Conversational
Windows 10 Migration

A ConversationalGeek® Book

Sponsored by ivanti

Learn about:

- Windows 10 Deployment Challenges
- Windows 10 Migration Scenarios
- Troubleshooting Windows 10 Migration

2nd Edition

By Johan Arwidmark
(Microsoft MVP and Chief Technology Officer with TrueSec)

Sponsored by Ivanti

Ivanti is IT evolved. By integrating and automating critical IT tasks, Ivanti helps IT organizations secure the digital workplace. For more than three decades, Ivanti has helped IT professionals address security threats, manage devices, and optimize their user experience. From traditional PCs to mobile devices, virtual machines, and the data center, Ivanti helps discover and manage your IT assets wherever they are located, improving IT service delivery and reducing risk. Ivanti also ensures that supply chain and warehouse teams are effectively leveraging the most up-to-date technology to improve productivity throughout their operation.

Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

www.ivanti.com

Conversational Windows 10 Migration

By Johan Arwidmark

ConversationalGeek®

Conversational Windows 10 Migration

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Johan Arwidmark
Project Editor:	J. Peter Bruzzese
Copy Editor:	Chris Nelson
Content Reviewer:	Karla Reina

Note from the Author

Welcome to *Conversational Windows 10 Migration*. This is the second edition of the book and includes Creators Update (1703) information.

My name is Johan Arwidmark, Microsoft MVP and Chief Technology Officer at TrueSec, an elite team of infrastructure and security consultants who travel the globe helping customers migrate to Windows 10 (and other things).

In this book I'm sharing real world tips and tricks and other useful info about Windows 10 migrations - things we've picked up over the past year or so on various Windows 10 migration projects. I'll also give you a crash course in the changes Microsoft has made for Window 10 deployment and migrations.

On a final note, I want to emphasize this book is not intended to be a sales pitch. Sure, there is a sponsor behind it, allowing the great team at Conversational Geek to publish it for free, but this book is written to give you valuable Windows 10 migration info, and what to watch out for when migrating to Windows 10, not specifically to sell a solution or product.

Johan Arwidmark

Twitter: @jarwidmark
Facebook: http://facebook.com/deploymentresearch
Blog: http://deploymentresearch.com

The "Conversational" Method

We have two objectives when we create a "Conversational" book: First, to make sure it's written in a conversational tone so it's fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

"Geek in the Mirror" Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it's the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these "geek in the mirror" boxes are not to be skipped.

Within these boxes I can share just about anything on the subject at hand. Read 'em!

An Overview of Windows 10 Adoption

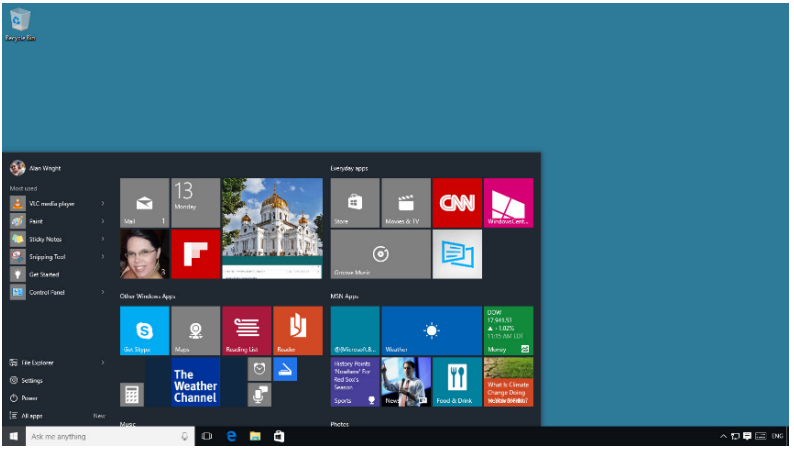
Windows 10 is off to a flying start. In fact, it has, by and large, been adopted by organizations more quickly than any Windows release before. This is mostly due to the fact that Windows 8/8.1 was not liked by the masses, but also because of the wide-spread testing phases and feedback processes that were accomplished via the Windows Insider Program. These led to a solid OS.

The later releases of Windows 10, the anniversary edition (1607), and the creators update (1703) turned out to be adopted by organizations more quickly than ever before.

The wide-spread testing phases and feedback processes that are accomplished via the Windows Insider Programs certainly

have helped, too. There is now also a Windows Insider Program for Business, which focuses on productivity, deployment, and management features. The original Windows Insider Program now coexists with the Windows Insider Program for Business. The Insider Programs have allowed Microsoft to get feedback from millions of people during the Windows 10 development.

The new Windows Insider Program for Business was announced in April 2017, and you can read more about it here: https://insider.windows.com/en-us/for-business.

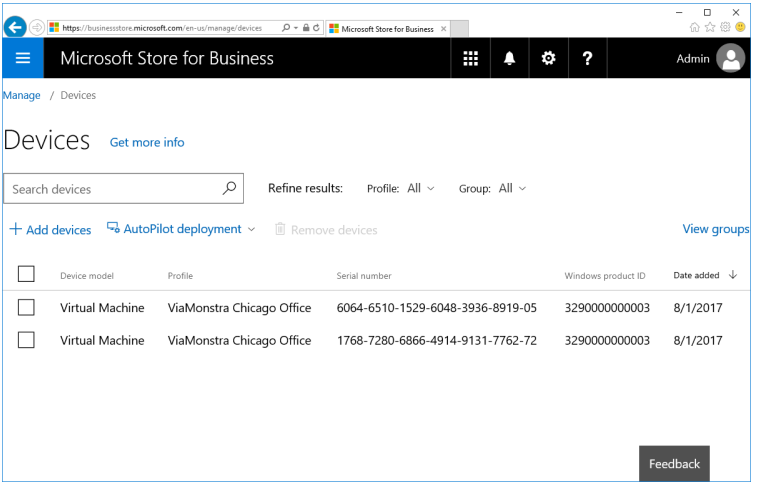


The new Start Menu in Windows 10

With Windows 10, Microsoft changed a lot in terms of how the OS is updated (serviced). The company also introduced new deployment options, most notably provisioning packages and the in-place-upgrade scenario. In 2017 Microsoft updated the release cycle terminology and structure. Now Windows 10 is released twice a year: in the spring and in the fall, sharing the same release cycle as Office 365. The initial release of an updated version was previously labeled as Current Branch (CB), but is now labeled as Semi-Annual Channel (Pilot) (SACP). And

the Current Branch for Business (CBB), which was used to indicate Windows 10 was ready for broad deployment, is now Semi-Annual Channel (Broad) (SACB). As before, each new version is supported for 18 months from its original release (the SACP release).

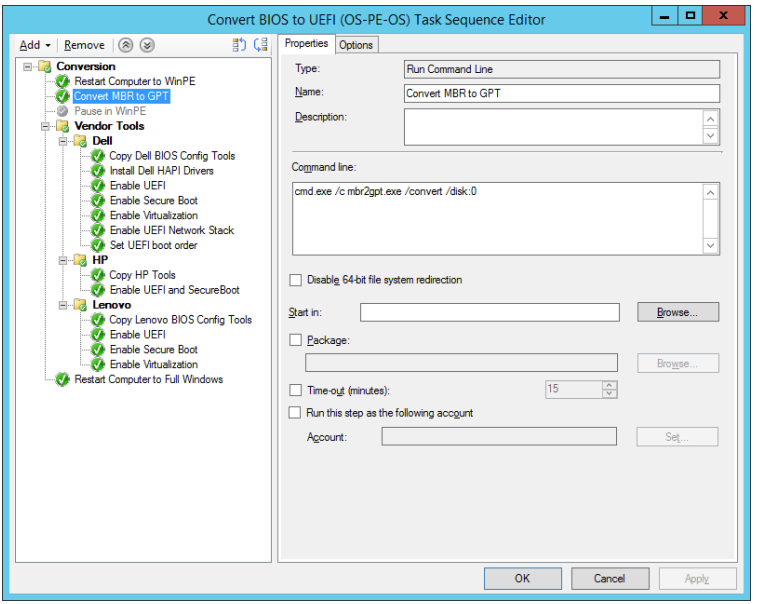
From a deployment perspective, there were also some interesting changes introduced this year, most notably updates to provisioning packages and the brand-new Windows Autopilot concept. Windows Autopilot enables either an OEM or an IT admin to prestage devices in the Microsoft Store for Business so that as soon as they are booted the first time and go into the OOBE phase of the deployment, the machines are automatically configured and put under management. Technically you simply run a PowerShell script to gather the hardware ID from the machines, upload the hardware ID to the Microsoft Store for Business, and then boot the machine into the OOBE phase.



Hardware ID from a few machines uploaded to the store.

Note: The Microsoft Store for Business is located at: https://businessstore.microsoft.com

Another deployment change introduced with Windows 10 1703 (the creators update) is the ability to perform supported BIOS-to-UEFI conversions. You can do this in two ways, either online, assuming you already are on Windows 10 v1703, or offline in WinPE, supporting all currently supported Windows 10 versions (v1511, v1607 and v1703). This conversion of the partitions on the hard drive, combined with calling the vendor BIOS utilities, allows for complete automation of the BIOS-to-UEFI conversion.

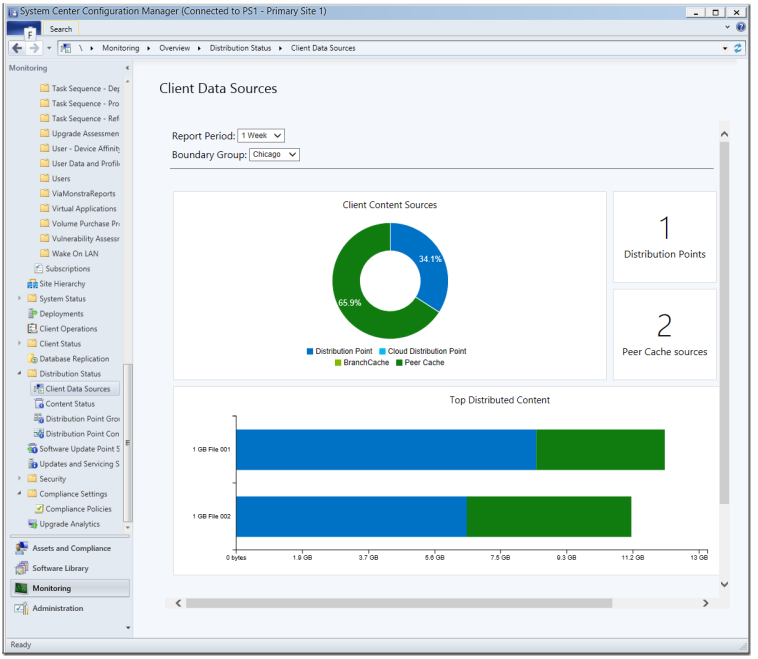


A ConfigMgr task sequence configured for conversion.

Another interesting fact about Windows 10 is how much network bandwidth is needed to keep it up to date. The Windows 10 quality updates that are released at least once per month (sometimes more) are getting very big, currently around 1 GB. You also have the feature updates (a new Windows version), which are about 3 GB in size. In short, Windows 10 is going to hit your network quite hard, requiring much higher capacity compared to updating Windows 7. The reason for the size increase is not only changes to the servicing model. There

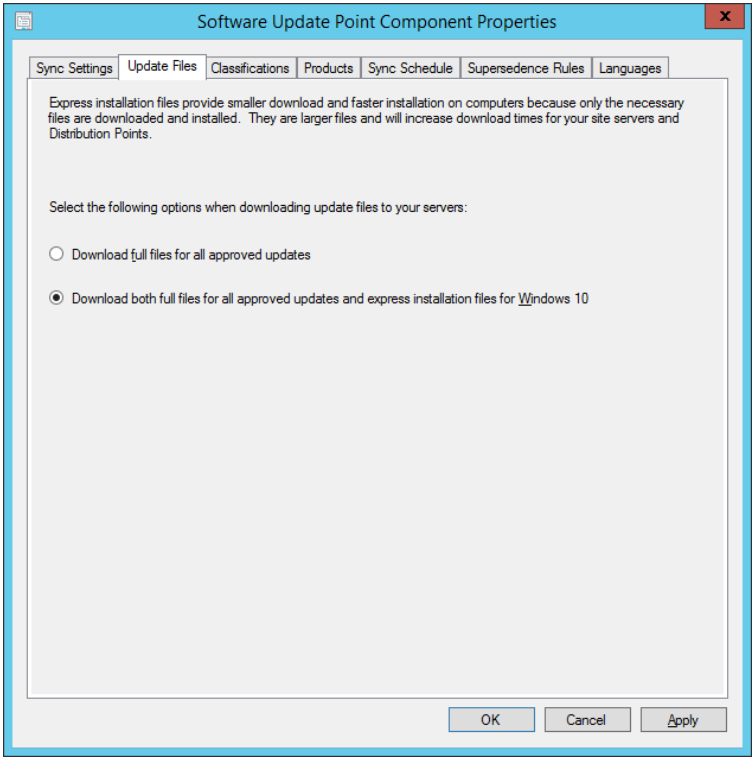
is also no pick and choose any more; it's simply one giant update, which is also cumulative from previous months. This means that you only need to apply one update to get the machine into an updated state. This way of servicing Windows 10 updates obviously introduces challenges, especially if you have a distributed environment with slow, or just heavily used, WAN links.

Don't worry, keep calm. There are solutions in place to help you distribute Windows 10 updates/upgrades quite efficiently without killing your network. Peer 2 Peer solutions for content distribution have been around for many years, and even Microsoft, though late to the game, has implemented them in its systems management solution.



ConfigMgr showing client data sources.

Another software update feature that reduces the network impact of Windows 10 deployments is the Express installation files option that you can enable in both standalone WSUS and ConfigMgr Current Branch. When you enable express installation files, only the delta from each month is downloaded to the client. Typically, that is about 100 MB instead of almost a GB. Now, the downside of enabling this feature is that those packages are much larger to download, several times larger; but because this saves so much bandwidth when downloading to the clients, it's worth it.

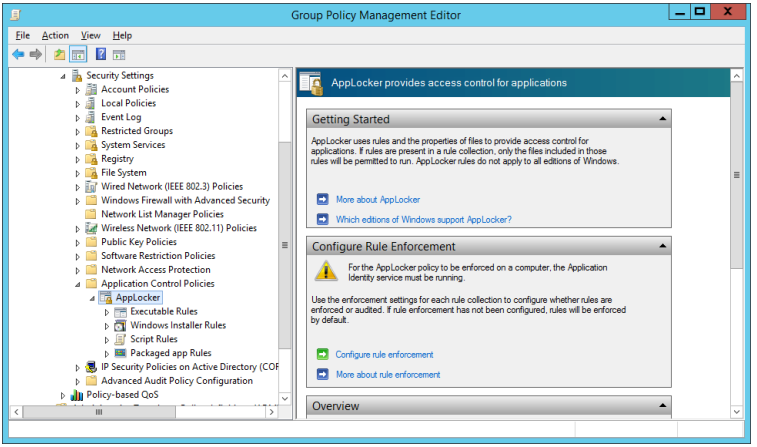


Enabling express installation files in ConfigMgr (a client setting is also required).

Windows 10 Editions

As with previous Windows releases, Windows 10 comes in many different versions, some for end-consumers and some for organizations. The version you should be using is Windows 10 Enterprise because that version contains all the new security features and has all deployment and management capabilities. The rare exception is if you work at an educational organization, then you probably use the Windows 10 Education version, which has the same features as Windows 10 Enterprise but is licensed differently.

I don't consider the Windows 10 Pro version good enough for organizations. It's missing too many important features: AppLocker to block access to Windows 10 applications, DirectAccess for remote workers, and as mentioned previously, most of the new Windows 10 security features, just to mention a few.



Configuring AppLocker for Windows 10.

In August 2017, Microsoft announced a new version of Windows 10 called Windows 10 Pro for Workstations which is

marketed as a high-end edition of Windows 10 Pro. This new SKU adds additional support for server-grade PC hardware and is designed to be used for compute intensive workloads.

There is another version you may stumble across, and that is Windows 10 Enterprise LTSB (Long Time Servicing Branch). That version is specially targeted to environments that cannot change, like a machine controlling a power plant or emergency equipment at a hospital. The LTSB version is not for normal use, even though it may be tempting to try it.

For a solid list of all editions of Windows 10 with a feature comparison across all editions, check Wikipedia (they have a great chart): https://en.wikipedia.org/wiki/Windows_10_editions

To learn more about the different editions and compare the features, you can check with Microsoft on the following page: http://tinyurl.com/p99ohhs

The Big Takeaways

Windows versions worth deploying on a grand scale tend to take the leapfrog approach. For example, Windows 95 (awesome), Windows 98 (not so great), Windows 98 SE (solid), Windows ME (cough…cough… next!), Windows XP (unforgettable), Windows Vista (forgettable), Windows 7 (gold), Windows 8/8.1 (bronze) and last, but not least… Windows 10. The future for Microsoft in terms of the OS look and feel, functionality and more.

Ultimately, the desire to move to Windows 10 is going to cause many organizations to have to figure out the best way to migrate their existing systems. And that leads to our next chapter.

Migration Strategy for Windows 10

"Are you daydreaming about an easier way to do a Windows migration?"

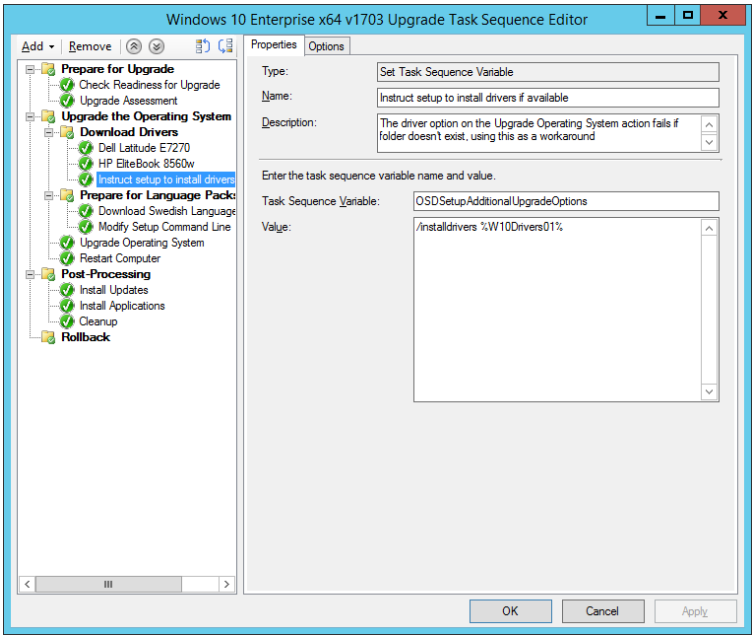
Migrating (or upgrading) a single desktop or laptop to a newer flavor of Windows can be a chore. Doing it to hundreds or thousands of systems can overwhelm IT admins and/or desktop admins tasked with the responsibility.

But it's not like the old days where you had to do it manually with each system. There are tools to automate the process, some of which are provided by Microsoft and others through third-party providers seeking to make the process simpler for their customers. Let's review some of the options provided by Microsoft.

Windows 10 and In-place Upgrades

To help support migration from earlier versions of Windows, such as Windows 7, Microsoft added the in-place upgrade

scenario. And even though this scenario has been used by more than 400 million end-consumers by now, it has not been adopted much in organizations. This is mainly because of its many limitations, but also because organizations have seen Windows 10 as a way to start fresh and leave legacy configurations behind. I mean, the in-place upgrade, after all, will upgrade the machines exactly as they were on the legacy version. There is no pick and choose here.



A Windows 10 in-place upgrade task sequence.

So what are the limitations? Well, for a start, you cannot use your own corporate image in an in-place upgrade. You have to use the default Microsoft image (with updates). And until Windows 10 v1703, you could not switch from BIOS to UEFI during an in-place upgrade, though now you can. In addition, there may also be software installed on the box that prevents you from running the upgrade. Software like third-party antivirus or disk encryption programs are known for making the Windows 10 upgrade process quite upset. It can also be

that you are on a different language or architecture, for example you cannot upgrade a Windows 7 x86 to Windows 10 x64. There are a few more limitations, but the ones listed here are the most critical ones.

Oftentimes, when Windows 10 setup misbehaves, you need to check to ensure the cause is not a third party antivirus or disk encryption solution.

Traditional Deployment Scenarios

Windows 10 still supports the three classic deployment scenarios: bare-metal deployments, refresh (wipe-and-load), and replace (side-by-side). This means you can continue to deploy Windows 10 in the same way as you deployed Windows 7 or Windows 8/8.1, typically with your own corporate image (reference image) and in a completely automated fashion. Here are some more details on each scenario:

- New computer. A bare-metal deployment of a new machine. Again, this scenario assumes you don't want to keep any data.
- Computer refresh. A reinstall of the same machine (with user-state migration and an optional full WIM image backup).
- Computer replace. A replacement of the old client with a new client (with user-state migration and an optional full WIM image backup).

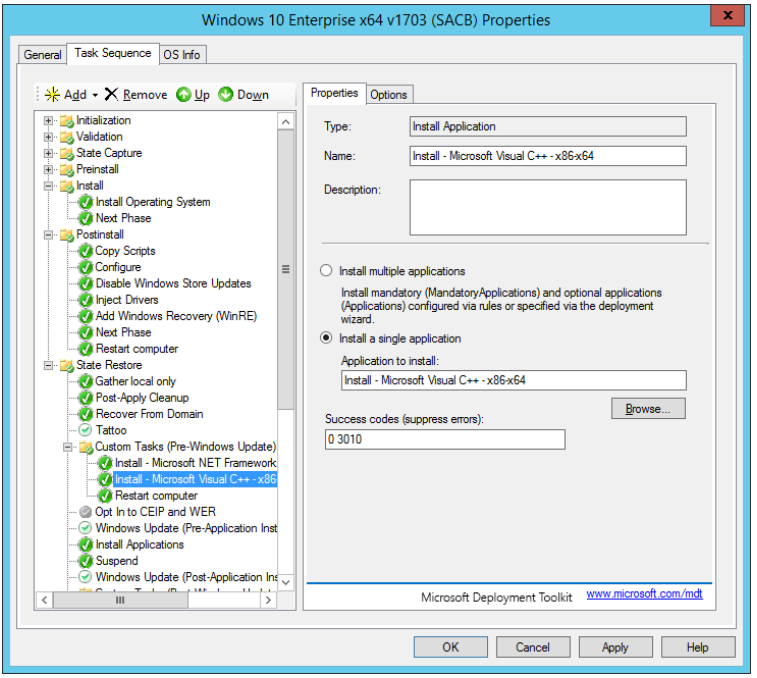
The traditional scenarios do not require, from a technical point of view, that you have a reference image, but you really should have one. The best way to build reference images - and this is not related to how you deploy them later, or what solution you

use – is to use the free Microsoft Deployment Toolkit (MDT) to do it. MDT is remarkably good in creating reference images that are compatible with every deployment solution out there. MDT helps you create a truly generic image, and in an automated fashion.

When automating build of Windows reference images with MDT, you often stumble across the term “Image Factory”, which is exactly what it is :)

In deployment projects, we fight hard to keep a somewhat thin reference image because that allows the imaging process to be flexible at deployment time, for example dynamically generating lists of applications to install for different departments. By “thin image,” I mean an image that is fully up to date and has all the runtime support (Visual C++ and .NET), but doesn’t have many applications. The rare exception is if everyone in the organization is using the same version of Office, I typically include that in the image, as well. The reason is because the Office setup is quite big, and it can be updated when building the reference image rather than at deployment time. That saves both time and network bandwidth.

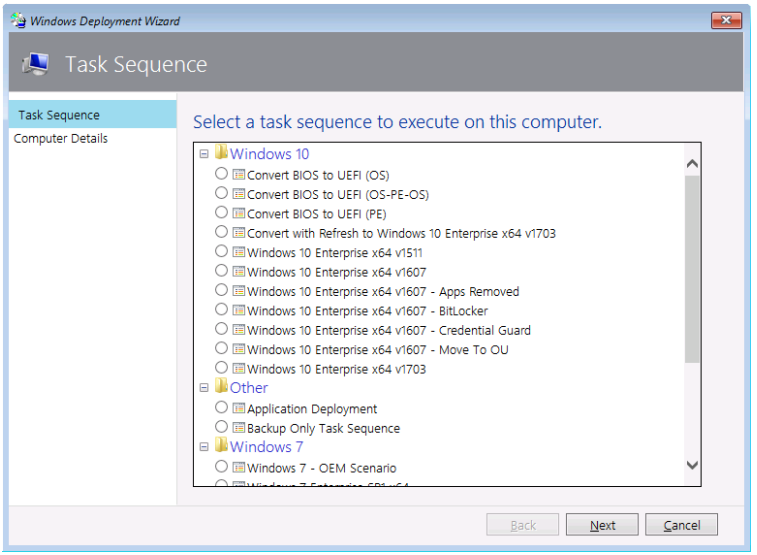
However, sometimes you have to build thicker reference images, meaning images with lots of applications in them, simply to meet a Service Level Agreement (SLA), for example being able to deploy a new classroom over lunch because the next class needs a different setup. Please note that the more applications you put into an image, the more costly it becomes to manage and the more frequently you need to update the image.



Task sequence for a standard Windows 10 reference image.

Level of Automation

Back to the actual production deployment for a while, no matter what solution you use to deploy Windows 10, it's you who determines the level of automation. Some organizations prefer to prestage all deployment info before deployment, some prefer to generate settings on the fly during deployment, and some prefer to prompt for information at deployment time. In general I prefer to have info prestaged because it allows a fully automated deployment and minimal technician time, but there is no right and wrong here. You simply choose the level of automation that fits your organization the best.



Prompting for which Windows version to deploy.

All Microsoft deployment solutions offer customizations for the automation level. It's all in the Microsoft Deployment Toolkit (MDT), which an admin would find at: http://microsoft.com/deployment

Dealing with User State

For the last two scenarios in the preceding section, the computer refresh and computer replace scenarios, the design behind them assumes that you are interested in taking care of user data and settings.

And, taking care of user state, meaning user data and settings on the machine, is often a factor that gets neglected. I have seen many IT organizations simply fall back to company policies that may say users are not allowed to store any data locally. But what if they do? Well nobody blames you, the sysadmin, but if data is lost, there is still a cost for the organization as a whole to restore it. You can avoid that cost, and end user

frustration, by using the migration engines the deployment solution provides or by looking at third-party options to help with migrating user data and settings.

As I mentioned earlier, the one scenario in which you don't have to worry about user state at all is the Windows 10 in-place upgrade scenario, because when that scenario is used, it will migrate every single application, all the data, and all the user settings to the new setup. There is no pick and choose here, it's everything. That also means that if you're already not super happy about the current environment, in-place upgrade is not for you.

Computer Refresh Workflow

So how does the computer refresh really work? Well, here's the high-level overview:

1. You as an admin push out a deployment to an existing machine. This deployment starts running through a series of steps needed to drive the refresh scenario.

2. If the backup solution used is running online, that's typically the first thing that happens. This backup is normally stored locally using hard links for performance reasons, but I've seen configurations where the data has been copied to a file server as an extra backup.

3. The next step is that the deployment stages WinPE on the hard drive and reboots the machine so it starts in WinPE.

4. In the WinPE phase, any offline backup happens. That can be user state (unless run online) and/or a full image backup, where typically a WIM file is created of the entire hard drive.

5. The next step is applying the Windows 10 image, fixing up any boot loaders, and then doing another reboot.

6. After the reboot, the deployment installs any software updates missing from the reference image, as well as any applications that have been assigned.

7. As a final configuration, the previous user state backup is restored so the machine is completely ready for deployment.

Computer Replace Workflow

That was the computer refresh scenario, but what about the computer replace scenario? Well, it's quite similar to the computer refresh scenario, but because you are replacing computers, you cannot really store the backup locally on the machine. Most of the time, you either slingshot the backup to the new client directly, or use a file server, a NAS, another client, USB media, etc. to store the backup in between. So for computer replace, the standard process is divided into two main parts, a backup job and then a normal bare-metal deployment. The backup process breaks down to this:

1. You as an admin push out a deployment to an existing machine. This deployment starts running through a series of steps needed to drive the replace scenario.

2. If the backup solution used is running online, that's typically the first thing that happens; however, for the replace scenario, this backup is normally stored anywhere but locally, again, for example on a file server.

3. The next step is that the deployment stages WinPE on the hard drive and reboots the machine so it starts in WinPE.

4. In the WinPE phase, any offline backup happens. That can be user state (unless run online) and/or a full image backup, where typically a WIM file is created of the entire hard drive.

This ends the first part of the replace scenario. The next and final part is a normal bare-metal deployment:

1. PXE-booting, or booting from USB media, starts WinPE.

2. Then the Windows 10 image is applied, boot loaders are configured, and then a reboot happens.

3. After the reboot, the deployment installs any software updates missing from the reference image, as well as any applications that have been assigned.

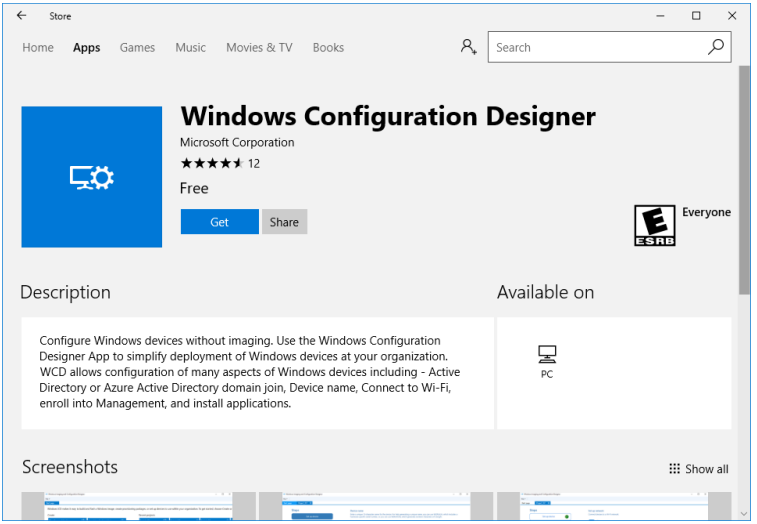
4. As a final configuration, the previous user state backup is restored so the machine is completely ready for deployment.

For the refresh and replace scenarios, you typically spend quite a bit of time figuring out what data and settings to migrate because there is simply no one-size-fits-all configuration. It's different for every organization.

Provisioning Packages

As you learned previously when I introduced the Windows Autopilot program, another interesting technology that is available with Windows 10 is the provisioning packages, which contain file assets and settings for Windows 10. For example, a provisioning package can contain an application install, include instructions to join a machine to a domain or to set a computer name, install a certificate, or change the version of Windows 10 (like going from Pro to Enterprise).

Provisioning packages are authored using the Windows Configuration Designer (WCD), an application that is included in Windows ADK, but it is also available as a Windows Store application.



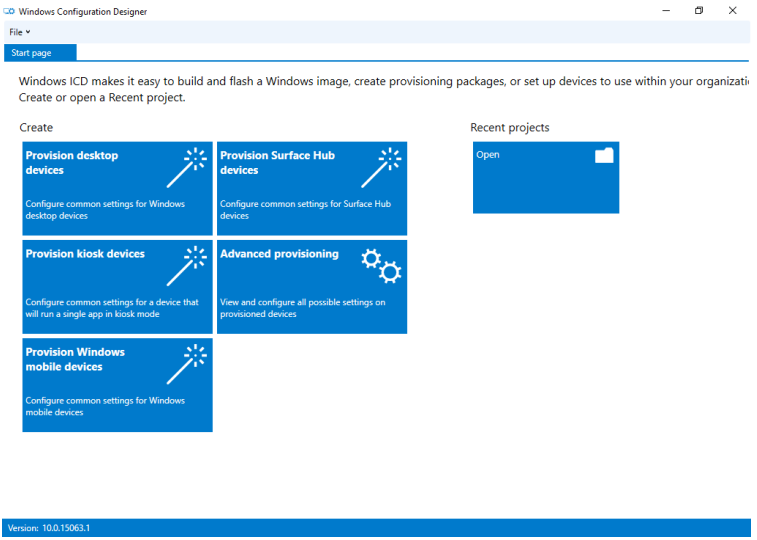
Windows Store showing the WCD application.

The very idea behind the provisioning packages is that a user should be able to go downtown and a buy a machine in any store of their choosing. That machine would obviously not be deployed with Windows 10 Enterprise, be part of the organization domain, etc., but by running the provisioning package, it "fixes up" the machine for corporate use.

Provisioning packages can also be used to simply apply Windows 10 policies, for example you can set a policy to control whether you can use the camera on a computer or how Windows Defender should be configured. Many of these policies overlap with what you can do with Windows 10 group policies, but not all of them.

The idea behind provisioning packages is quite good, but please note it's not yet integrated with the deployment solutions available. It's a feature on its own.

Creating provisioning packages is pretty straightforward: either you use some of the native scenarios (wizards) in the WCD application, or you go directly to Advanced provisioning and define all settings manually. Once you have configured all settings, you export them as a provisioning package (a PPKG file).



Creating provisioning packages in WCD.

Windows 10 and Group Policy

Some of the more interesting things you may come across when migrating to Windows 10 are existing Windows 7 or Windows 8/8.1 group policies that break things in Windows 10. For example, in one of my earlier Windows 10 projects, I stumbled across a customer that had been using AppLocker to

lock down applications, and the way they had done it was basically whitelisting applications that were allowed to run. Now, in Windows 10, both search and the Start menu are applications, and the end effect of the AppLocker policy was that users could not use the Start menu. It also locked down command prompts, so administration was limited. :)

With Windows 10, you want to start fresh on group policies. After all, group policies have been around since Windows 2000 was released, and many environments have accumulated more and more of them as Windows XP, Windows Vista, Window 7, and Windows 8/8.1 passed by.

My recommendation is to take Windows 10 as a great opportunity to review your existing policies. Create a new Windows 10 OU structure for the Windows 10 pilot project, and only link a very few (or none) of the existing group policies to it. Some you may have to, like certificate enrollment policies, WSUS policies, etc., but I recommend that you be very selective.

You also have the option of using WMI filters to limit to which operating system they should apply, but in general it's easier to use a new OU structure, at least during the pilot project.

If you are going the WMI filter approach for Windows 10 and group policies, please remember that it is a string comparison, and the string "10" is actually not higher than "6.1, 6.2 or 6.3" which are used for legacy Windows versions.

Windows 10 Drivers and Hardware Configuration

You do have to worry about drivers in all of the Windows 10 migration and deployment scenarios. For example, if the Windows setup program does not detect suitable drivers

during an in-place upgrade, it will abort the setup. Finding suitable drivers for Windows 10 is an art on its own, but your starting point should always be with the hardware vendors. Not only are they very likely to have tested drivers for Windows 10, they will also support you if you have any issues with them. Also the various vendors have gotten increasingly better in providing drivers that are ready to be used for mass deployment. Here is a quick list of the leading vendors:

- For HP hardware, I recommending using the HP SoftPaq Download Manager utility, which can download and extract drivers on a per model basis, and is suitable for import into deployment solutions like MTD or ConfigMgr.

- For Lenovo, you can either try your luck with ThinkVantage Update Retriever utility, or use the SCCM packages available on the Lenovo web site. Anyway, the trick to using the utility is to first download the drivers and then use the managing features to export the drivers in a flat structure for use in Windows 10 deployments.

In the Lenovo case, don't let the word SCCM fool you. These packages can be used with any deployment solution.

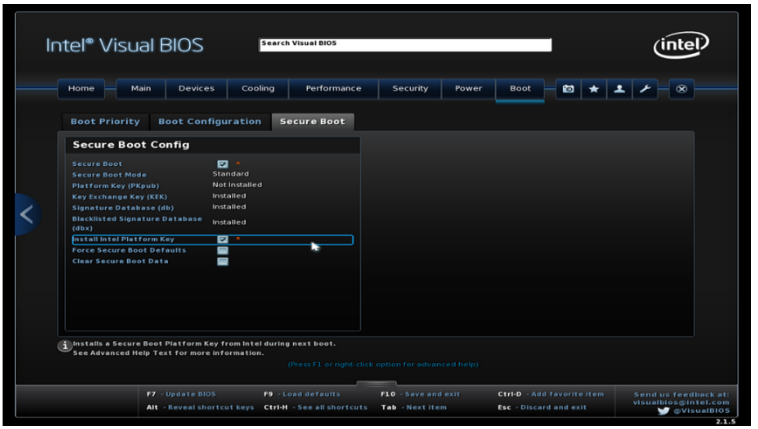
- Dell, which was one of the first vendors to come out with good drivers for Windows deployment in general, has good driver packages (CAB files) for Windows 10 deployments. Dell also provides one of the best WinPE driver sets in the industry.

In terms of hardware configuration, I also want to discuss BIOS- vs. UEFI-configured machines. Today, because they are running Windows 7, most machines are configured to run in a BIOS-mode configuration, even if the hardware supports UEFI. The reason is simple: depending on hardware, it can be quite "interesting" to deploy Windows 7. Try, for example, to deploy Windows 7 to a Microsoft Surface machine, and you'll see what I mean. That being said, some hardware does support compatible modules that allow you to deploy Windows 7 in EUFI-mode, but the fact is, most organizations are still running their Windows 7 deployment on machines in BIOS mode.

If you do manage to deploy Windows 7 to a Microsoft Surface, please ping me, I would be really interested in how you did it :)

Why you should you configure your deployment to enable UEFI then? Do you really need to bother? The answer is yes, you do. Most of the new security features in Windows 10 require secure boot, which in turn requires UEFI. This means that at some point you need to make a decision. Should I continue to run in BIOS mode and miss new (and upcoming) security features? Or should I now switch my machines into UEFI mode? Well, some organizations I've worked with have made the decision to switch as soon as the first Windows 10 images are rolled out. Other organizations have decided to take a bit of laid-back approach: They keep BIOS-based setups on their existing machines for now, but every time they replace a broken hard drive, or buy new hardware, they configure that machine for UEFI. Their general thought with this approach is that within a few years, all machines will have been swapped out, and everything will be running in UEFI mode. Other companies I've worked with wanted to use the security features right away, for example one project did a full

implementation of Credential Guard with Windows 10, one of the features that requires UEFI to work.



Enabling EUFI on an Intel NUC machine.

Windows 10 and Application Readiness

Windows 10 has been quite awesome in its application support, and after been doing Windows 10 migration projects for almost a year, I've only encountered a handful of applications that didn't work with Windows 10 in its default configuration. Not surprisingly, most of them were VPN clients. :)

One thing to look out for, though, is the Credential Guard feature. If you want to use that security feature in Windows 10, you need to retest your applications. Many applications that work perfectly fine on Windows 10 without Credential Guard may fail pretty badly when you enable that feature.

If you plan to use the Credential Guard security feature in Windows 10, make sure you test your applications with that feature enabled.

Anyway, even though Windows 10 has pretty good application support, it still makes sense to test all the apps during the Windows 10 pilot so that you can address any issues found early on. So far, most issues related to applications in Windows 10 have not been with normal desktop applications, but actually with websites or web applications, which have issues with Internet Explorer 11 in combination with Windows 10.

So what to do if an application doesn't work in Windows 10? Well, if its vendor is still around, you typically check with them. If they are not around anymore, there are many application compatibly tricks you can try, such as shimming applications, virtualizing applications, running them remotely, and much more. For more advanced application readiness, you might want to review third-party options available in that space.

A valuable resource for Windows 10 application readiness is the Upgrade Readiness solution, which is part of Microsoft Operations Management Suite (OMS). It's a free solution that uses telemetry data from Windows 7 and higher clients to upload info about installed applications and then allows you to verify whether they are compatible with Windows 10.

The Big Takeaways

Microsoft has done its best to provide a variety of methods and tools (like the Microsoft Deployment Toolkit, MDT) for upgrading to Windows 10. The tools require some effort and time to master and in some cases you may have the time and personnel to accomplish this. In other cases, you may look to assistance from a third-party solution to make the task easier.

Vendor Sponsor Chapter: Ivanti

"How do you do it???

The path to Windows 10 is filled with challenges – some you'll identify in the planning phase and others that only rear their ugly head mid-migration.

At Ivanti we have helped thousands of organizations "smooth out" and accelerate migrations between Windows versions and between physical and virtual desktop deployments.

This update to Conversational Geek Windows 10 Migration highlights many areas where Ivanti solutions can simplify the multitude of tasks necessary for implementing, updating, and securing Windows 10, as well as migrating the applications, user settings, and data that users will expect in their shiny new Windows 10 environment—or else.

Ivanti lets you take control of your Windows 10 migration and take action when you're ready by allowing you to capture files and user settings, centrally upgrade endpoints in place, track

your progress, and audit success—all without disrupting users' work. Users experience no downtime and get their user settings and files at their first logon to Windows 10.

Get to Windows 10 Easier and Faster

Ivanti's Windows 10 migration solution delivers these features:

- File migration – capture every file (even PSTs!) from the user's old desktop or laptop without disrupting that user's workday and make those files instantly available from their Windows 10 desktop
- User profile capture and migration – precise, automated capture of settings and user persona that you want to migrate to the new environment
- Granular desktop policy – without the complexity and overhead of Group Policy WMI filters and Preferences that can 'break' Windows 10 during migration
- Security and desktop lockdown – mitigate ransomware, reduce help desk calls and software licensing costs with application and privilege control
- Patch management – centralized, advanced control of updates for 3rd party and Microsoft apps in addition to Windows and Mac OS

If you're facing any of these Windows 10 migration challenges, talk to the person who gave you this book to find out how Ivanti can help.

NOTES

.

Easily “converse” about Windows 10 migration in any setting.

Windows 10 is enjoying the fastest adoption by organizations than any Windows release before. In this book you learn the key concepts, scenarios and challenges when migrating to Windows 10, augmented by real world notes from early adopters of Windows 10.

About Johan Arwidmark

Johan Arwidmark is a consultant and all-around geek specializing in Systems Management and Enterprise Windows Deployment Solutions. Johan also speaks at several conferences each year, including MMS and TechEd/Ignite events around the world. He is actively involved in deployment communities like deploymentresearch.com and myitforum.com, and has been awarded Microsoft’s Most Valuable Professional (MVP) designation for more than twelve years.

Follow him on Twitter @jarwidmark