ivanti

Five Reasons You Need User Workspace Management More than Ever with Windows 10

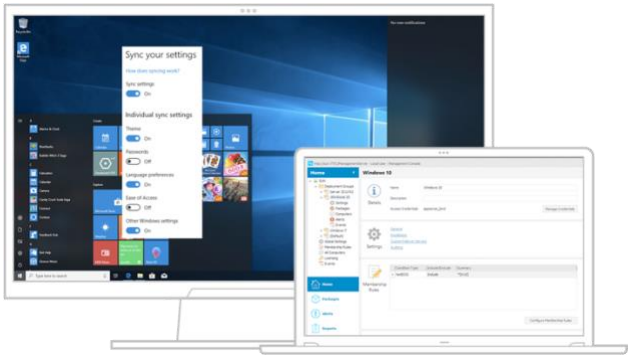
As more enterprise-level features are added to Windows 10, it's time to ask the question whether you still need third-party solutions to enhance the user experience and protect your endpoints? Here are five things to consider:

1. Is Personalization Free?

Windows 10 has a built-in "Sync your settings" feature that suggests at first glance that it provides personalization "built in". Its goal is that, as a user roams between computers, their desktop and application settings roam with them. It provides some basic control on which settings follow the user.

This is a great feature for consumers, because these settings are synced to the Microsoft cloud using your Microsoft account. Whenever you sign onto a new Windows 10 device using that Microsoft account, many of your key settings will be synchronized automatically. In the enterprise, however, it's a little more complicated. If you only use on-premises Active Directory you can federate and sync a Microsoft account through ADFS and use "Sync your settings". This is disabled if you're using Azure AD, and you must use Enterprise State Roaming, which is very similar but stores settings with your corporate account in Azure AD. All of this presents problems for IT.

First, if you are using on-premises AD and syncing to a Microsoft account for each user, then sensitive info like passwords are now stored outside of your control, which might have security, privacy, and regulatory implications, especially with the introduction of GDPR. If a user leaves the company, they keep their Microsoft account. This problem is avoided with Enterprise State Roaming, but that requires you to have an Azure AD Premium subscription, which costs extra.



Second, both syncing to a Microsoft account and Enterprise State Roaming only apply to the rare breed of Universal Windows Platform (UWP) apps, aka Modern apps, Windows Store apps, Metro apps, and even WinRT apps. There are an increasing number of them built into Windows 10—Edge, Calculator, Sticky Notes, and even the Start Menu—but 99% of the apps that are used in the enterprise are based on the Win32 API, and "Sync your settings" won't help you with those.

Third, even for UWP apps, it requires that the app developer choose to store their settings in the Microsoft Cloud using this method, and if the desired setting isn't included, there's no way to add it without a third-party solution.

Office 365 has a separate roaming-settings feature that captures select Office settings in the Microsoft cloud, but documentation is limited and has not been updated for Office 2016. Like Windows 10 "sync settings", it requires use of a Microsoft Account or Azure AD account and there is no control over which settings are stored, and there is no rollback or archive control. It also cannot be extended to any other Win32 applications.

This is where third-party solutions are as valuable as ever: total, flexible coverage of all Windows desktop and application settings, with complete IT control and data privacy.

2. Security at the Endpoint

Windows 10 is the most secure version of Windows ever, and technologies like Device Guard (aka Windows Defender Application Control Configurable Code Integrity and Virtualization-based security) and Credential Guard offer new ways to protect against traditional attacks. Both are actually collections of technologies and, at its most extreme, you could use Device Guard to turn your PCs into something resembling a phone or Apple/Android-style tablet, only able to run apps from the Windows Store or those that have been explicitly sanctioned by IT by creating signatures for them (which, by the way, need recreating every time the app changes). In other words, the full version of Device Guard is an extreme form of application execution control, preventing unwanted executables from running, but also making it very hard to run your existing estate of Line-of-Business apps, and requiring IT overhead every time one of them changes.

Another approach Microsoft has recommended is to convert existing Win32 apps into a UWP app (using Desktop Bridge) so that the apps run without administrator privilege and can be wrapped and protected. Unfortunately, the conversion process is not straightforward and almost always requires code changes to the Win32 app, something that isn't possible with older apps or those from external vendors. Device Guard has subsequently been adjusted into more of a marketing term to cover a range of technologies under the Windows Defender brand.

Credential Guard secures the LSA (Local Security Authority) Windows subsystem in a hardware-protected Hyper-V virtual machine. Of course, it comes with demanding hardware requirements, and could cause third-party apps that interact with the LSA to break until they are updated for Windows 10, but it is a useful security feature and thwarts numerous attack vectors.

Third-party vendors still provide far easier management of problems like user privilege elevation and local administrator control, browser and application network access, as well as more flexible application execution control using file metadata and other pattern-matching capabilities, so that there's no IT overhead every time an app goes through a minor update. The Windows 10 features discussed above do not erode the value of these solutions.

3. Data Storage

OneDrive is wonderful for the consumer, and Windows 10 and Office 365 take integration with OneDrive to new levels of ease. OneDrive for Business gives IT more control over user files and folders synced to the Microsoft cloud, but many organizations still require that user data be kept within their own devices and data center. Where on-premises storage is a necessity, and Offline Folders is not good enough, then third-party solutions allow selective sync, granular control over file types and background transfers, complete auditing of file distribution, and the same cross-platform access benefits of OneDrive.

Where storage of user files in the cloud is acceptable to an organization, Office 365 provides 1TB of storage for each user, but it's managed outside the visibility of IT. There's no easy way for IT to audit file access, set policy on the types of files that are synced and stored, or to control access to a mix of on-premises and cloud storage. Again, this is still an area where a third-party broker can deliver a seamless user experience, take advantage of Office 365's 1TB of storage per user, and keep IT firmly in control.

4. Migration and Roaming between Windows 7 and 10, and between Windows Server 2008 and 2016

Most organizations skipped Windows 8 and 8.1, and because of the Windows 8-style desktop experience, many also skipped 2012 and 2012 R2 for RDSH/XenApp/Terminal Server deployments. With support for Windows 7 due to end in 2020, we are finally seeing an acceleration in the adoption of Windows 10 in the enterprise. In addition, users expect the Windows 10 experience from shared virtual desktops and sessions, so a move to Windows Server 2016 is required—often in conjunction with an upgrade to Citrix XenApp.

That said, over 30% of business desktops are still on Windows 7, which means there will be users moving back and forth between version 2 (Windows 7) and version 5 (early Windows 10 and 2016) and version 6 (later Windows 10 and

2016) profiles, not to mention x86 and x64 CPU architectures. Roaming profiles out-of-the-box with Windows just won't handle that. Without a third-party tool that enables roaming between profile versions, users won't get a clean experience.

5. How Will You Track Adoption?

Can you tell who on your domain is using Windows 10? You already know about the managed devices where you intentionally deployed it, but what about all those BYOD and COPE devices that people brought onto the network? You might be able to get something out of Active Directory tools, but agentless discovery of what's on the network is still the domain of third parties. As you would expect, Ivanti offers a range of tools to track not only which devices are on Windows 10, but also which license version, build, and device type, and can produce interactive dashboards, alerts, and reports as your migration project progresses. Check out the Ivanti website for more information on Windows 10 migration solutions.

Summary

Windows 10 contains many great features and enhancements, but in enterprises of any size where IT wants to control and protect the user security and experience, third-party solutions are still essential for:

1. Roaming and recovery of desktop and application settings
2. Application control and least privilege security
3. Data sync and recovery
4. Roaming between Windows 10/2016 and earlier Windows versions
5. Tracking adoption and spread of Windows 10

Learn More


ivanti.com


1 800 982 2130


sales@ivanti.com