Considerations in Deciding How to Manage Windows Devices

IT has fundamentally shifted in recent years. The days are long gone when employees worked almost exclusively on corporate-owned PCs running Windows* that are joined to an Active Directory Domain Services* (AD DS) domain. Now, many users in an organization—especially executives—expect to be able to connect to corporate resources wherever they are from their Apple iPhone* and iPad* devices or from Android* devices to get work done.

More recently, there's been a new development: Windows 8 has brought a touch-based operating system to desktops and laptops equipped with touch screens. Energy-saving innovations in 4th generation Intel® Core™ processors and Intel® Atom™ processors, meanwhile, have increased battery life and made PCs more attractive as mobile devices.

Fan-less tablets, made possible by energy-efficient 4th generation Intel Core processors and Intel Atom processors, have also given workers a truly mobile experience while running a full version of Windows. Now, enhancements in Windows 8.1 and Windows Server 2012 R2* offer the possibility of a different management model for Windows 8.1 PCs.

Thanks to Windows 8.1, for the first time, it's possible to manage devices running Windows through enterprise mobile management software instead of through traditional methods. This new option begs the question: How do you decide which management path to take?
Traditional Management

In traditional PC management, IT has full control of the devices, from procurement to retirement. The organization purchases and receives the devices directly from OEMs. Typically, IT replaces the OEM image on each device with custom images that are optimized for their environment, then sends the devices to their respective users.

After the devices are in users’ hands, IT is still responsible for updating, securing, and maintaining the images. This is done by joining the devices to an AD DS domain and applying Group Policy Objects and using a tool like Microsoft System Center Configuration Manager to perform management tasks, such as hardware and software inventories, deploying applications, applying patches, and managing compliance settings. Other typical agents that IT manages are for antivirus, backup, and encryption.

For this type of management to work, the devices should be connected to the corporate network a majority of the time. Remote devices or laptops achieve this with VPN connections.

The biggest benefit of traditional management is the high degree of control, stability, and security that you can bring to each user’s environment. This lets IT give users virtually unfettered access to internal corporate resources from these devices.

Factors Favoring Traditional PC Management of Windows 8.1 Mobile Devices

Factors Favoring Mobile Management of Windows 8.1 Mobile Devices

How Will the Device Be Used?

Enhancements in Windows 8.1* and Windows Server 2012 R2*
Whereas traditional PC management is fully controlled by IT, the end-user has much more responsibility in the mobile management paradigm. By far, the main business usage for mobile devices is corporate email, calendar, and contacts. Mobile device management (MDM) is largely an attempt to provide corporate email, calendar, and contacts in a secure manner (that is, while protecting corporate data) with the least impact on user experience. Mobile management also entails application deployment and management, but email is the most common use case.

The life cycle of a mobile device is typically very different from the life cycle of a traditionally managed, corporate-issued PC. Foremost, the user purchases the device and receives it, not IT. Even if IT purchases it, it is still sent directly to the user. The user then enrolls the device over the air to a management service, typically an MDM server that is hosted on-premises or in the cloud. The management service then configures the device according to IT policy. Possible configurations include password policies, device restrictions, certificate provisioning, WiFi, VPN, and encryption.

Mobile management moves many management responsibilities from IT to the user with the user having ultimate control over the device. For example, users control when their devices get patched or upgraded to a new operating system (and these upgrades happen rather simply). Users also install most of their own applications and have to approve the installation of applications that are pushed by IT.

This contrasts sharply with traditional PC management, where IT controls patch deployment, operating system upgrades, application deployments, and everything else. Other differences between mobile management and traditional PC management are that MDM solutions have limited visibility into users’ personal data on mobile devices and users can easily un-enroll mobile devices from management, after which the devices will return to the same state they were in before enrollment.

**Windows 8.1 and Mobile Management**

The combination of a touch-based operating system like Windows 8.1, long battery life, and thin and light form factors makes Ultrabook™ devices, tablets, and 2 in 1 devices powered by 4th generation Intel Core and Intel Atom processors true mobile devices. Windows 8.1 devices powered by Intel processors can be managed by using traditional PC management or mobile management methods. Windows 8.1 adds mobile device management capabilities to the device through a built-in Open Mobile Alliance Device Management (OMA DM) agent and MDM APIs. Windows Server 2012 R2 includes a host of features that work together with Windows 8.1 to give more access to corporate data securely to non-domain-joined devices.

Despite the benefits of the traditional management paradigm, there are some good reasons not to join devices running Windows—such as 2 in 1 devices, Ultrabook devices, or tablets—to a corporate domain, even when you can. The bring-your-own-device (BYOD) scenario provides the most obvious example: if users bring their own personal mobile devices to work, the very suggestion of joining AD DS can be a non-starter. Employees naturally can be hesitant to cede control of their personal devices to their employer.

The new mobile management features in Windows 8.1 and Windows Server 2012 R2 enable non-domain-joined devices to have selective access to corporate resources depending on the amount of control IT has over the devices (and IT’s risk tolerance). This management alternative is often used to let employees access workplace resources from their personal devices, but it can be used to support company-owned devices as well.

Enterprise mobile management solutions that support the Windows 8.1 MDM APIs include AirWatch®, with other solutions coming to market in the future.

**Benefits**

As with traditional management, mobile management has its own set of benefits, primarily that it enables workers to access corporate resources and be productive on mobile devices while still maintaining policy-based control. This benefit is made possible by new features in Windows 8.1 and Windows Server 2012 R2. (For a summary of these features, see “Enhancements in Windows 8.1* and Windows Server 2012 R2*.”)

**Benefits of Mobile Management**

For devices that are not domain-joined or image-managed by IT, mobile management provides these benefits:

- IT has some policy-based control over devices that are not joined to the corporate domain.
- IT does not have to worry about physical device deployment logistics in a BYOD scenario.
- IT can deploy corporate apps to non-domain-joined devices.
- IT can implement data-leakage controls to protect corporate data on mobile devices.
- IT can remotely configure and secure devices over the air, to help ensure that devices are compliant with IT security policies.
- Devices can be granted or denied access to resources based on user and security policy compliance.
- All corporate data and configuration settings can be remotely wiped from lost or retired devices, while personal data and applications remain intact.
- Mobile management might decrease the need for VPN connections; VPN connections might drain device battery more quickly.
Factors Favoring Traditional PC Management of Windows 8.1 Mobile Devices

There are no hard-and-fast rules about which management method to use. In general, the following factors tend to favor treating mobile devices running Windows as PCs:

- The company owns the device.
- The device is used mostly while connected to the corporate network.
- Employees other than the primary user occasionally need access to the device.
- The user needs broad access to corporate resources from the device.
- The device is the user’s primary PC.
- IT needs to deploy desktop applications to the device.
- Users need to access resources, such as printers without near field communication (NFC), on company premises.

Factors Favoring Mobile Management of Windows 8.1 Mobile Devices

In general, the following factors tend to favor managing devices running Windows using mobile management:

- The user owns the device running Windows (as in a BYOD scenario) or is corporate-owned but personally enabled (COPE).
- The device is most often used while not connected to the corporate network.
- No other employees need to use the device.
- The user can live with limited access to corporate resources.
- The device will be used in remote locations or satellite offices without a VPN server nearby (or without reliable corporate connectivity).
- The device requires light, infrequent connectivity to the corporate network.
- The device is not the user’s primary device but a secondary or tertiary companion device.
- IT does not need to deploy large updates to the device.
- IT is not responsible for the image loaded on the device. Users can get the majority of their applications from an app store.
- User experience, such as battery-life drain due to extensive VPN usage, might be adversely affected by traditional management of the device.

How Will the Device Be Used?

Windows 8.1 and Windows Server 2012 R2 introduce features that provide IT departments with greater flexibility. Now, IT can choose to manage Windows 8.1 client devices either as PCs through AD DS or as mobile devices through enterprise mobility management software.

Employee-owned Windows 8.1 devices are natural candidates for mobile management, but IT departments might find it advantageous to manage even certain company-owned Windows 8.1 PCs, Ultrabook devices, tablets, and 2 in 1 devices as mobile devices, such as those used by frequently traveling sales staff that rarely connect to the corporate network.

When you are making your decision about how to manage a particular Windows 8.1 device, one of the most important factors to consider is how often the device is used in a mobile setting outside of the corporate network. Companion devices with touch interfaces and wireless capabilities that run Windows 8.1 can be good candidates for mobile management. Factors favoring traditional AD DS management include the device being used most often while connected to the corporate network, the device requiring broad access to corporate resources, a need for the user to access company printers without NFC enabled from the device, and a need for other employees to sign on to the device. You might want to do your own testing on your networks to decide what balance of performance, usability, and security is acceptable for different devices in your organization.

For more information on Ultrabook devices, tablets, and 2 in 1 devices powered by Intel Core processors and Intel Atom processors, visit:

www.intel.com/tabletforbusiness
www.intel.com/ultrabookforbusiness
Enhancements in Windows 8.1* and Windows Server 2012 R2*
Windows 8.1* and Windows Server 2012 R2* introduce many new features (such as Workplace Join and Web Application Proxy) that make mobile management more attractive as a PC management option. Taken together, these enhancements can help securely provide access to more internal resources for users working outside a company network on non-domain-joined devices.

Remote Business Data Removal
Data on a mobile device running Windows 8.1 can be marked as personal or work related. Using mobility management software, you can remotely wipe only the corporate data and leave a user’s personal data intact if a device is un-enrolled or lost.

Open Mobile Alliance Device Management (OMA DM)
Windows 8.1 devices come preloaded with an open-standards-based mobile device management (MDM) client, enabling third-party applications to perform basic management of settings, software distribution, inventory, device enrollment, and remote data wipe of Windows 8.1 devices. An important benefit of including this device in Windows 8.1 is ease of management. You can manage Windows 8.1 devices with mobility management software from many different vendors, and you don’t have to first install a management client on the device.

Workplace Join
Workplace Join offers users’ devices a middle management ground between being joined to the domain and not being joined. Through Workplace Join, devices are registered in AD DS*, but they don’t have full computer accounts. This new medium level of security lets IT control access to corporate resources based on user identity, the device from which the user is connecting, and the network location. However, IT does not have any control over, or access to, the user’s device.

Single Sign-On (SSO)
Users working on devices not joined to the domain can now gain access to corporate file resources after providing credentials only once.

Work Folders
Work Folders are synchronized folders that store a user’s personal work files. The main copy is located in the company’s data center, but the folder can be synchronized on any device connected to the Internet (BYOD or not) and running Windows 8.1. This feature makes personal work folders readily available to users anywhere.

Web Application Proxy
Web Application Proxy is a server role that provides users outside the company network with access to select applications running on internal servers.

Near Field Communication (NFC) Tap-to-Pair Printing
Printing has been one of the pain points for users working on non-domain-joined devices when they visit the company network. NFC tap-to-pair printing addresses this problem for NFC-capable printers and devices. With this feature, you can install a printer and its drivers on a device that is not domain-joined simply by tapping the device on the physical printer.