned devices. (Just like with MDM, removing a provisioning package from a personal device removes enterprise data access and returns it to its previous state.)