Top 10 Tips for Windows 10 Migration

According to a recent global study by Dimensional Research, 37% of IT organizations plan to fully migrate to Windows 10 within the next year, 35% within the next two years, and 14% have not established a migration timeline. If your organization fits into one of these categories, this document consolidates our experience gained from working with customers on their OS migrations.

Tip #1 Pick the Right Branch

With Windows 10, Microsoft has introduced a far more frequent update cadence to ensure Windows 10 endpoints remain up to date. However, this rolling upgrade practice offers alternative options for different lengths of servicing windows, namely “branches”, which dictate when feature updates are made available to endpoints.

The two key branching options are Current Branch for Business (CBB) and the Long-Term Servicing Branch (LTSB).

Endpoints that employ CBB will receive two major updates per year, while endpoints that use LTSB will receive major feature updates infrequently, perhaps every two years. In addition, Microsoft has removed many of the non-essential, built-in CBB features from LTSB branch—such as Windows Store Apps, Cortana, and Microsoft Edge—and is aimed at supporting systems for critical functions like healthcare or air traffic control.

Consider your service window and system uptime requirements when determining which branch you plan to use. However, 95% of businesses should select CBB in order to benefit from increased security and feature updates.

Tip #2 Pick an OS Deployment Strategy

There are several device-related caveats to consider when undertaking a desktop migration project. First, some devices just won’t support Windows 10. Since late 2016, PCs no longer ship with Windows 7 pre-installed, and most modern processors will only be supported on Windows 10. So, do you replace, re-image, or upgrade your existing endpoints?

Second, independent research confirms that the biggest driver for early Windows 10 adoption is the “stealth IT migration” issue, where IT departments allow users to employ new devices that come pre-installed with Windows 10, even though they’re not officially supported by the business.

The recent Dimensional Research survey referenced above showed that there is no single best approach to Windows 10 migration being adopted. Of those surveyed, 52% planned on re-imaging existing endpoints using systems management tools, while 49% were looking at hardware migration, i.e. upgrading to Windows 10 as new devices are deployed. However, by timing computer replacement strategically to coincide with an OS migration, organizations may save time and costs associated with in-place upgrades.

Tip #3: Don't Let Applications be a Barrier to Migration

One of the largest obstacles facing organizations when migrating to Windows 10 are worries about application compatibility.

Happily, there are now many alternative application-delivery platforms that allow apps to be integrated smoothly into your desktop environment via virtualization, layering, or streaming technologies. By separating applications from the underlying OS, these technologies can alleviate application compatibility problems when using new operating systems like Windows 10.

So, when choosing your application delivery method, ask yourself these questions to help determine the approach that best fits the needs of you and your users:

- Will my users need access to applications offline?
- What privileges will users need to run these apps?
- How do I license these apps?
- How will my IT department handle upgrades?
- Given the above criteria, what approach will be most cost-effective for my organization?

You also need to consider Web applications. If your in-house web apps currently run without issue on IE9 in compatibility mode, or only with a specific version of Java, what will happen when you migrate to IE11 or Microsoft Edge? Do you redevelop your internal web applications, or do you virtualize them to continue support, which could be costly and time consuming? Alternatively, in order to solve compatibility issues, do you install multiple browsers (e.g. Chrome, Firefox, etc.), which are difficult to manage and can lead to security concerns?

Ivanti recommends re-testing your most critical line of business applications on Windows 10 before migration, with a specific emphasis on applications that require administrative rights to run.

Tip #4: Create the Ultimate User Experience

End user acceptance of a new workspace starts at logon. If the first logon is slow, user acceptance of the new workspace will be less-than-stellar from day one. And, with every slow logon and every slow-running, frozen, or unavailable application, etc., user acceptance—and productivity—will diminish.

To optimize usability and user acceptance of a new workspace, Ivanti recommends running analytics to evaluate user experience on the new workspace. You should baseline existing environments and record metrics such as logon times, memory and CPU utilization, application usage, and privileges needed to run resources. It's also prudent to ascertain how and where users are storing their data—which is crucial to ensure a good user experience, both during and after migration.

This exercise will allow you to pre-empt potential bottlenecks or resource hogs that could affect quality of service in your new environment. It will also help you understand license requirements and identify users with unnecessary and insecure privileges.

Tip #5: Personalize Your Users Workspace

In a recent Dimensional Research survey, over 90% of users surveyed expressed emotions ranging from annoyance to despair when asked for their reactions to changes on their desktop. The survey also revealed that 32% of users are already confused by the Windows 10 interface. If, after migration to Windows

10, users' personal settings are missing, it's inevitable that user acceptance of a newly-delivered Windows 10 workspace will be negatively affected.

To avoid this scenario, you could continue to support users on older operating systems and hardware. However, if those users also need new hardware running Windows 10, you'll have issues. Why? Windows 10 introduces an additional roaming profile architecture that makes it even more difficult to persist user settings when users switch between different devices and platforms.

In contrast, if a user logs onto their new (and dreaded) Windows 10 workspace and finds their familiar settings already in place, you'll minimize their fear of the unknown, increase user acceptance, and eliminate the need to continue supporting older versions of Windows.

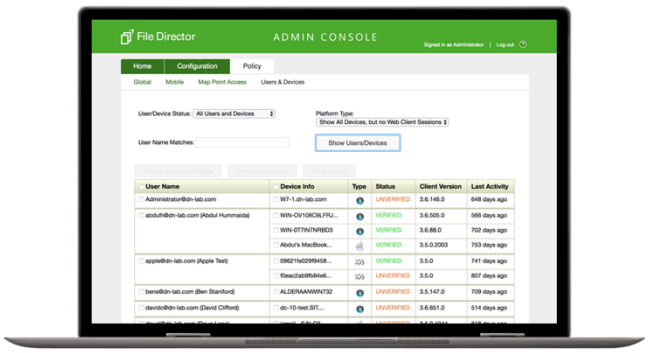
To persist user settings post-migration, you'll need to capture and manage user personalization independently from the underlying operating system and applications, which ensures that personal settings are always available, irrespective of which device or platform your users log on to.

Tip #6: Provide Users With Access to Their Data

One of the greatest challenges associated with providing new Windows 10 endpoints is how to migrate files and folders stored locally on the user's old device. In this situation, how does IT ensure both corporate and personal files are securely backed up and can be effortlessly migrated to new devices? It's also difficult for IT to establish how many local files exist in order to determine the best way to migrate them.

Storing user files and folders on file shares or home drives in the data center is another challenge for IT and end users. If users are working remotely or offline, they may not be able to access their files stored in the data center. If they have remote access to on-premises file shares, use of a VPN is typically required. This can frustrate users and adds another layer of security and complexity that causes headaches for IT in terms of break/fix, migrations, and upgrades.

Ivanti® File Director, powered by AppSense, enables effortless migration of user data, no matter where it resides. With File Director, user-file and folder migration becomes a simple, stress-free task that, once initiated, means IT is prepared instantly for any future migration projects. In addition, the data migration process is 100% unobtrusive to users.



Tip #7: Ensure Windows and Applications are Fully Patched

With ransomware attacks and other types of malicious outbreaks on the rise, it's becoming difficult for organizations to satisfy compliance mandates while protecting against new and more intelligent threats.

Social engineering tactics use deceptive techniques to manipulate users into performing non-secure actions or divulging private information. A lot of these targeted attacks look for vulnerabilities and weaknesses in OS and application content, typically due to unpatched operating systems and applications.

A comprehensive patch management solution can protect your entire Windows 10 estate without disrupting business continuity by detecting vulnerabilities in both your Windows 10 endpoints and installed applications.

Tip #8: Stop Malicious or Unlicensed Applications

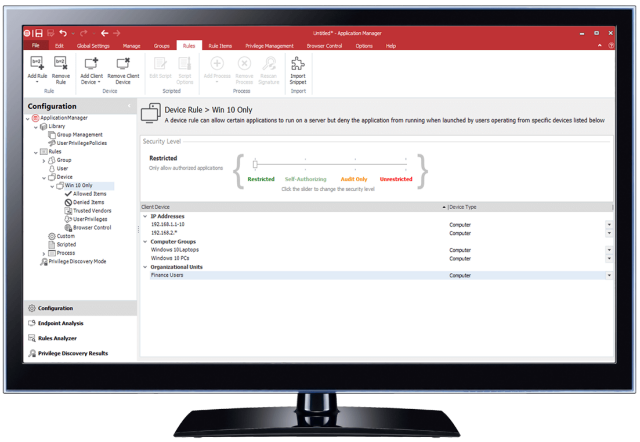
Will your users be employing Windows 10 Store apps? If so, how will you control which apps they can access, install, or run? You could encounter

productivity, compliance, and security issues without some form of application control.

However, it's not just Windows Store apps you need to control, but traditional Windows apps as well. With more users employing multiple devices to do their work, controlling software license usage is an increasingly critical IT role.

Additionally, if users can introduce unlicensed software, ransomware, or other malicious executables, they can compromise the security and compliance of your existing desktop estate. Do you want this happening in their new, pristine Windows 10 workspace?

Traditional whitelisting and blacklisting technologies typically require ongoing maintenance when new service packs or upgrades are released, or when new, unknown malware is propagated. This can increase IT support costs. In addition, these types of solutions are often easily bypassed by renaming unknown or blacklisted applications as an application on the whitelist.



Ivanti® Application Control, powered by AppSense, uses a Trusted Ownership™ model, where any application installed by a non-trusted owner, i.e. a standard user, is blocked automatically from being installed or executed. This protects your environment from zero-day threats and eliminates the problem of out-of-date reactive solutions such as antivirus software, which must know about a threat before update definitions can be downloaded and applied.

For controlling traditional Windows apps, Application Control is recognized by Microsoft for enforcing device-based software license control. By controlling which users or devices have permission to run named applications, limits can be placed on the number of application instances, which devices or users can run the application, when users can run a program, and for how long.

Tip #9: Remove Admin Privileges from Users

Providing users with full admin rights can leave endpoints vulnerable to attack. This can significantly increase security and manageability costs, decrease productivity, create legal and liability issues, and make compliance elusive. Out of the 20 items on its list of Critical Security Controls, the Center for Internet Security ranks "controlled use of administrative privileges" at number 5.

But how do you maintain user productivity without giving users the keys to the kingdom?

By applying privilege management techniques, IT can remove full admin rights from users quickly and easily and instead provide them with elevated privileges for only the apps or tasks that need them. This simplifies endpoint security, reduces support calls, and lowers TCO.

Tip #10: Plan for a Hybrid Environment

While IT teams strive to simplify, the reality is that today's enterprise computing environment is more complex than ever. Hybrid computing environments are the new normal. Enterprise IT success today has little to do with the technologies you're using and everything to do with how well you can bring disparate technologies together in a way that's efficient for both users and IT.

The greatest challenge with this new IT paradigm is being able to predict and react to context. Windows 10 is accessible from many different types of devices, from PCs, laptops, and tablets to handheld and even wearable devices. Users are logging on to their workspaces from many locations using different types of endpoints. You must be able to understand the

context in which users are logging on and adapt their workspace experience accordingly so they can be productive, wherever they are.

For example, a user in an Internet café will typically require a different level of corporate resource access than an employee within the secure confines of the corporate LAN. Make sure you utilize information about user context, such as location, device or connection type, even the time of day, to determine resource entitlement and secure your Windows 10 endpoints.

www.ivanti.com

1.800.982.2130

sales@ivanti.com

For more information about Windows 10 Migration, please visit:
www.ivanti.com/en-US/solutions/needs/migrate-my-users-to-win-10