

MANAGING MICROSOFT WINDOWS 10

MDM APIs AND AGENT-BASED TECHNIQUES

WHAT CHANGES SHOULD YOU EXPECT?

Mobile device administrators have long had access to mobile device management (MDM) features that enable easy, secure management of Apple iOS and Google Android devices. Laptop and desktop administrators have had separate tools that rely on agent-based technology to deliver similar levels of security for PCs and Macs. Microsoft now offers application programming interfaces (APIs) built into Microsoft Windows 10 that allow you to manage laptops and desktops the same way you've managed smartphones and tablets for years.

TWO-THIRDS of Windows 10 PCs and tablets are expected to be managed via unified endpoint management (UEM) platforms by 2019.¹



HERE'S WHAT IT AND SECURITY LEADERS NEED TO KNOW

If you're migrating to Windows 10 while still supporting legacy systems...

Windows 10 is now the Microsoft operating system (OS) of choice, and organizations that haven't yet migrated are expected to make the move soon. But as you transition your laptops and desktops, you also need to support legacy systems such as Microsoft Windows 7 until the migration is complete.

IBM® MaaS360® with Watson™ offers a combination of traditional client management and modern API management that can enable you to manage all Windows devices in one place. For example, you can manage a Windows 10 laptop by using the Windows MDM APIs for lock, locate and wipe while having a MaaS360 agent on the laptop for patching and software management.

- Manage devices with both client management tools and MDM APIs
- Streamline deployment by shipping hardware running Windows 10 to users without requiring up-front custom imaging
- Maintain systems without touching them—and roll out over-the-air (OTA) updates to security and networking configurations
- Consolidate post-deployment management of Windows 10 and legacy systems
- Integrate with Microsoft stores for new applications (apps) while using MaaS360 to distribute legacy software, such as Win32 apps

If you need one simplified solution to manage and deliver MDM/EMM/UEM...

With MaaS360, you can manage all major OSs, including Windows 10, Apple macOS, iOS and Android. The UEM solution spans OSs, devices, apps and data.

- Enroll devices OTA
- Provision Wi-Fi profiles, email and corporate apps automatically
- Deploy a unified application catalog for Windows, iOS, macOS and Android
- Manage inventory of hardware and software, apps, patching and updates

53% of global enterprise infrastructure decision makers surveyed say **SECURITY AND PRIVACY** is a key reason for upgrading to Windows 10.²



If you need to deliver consistent security across all device types and OSs...

Many Windows-based security and management functions that were only supported by group policy objects (GPOs) have API support, bridging the management gap that once existed.

With MaaS360, you can leverage Windows 10 APIs to establish the same device and app security policies across laptops and desktops as you have for smartphones and tablets.

- Enforce encryption for OSs and apps
- Locate, lock or wipe devices remotely and in real time
- Configure passcodes and other security policies, whitelist or blacklist apps, and institute Windows Information Protection (WIP) for data loss prevention

If your mobile and endpoint administrator roles are being consolidated...

In the past, the mobile administrators or mail administrators oversaw management for mobile devices, while laptops and desktops were largely supported by end-user computing groups.

The IT teams that separately managed laptops and mobile devices are now starting to come together.

MaaS360 UEM gives this consolidated team a single platform that provides visibility and control across all endpoints and end users without numerous point solutions.

Technology convergence is changing the way you manage endpoints

See how easy it is to manage laptops, desktops, smartphones, tablets, wearables and Internet-of-Things (IoT) devices, along with their data and apps—all from a single management console.

Try MaaS360

at no cost for 30 days, and learn how you can simplify your Windows 10 migration.



© Copyright IBM Corporation 2018. All Rights Reserved. IBM, the IBM logo, ibm.com, and MaaS360 are trademarks or registered trademarks of International Business Machines Corporation in the United States. Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

¹ "IDC FutureScape: Worldwide Mobility 2018 Predictions," IDC, October 2017.

² "Windows 10 Finally Delivers on Microsoft's Security Promises," Forrester, October 20, 2017.