Windows 10 and mobile device management

Jack Madden, TechTarget

WHITE PAPER

Table of Contents

Windows 10 has many mobile-style features. For enterprise IT, the most important of these are new security features and a new way to manage devices—using mobile device management (MDM) APIs—as another option besides tradition agent-based client management.

MDM won't be used for all Windows 10 devices, and traditional management techniques will be around for a long time. However, almost all devices will get some utility out of the new management options, and for a subset of devices, they will be revolutionary.

SPONSORED BY

Microsoft

TechTarget® Custom Media

A TECHTARGET WHITE PAPER

MDM concepts

Supporting MDM means that a device has well-documented APIs to control settings and perform management tasks, integrated directly into the operating system itself. The APIs can interface with a standard management protocol, so that MDM servers can easily use device settings, queries, and other factors to build policies.

It may appear that MDM APIs provide fewer options than traditional management, but in MDM contexts certain restraints and assumptions in place. For example, apps can only interact with each other and with the OS in limited, defined ways, and the OS has built-in hardware-based security features to ensure its integrity. Under these conditions, fewer management controls are needed.

Because modern devices are so "mobile," MDM is designed to work remotely, over the internet. There's no need for a device to be on a corporate network or reboot for changes to take effect. Instead, MDM happens real time, and policies can respond instantly to changing conditions.

In the last few years, MDM has also evolved to accommodate the concept that devices (of all types) are used for both work and personal purposes. MDM APIs can have granular control over individual applications and data stores, ensuring that corporate assets are managed and secured as needed. Personal data privacy is respected, and BYOD can be enabled by limiting the scope of management actions (including remotely wiping data) to just enterprise apps and data.

MDM features in Windows 10

All of these modern MDM concepts are built in to Windows 10 (and some of them are available in Windows 8.1, as well). For example, Windows 10 features Device Guard, a set of hardware and virtualization-based controls that ensure only trusted apps can run.

Newer Windows apps—Universal Windows Platform apps, which come from the Windows Store and are packaged in .appx files—can be installed and removed cleanly and quickly. They use the Windows Runtime API (as well as some Win32 APIs and the .NET Framework on some devices) and have limited access to sensitive device features.

On a device-wide basis, MDM for Windows 10 can control basic security features such as passcode policy, remote lock/wipe/password reset, manage OS updates, set encryption policies, and restrict device features as needed. MDM can enable corporate access by configuring Wi-Fi, email accounts, VPNs, and installing certificates. MDM servers can query devices for information about hardware, current status, location, app inventory, and security posture (using the Windows Health Attestation Service and other security-related queries). Both custom and publicly-available apps can me installed and removed.

To accommodate dual work and personal usage, Windows 10 has a set of DLP controls called Enterprise Data Protection. Enterprise Data Protection can designate which apps and other data sources are considered to be enterprise assets, and then encrypt them, control how data is shared, and limit them to a VPN.

The great news is that all of these features apply no matter what type of device is used. Many people associate MDM with just phones and tablets, but Windows 10 MDM works for all types of devices, including regular non-

touchscreen laptops. In addition, Windows 10 Mobile devices (i.e. phones) are managed with the exact same concepts and most of the same specific policies.

The overall concept of MDM configuration is that it can turn any device—even a new device off the shelf from a retail outlet—into an enterprise-ready machine without the need to fully image it or connect it to a corporate network. All that is required is a simple enrollment and configuration process.

How Windows 10 devices are enrolled in MDM

Windows 10 devices can be enrolled directly to an MDM server through the user interface. MDM supports auto-enroll, or users can enter the server address manually. The server will authenticate users and then enroll the device, configure it to enterprise standards, and begin ongoing policy enforcement using a combination of device queries and configuration changes.

Another way to bring a device into MDM is by joining it to Azure Active Directory. Azure AD acts as an identity and access management service and can give users single sign on access to applications. When a device is joined to Azure AD, conditional access polices can require it to be enrolled in MDM automatically.

For bulk or offline enrollment, a new concept called provisioning packages can be used. Provisioning packages can be downloaded to a device or installed from removable media; the package then enrolls the device and can also install enterprise apps and data.

Unenrolling a device—whether initiated by the user or by IT—safely removes all enterprise accounts, apps, and data. With MDM, there is much less of a chance that corporate data can be lost.

Flexibility for different use cases

Windows 10 MDM features and enrollment options are flexible enough to cover a variety of use cases.

For BYOD, users can enroll their device in MDM or join it to Azure AD at any time. IT can apply MDM policies that ensure personal data is not affected by management.

Dual work and personal usage often happens on enterprise-owned devices, too. When officially sanctioned, this is called COPE (corporate-owned, personally-enabled). MDM policies like Enterprise Data Protection are useful in this situation.

Another new MDM use case that Microsoft is promoting is the “out of box experience.” Users can take a brand new device from a retail outlet, and provision it using the Azure Active Directory join and automatic MDM enrollment process described previously.

For shared devices or other non-personalized devices that function as kiosks, embedded devices, or point of sale terminals, Windows 10 MDM has enough control to completely lock down the experience if needed. Besides all of the MDM policies already described, MDM can set wallpapers, configure the Start menu, limit devices to a single app mode, and prevent unenrollment.

How to decide when to use MDM

MDM is obviously a huge change from agent-based client management. For companies that rely heavily on complex desktop apps, it may not be suitable. Windows 10 MDM can push out very basic, well-written MSIs, but otherwise it's generally limited to managing Universal Windows Apps.

For organizations that use mostly cloud apps, accessed through the web or available from the Windows Store, then MDM becomes more attractive. Even companies that aren't at this point yet may still be considering them already, in service of the smartphones and tablets that have been proliferating for the last several years. Writing and sourcing new apps, modernizing old apps, using app transformation technologies, and remote desktop technologies could all serve to make MDM a viable option.

Even if MDM is not workable for all devices, it could be a good option for road warriors who mostly just need Office and web apps.

Or MDM could be accommodate personal Windows devices (perhaps as an alternative to other remote access technologies). IT admins have been weary of managing personal computers in the past (after all, who wants to let a user with who-knows-what come in and put it on the corporate network) but Windows 10 is completely different. With all of the mobile-like features and the conditional controls (including the Health Attestation Service), saying yes to personal Windows 10 devices is like saying yes to any other mobile device.

MDM servers and Microsoft System Center Configuration Manager

All of the MDM options described so far have referred to the role of MDM servers in a general way, but naturally there are many different options.

There are many MDM server products, and Microsoft offers Intune, which can be used alone or as an extension of System Center Configuration Manager.

Companies may want to take advantage of Windows 10 MDM APIs even for traditional domain-joined devices. In this situation, the Configuration Manager agent can interact with Windows 10 MDM APIs via the WMI Bridge.

It's also possible that a device may be domain-joined and managed while at the same time also enrolled in a separate MDM service. If there are any conflicts, the device will default to the more secure policy. (It's also possible for companies to prevent this from happening by blocking MDM enrollment through Group Policy.)

Configuration Manager can also act as an MDM server on its own, connecting directly to MDM APIs for on-premises devices only. This is intended for devices that have limited or no access to the internet for security and compliance reasons.

Conclusion

MDM isn't just a process for personal tablets and phones anymore—it's a whole new way of thinking about all devices and apps, and it can be useful tool for many different use cases.