Windows 10 and Group Policy

Keys steps to Group Policy success during your Windows 10 migration

By Darren Mar-Elia

CTO & Founder

SDM Software, Inc.

August, 2016

Overview

Microsoft just put the wraps on the "Anniversary Update" to Windows 10—the first major update after Windows 10 was released in 2015. And, as with all 2nd releases of the Windows operating system, many organizations are now looking seriously at deploying this new, more usable and more secure OS. Though with any OS upgrade, come the inevitable Group Policy-related questions, like:

- What is new for Group Policy in Windows 10, Anniversary Update?
- What policies should I be deploying specific to Windows 10?
- Should I finally get around to cleaning up my Group Policy deployment now that I'm upgrading Windows? (Hint: yes!)

This whitepaper will attempt to answer these questions and provide you with some easy-to-implement guidance around Windows 10 and GP to help simplify your deployment.

What's New in Group Policy in Windows 10?

There have been three major releases of Windows 10 since the summer of 2015---the RTM version, the 1511 November Update, and now the 1607 Anniversary Update. In each release, Microsoft has continued to update the Group Policy capabilities for managing Windows 10-specific features. I would go so far as to say that if you had contemplated rolling out Windows 10 RTM, you would not have been able to manage very much of that new OS via Group Policy. That changed dramatically in the 1511 release and continues with 1607. From the ability to manage the Start Screen, to locking down features such as WiFi-Sense, to shutting off our good friend Cortana, Microsoft has increased the coverage of configuration "knobs and switches" for Windows 10 specific features. They've done this primarily via the use of new Administrative Template (ADMX) settings rather than extending the core functionality of Group Policy with so-called Group Policy Client Side Extensions (CSEs). Administrative Template policy is 100% registry-driven, and the new Windows 10 ADMX files that ship with each version add more and more settings that can be controlled via GP. If the Group Policy Settings Spreadsheet (https://www.microsoft.com/en-us/download/details.aspx?id=25250) that Microsoft puts out after each new Windows release is to be believed, then 295 settings have been added since Windows 10 shipped. Among them, here are some highlights that you might find useful when it comes to managing Windows 10 in a typical enterprise:

- **Manage Cortana**: Can be found in the not-so-obvious location of *Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana & Allow Cortana above lock screen*
- **Manage App-V**: App-V used to be part of the Microsoft Desktop Optimization Pack (MDOP) but has now been included within Windows 10 Enterprise as of the Anniversary Update. It can be managed under *Computer Configuration\Policies\Administrative Templates\System\App-V*
- **Manage what UWP (Windows Store) applications can access on your system**: Can be found under *Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy*
- **Manage the Microsoft Edge Browser:** Can be found under *Computer (and User) Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge*
- **Manage the Windows Defender client**: Can be found under *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender*

These are key Windows-10 specific areas where policy management has been added, in addition to the 1000s of settings that have been in Group Policy since Windows 2000. To be sure, Microsoft has not created 100% coverage for Windows 10 features in Group Policy. In fact, I would argue that they've done less in this new OS version than any previous version of Windows, with respect to Group Policy enabling OS features. But, they have done a pretty good job of creating policy settings for the things that enterprises care about. And speaking of what enterprises care about, what are those key policy areas that you should be looking to configure when it comes to managing your Windows 10 configurations using Group Policy?

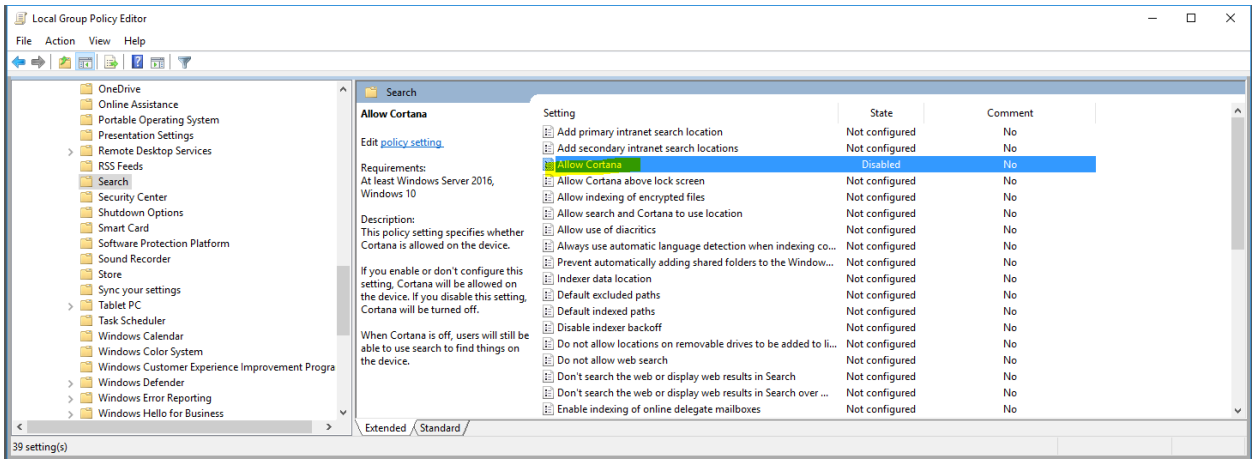
Policy Guidance for Windows 10

Without exception, the first sorts of policies I look for in any OS release are those related to the security and lockdown of the OS. Each new version of Windows adds features and new capabilities. I look for features that could present opportunities for data loss, privacy issues or outright security exposures, and focus on them first. Basic desktop lockdown, such as disabling the command shell or registry, or turning off menu selections within certain applications, are less interesting to me from a security perspective than *real* security options, which I classify as security that protects core OS resources. Don't get me wrong—some of these lockdown settings are useful to configure in Group Policy, if for no other reason than Microsoft provides no other way to control these features. And I will be recommending some of those in this section. But by and large, Group Policy is best at configuring Windows' core security features, and those are what I encourage IT people to focus on.

Windows 10 Features to Control

So, what are some of the key Windows 10 features we might be interested in configuring using Group Policy, in the typical organization? Here are some of my top recommendations:

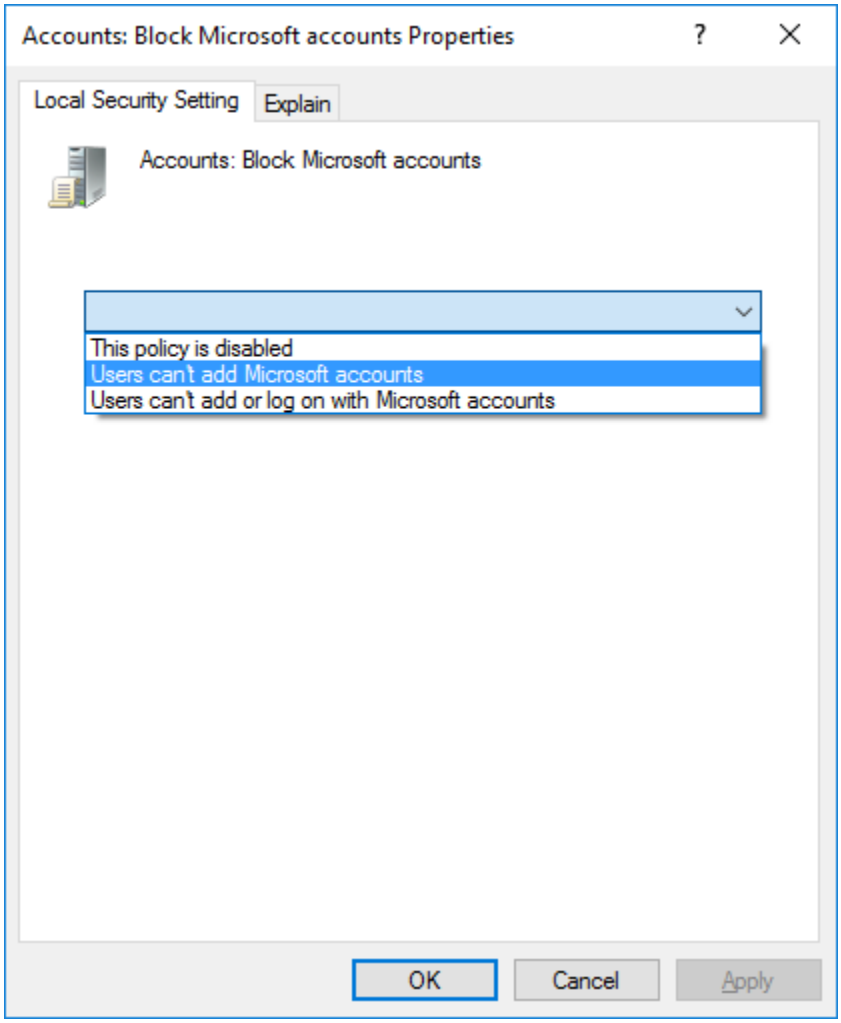
1. **Cortana**: Cortana is a powerful search feature within Windows, not to mention a nifty way to talk to your computer and have it talk back to you. But Cortana presents a problem for many IT organizations. Why? Because for Cortana to do its thing, it needs access to user data—be it calendar, email or other personal data, so that it can fulfill its role as personal assistant. And that user data, at least in some form, is stored by Microsoft in their Bing cloud platform. Some organizations may not find that terribly consistent with their data privacy policies, especially if Cortana is accessing corporate email/calendar and other sensitive data to do its thing. As a result, organizations can turn off Cortana using the "Allow Cortana" policy mentioned in the previous section and shown here:



2. **Windows Update**: in Windows 10, Windows Update takes on a whole new level of complexity, with Microsoft providing something called "Windows Update for Business." Windows 10 is the first OS provided by Microsoft that does not really give you an option to choose whether to install updates or not. As a business organization, you can defer so-called "quality" (i.e. security patches and the like) updates for up to 30 days, so that you can test them first before deploying them. For "feature" updates, which include new versions of Windows 10 like the recently released 1607 build, you can defer those for up to 8 months. These deferrals are controlled using some new policy settings just made available (and only in effect for) the 1607 build, under *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Defer Windows Updates*.
3. **Privacy**: Privacy is another important area that most customers of Windows 10 are likely to want to control. Unfortunately, there is no single area in Group Policy to allow you to control all privacy settings across the OS. Instead, privacy related settings are scattered around the Administrative Templates namespace. In addition to the Cortana ones I've suggested above, here are a few others that you will likely find useful:
    a. **Turn off WiFi Sense**: *Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings\Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts and to hotspots offering paid services*: **Set to DISABLED** to turn off WiFi Sense.
    b. **Input Personalization**: *Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language Options\Allow Input Personalization*: **Set to DISABLED** to prevent Microsoft from collecting information about your users from their typing, speech and inking habits.
    c. **OneDrive**: *Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file Storage*: **Set to ENABLED** to prevent users from using personal OneDrive accounts on their organizational machines.
4. **Browsing**: Microsoft continues the tradition of providing Administrative Template control of the browser, extending its capabilities to the new Edge Browser, in addition to IE. Most of the Edge settings are per-computer and per-user and only support Windows 10 build 1511 or higher, but you can do things now like set Pop-up blocker allow lists, configure home page and favorites, and even whether the new Edge extensions framework is enabled or not. There is nowhere near

the number of settings available for Edge that there were for IE, but if you are looking to start letting your users take advantage of Edge, you do have some options.

5. **Microsoft Accounts**: A lot of organizations may not want to allow users the ability to connect their personal Microsoft accounts (e.g. Live, Hotmail, Outlook.com) to their Windows 10 PC. You can use Group Policy to disable the ability to do so, not through an Administrative Templates policy, but through a security policy under *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts:Block Microsoft Accounts.* There are three options available there, including allowing Microsoft accounts to be added, not allowing MS accounts to be added, and not allowing MS accounts to be added or used for login, as shown here:



Preparing for Windows 10

Whenever a new Windows OS rolls out, many IT shops will use the opportunity to assess how they manage their Windows desktop platform. Part of that assessment usually involves looking at how Group Policy is currently used, whether there are specific policy settings that should be rolled out for the new OS, and how that rollout should occur. I won't say that every new OS is an invitation to completely re-

work your Group Policy deployment, but if you haven't done it since you've been using Group Policy, Windows 10 may be a good time to plan for it, since it is likely to be Microsoft's last major desktop OS release in the traditional way we think about releases.

That said, what are some of the things you can do to cleanup, test, then deploy and manage Group Policy in a Windows 10 world? Here's how we at SDM Software think about it – I like to break the process into phases:

PHASE 1: **Figure Out What You Have**: This involves performing an inventory of your current Group Policy deployment and understanding where you might have policies that either no longer apply, are duplicated, in conflict with or otherwise unnecessary for your new OS deployment. SDM Software provides the **GPO Reporting Pak** for that job, as it's specifically designed to give insight into Group Policy settings across your entire environment.

PHASE 2: Normalize What You Have: The normalization process is about taking the insight you gained in Phase 1, and using that to clean up and optimize your Group Policy design. For a new OS rollout like Windows 10, that likely involves finding policy settings that no longer are relevant for the new OS, or enabling settings that were not around in earlier releases, such as those I discussed in the sections above. The normalization process can be done "on paper" or in a test environment. (Note: many shops create a whole new test AD domain for these kinds of upgrades, but even a test OU in your existing environment, where you keep your Windows 10 clients, can serve the purpose here.) One issue you will need to think about is ADMX files—each new OS version provides a new set of these. I discuss this next.

ADMX File Management

One challenge with Windows 10 is the need to deploy the new ADMX files for Windows 10 before you can enable those Windows 10 specific settings in your GPOs. If you work in an environment with the ADMX "Central Store," then you know that updating your ADMX files is an all or nothing proposition. In past versions of Windows, you could reliably expect that Microsoft would respect the tradition that newer OS ADMX files were supersets of previous versions, and so you could safely update the Central Store with the latest and greatest ADMX files without risk of losing functionality managing down-level versions of Windows. Unfortunately, it seems that Microsoft has broken that covenant in the latest versions of Windows 10. As a result, I now recommend that you either design and test your Windows 10 GPOs in a test domain separate from your production one, where those newer ADMXs are installed, or use this trick to temporarily override the Central Store for purposes of testing those new ADMX files in your existing domain.

PHASE 3: Deploy and Manage the New Environment: Once you've inventoried what you have and decided what policies you need to deploy for Windows 10, it's time to deploy your new Group Policy, ensure it stays the way you want it, and gets delivered to your new Windows 10 devices the way you expect. SDM Software can make things a little easier here, too. Our Group Policy Automation Engine can help you automate the deployment of your new GPO settings via PowerShell. Our Group Policy Auditing & Attestation product can help you track who is making changes to your GPOs and let you assign owners to key GPOs to ensure that they review them periodically for continued usefulness. Finally, our Group Policy Compliance Manager can collect GP processing health and delivered settings from your new Windows 10 systems to ensure that your Group Policy settings are being correctly applied.

In your own environment, these 3 phases may take more or less time, depending on the complexity and challenges you have with your existing GP deployments. Our experience is that customers who take these new OS deployments as an opportunity to clean up their configuration management environments with Group Policy, reap rewards in terms of easier troubleshooting, more secure configurations and a better user experience for their end users sitting in front of those Windows 10 desktops.

Summary

Each new OS release from Microsoft introduces new capabilities and new settings that can be managed via Group Policy. It's important that you take a step back and think about how you will manage your Windows 10 systems in the most secure and organized way possible. SDM Software has helped customers achieve this manageability with our Group Policy solutions. For more information on how SDM Software can help with **your** Windows 10 Group Policy deployments, contact us at sales@sdmsoftware.com.