PolicyPak
SECURING YOUR STANDARDS

Maximizing Your Investment in MDM and Autopilot (With Microsoft Intune, VMware Workspace One, or MobileIron)

Simplify Windows 10 management. Deliver real Microsoft Group Policy settings today. Lock down device and user security with any MDM service.

Let's be clear: PolicyPak MDM Edition is not an MDM service, and it isn't a substitute for your current MDM solution. Instead, its purpose is to make any existing MDM service more effective by making it a more comprehensive solution; in fact, a lot more.

PolicyPak MDM Edition can supplement your MDM service, like Microsoft Intune, VMware Workspace One, or MobileIron, with features those MDM services don't have. If you want to augment your Windows 10 management capabilities significantly, deliver nearly 100% of Microsoft Group Policy settings, as well as provide lockdown security protection for your users and devices, then this paper is for you. In this paper, we show you how PolicyPak MDM Edition can maximize the investment you made in your MDM service, and give you control over your Windows 10 computers in a way you didn't think possible.

MDM vs. Group Policy

MDM is not trying to be Group Policy. Group Policy is two things: it's an on-prem "engine" that uses various older protocols and requires on-prem domain controllers. However, Group Policy is also about settings within the Group Policy engine. Moreover, that's where the gold lies, and as such, the Group Policy settings you might be using might be missing from MDM. Common missing items include:

- Look-and-feel items, like managing Control Panel settings
- Third-party ADMX settings like Chrome, Acrobat, and Firefox
- Group Policy Preferences items like shortcuts, registry settings, and drive maps
- Security settings found in the Group Policy Editor

To reiterate, these settings are not in your MDM service because the underlying MDM platform doesn't have a means to manage them. That's just the way it is.

Microsoft's stated goals are to open up new scenarios with MDM and modern management that could not be done previously with on-prem only technology. This is why Microsoft is investing in both services like Autopilot and Hybrid Azure AD join. This goal means that it's almost guaranteed that some settings you are using in Group Policy today are absent in your MDM solution, and this is the number one reason MDM is not adopted.

Missing Group Policy settings today is the number one reason for MDM adoption problems.

As you'll see in this paper, when you use PolicyPak MDM Edition, you're able to instantly utilize your existing Group Policy settings with your MDM service. Currently, Intune covers less than 600 native settings, whereas Group Policy's ADMX settings cover around 4,000. If you add Group Policy Security and Group Policy Preferences, that number grows to well above 10,000. When you compare the coverage scope of Intune to Group Policy, it is like comparing a quarter to a dinner plate.

To examine the disparity of coverage between the two, let's look at three possible scenarios involving ADMX, Windows Security, and Group Policy Preference settings. The following examples involve Windows 10 client devices. While there are thousands of examples, we picked a handful for simple demonstration.

A Disparity of Coverage: Three Examples Where MDM Doesn't Cut it

ADMX Administrative Template Settings

Let's say you want to disable the command prompt for your local users to prevent them from prevent them opening a command prompt. This is a common undertaking, since run commands give high-level access to users that they can use to evade other system restrictions. The policy would be user based; for example, you might want your IT technicians to have access to the command prompt, but restrict it for regular users. This is easy to accomplish using the Group Policy Administrative Templates, like you can see in Figure 1.

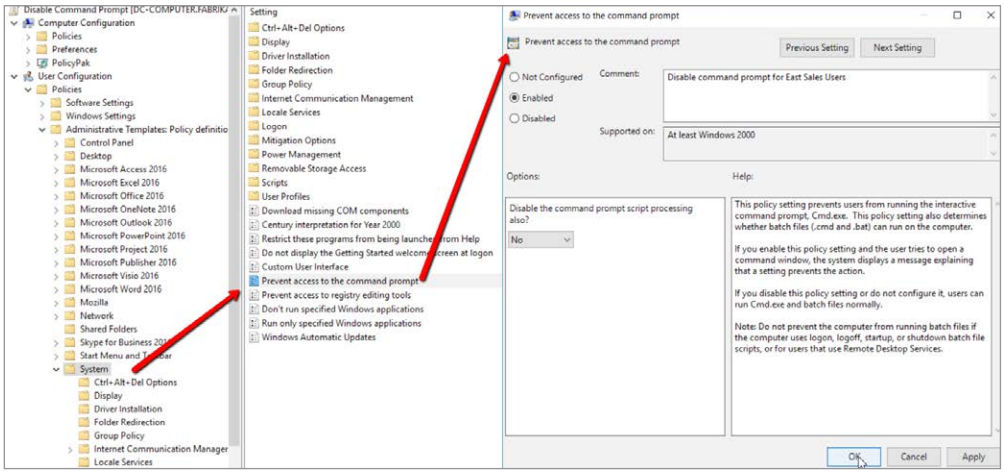

Figure 1: The built-in Group Policy ADMX settings you might already be using

You cannot "click and apply" this simple setting using an MDM solution like Intune or Workspace One, and moreover, there are thousands of these settings.

Windows Security Settings

It is a standard security policy to rename the Administrator account on all Windows devices. This task is simple using Group Policy Security Settings, where you can see that we renamed the account **PPuser**, as demonstrated in Figure 2.

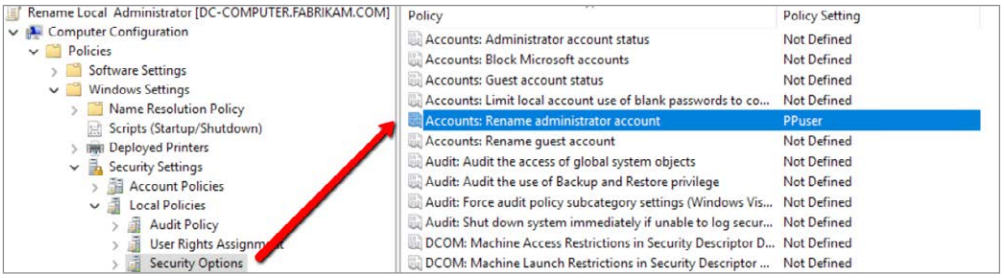

Figure 2: Using Group Policy Security Settings to perform a security settings change; many settings are not defined in MDM

Again, many security settings are not simple, clickable settings in MDM.

Group Policy Preferences Settings

Group Policy Preferences includes the ability to manage multiple go-to settings and does it very simply. Here are a couple of great examples.

Hardening your devices is an essential step of every enterprise security strategy. Part of this process includes reducing the attack surface of your devices by stopping unnecessary services from running on your devices. For instance, you may want to disable the remote registry service that prevents remote users from modifying the registry. Group Policy Preferences completes this action efficiently (like what you see in Figure 3), but MDM offers no ability to address this security concern.

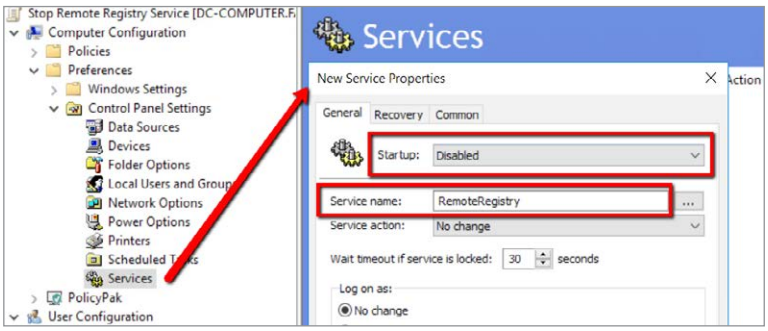

Figure 3: Using Group Policy Preferences to neutralize a security concern; something that is not possible in MDM

Another great feature of Group Policy Preferences is the ability to deliver any registry modification to your devices. Due to the well-publicized vulnerabilities of the SMB 1.0 protocol, such as EternalBlue and others, many organizations have issued mandates to completely disable SMBv1 as a strategic security countermeasure. Microsoft published a TechNet article in February of 2017 on how to disable it. One easy way is through the registry.

The registry path is:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Registry entry:

SMB1 REG_DWORD: 0 = Disabled

Now let's use Group Policy Preferences with the Group Policy Management Console to create a user-based GPO and deliver this registry setting, like what you see in Figure 4. A setting like this goes to work in seconds on-prem. It's a lot harder with more steps trying to this same item via MDM.

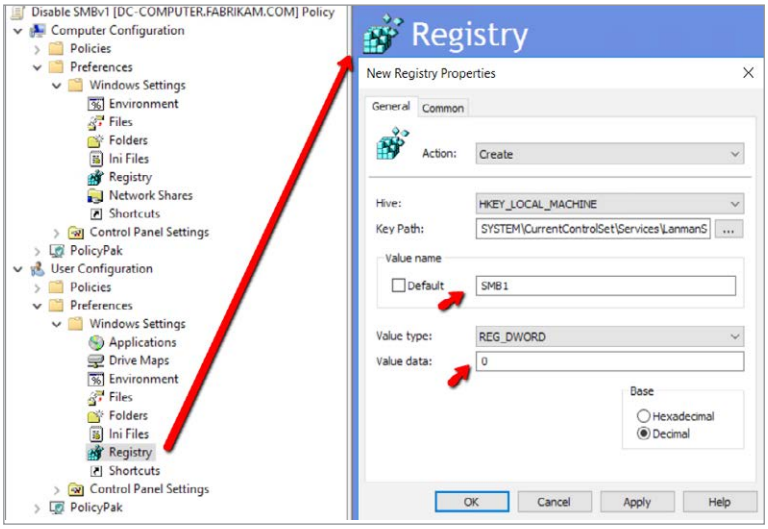

Figure 4: Making a simple registry change using Group Policy Preferences is not possible using MDM

These examples illustrate where you could extend your existing Group Policy and Group Policy Preferences investment to your MDM solution. However, you should remember that your MDM solution has no way to process these settings. You'll learn a little later how to take these existing Group Policy and Group Policy Preferences settings and enable your existing MDM service to utilize them, quickly.

What Can MDM Do via OMA-URIs?

When you configure your Windows 10 settings using the MDM service GUI, the corresponding configuration service provider (CSP) delivers that to the Windows 10 machine. A CSP is a component of the Windows 10 operating system, which receives directions and performs device-specific settings.

However, how do you know what these supported settings are and how do you configure them? Well, you have to do some research on your own and find them. Yes, there is available documentation on this from Microsoft, but it takes your IT team research time to paw thru the MDM settings, learn how the CSP works and craft custom settings for that CSP.

When the settings are not GUI-enabled, an IT admin must create a custom profile and configure the Open Mobile Alliance Uniform Resource Identifier (OMA-URI). All of this is an involved, arduous process at a time when IT departments are trying to streamline basic management tasks to allocate their time to value-added projects. And of course, all of this is only relevant if the settings exist within the CSPs.

If MDM doesn't have the setting you want, and the setting is only available in Group Policy, there is no in-box solution to take all existing Group Policy ADMX, Group Policy Preferences, and Group Policy Security settings when you head toward MDM.

There are a lot of useful security and user experience items in Group Policy that you can't get in MDM. Some of these items include:

- Security settings
- Audit policy
- User rights assignment
- AppLocker settings
- 3,000+ Administrative Template settings
- The ability to manage anything in Control Panel
- Manage the Start Menu and Taskbar for your users
- The plethora of available settings in Group Policy Preferences

PolicyPak: The Quickest and Easiest Path from Group Policy to MDM

Thankfully there is another solution that allows you to leverage your existing Group Policy knowledge and investment and bring it into your MDM solution.

When you add PolicyPak MDM Edition to your existing MDM solution, you retain Group Policy functionality, and also get other Windows 10 desktop management and security features which provide greater efficiencies and security to your on-the-go devices and users.

There is a rich collection of management and security features that only PolicyPak delivers.

- Eliminate local admin rights and block ransomware
- Manage Settings for more than 400 applications and browsers such as Chrome, Firefox, Java, and similar
- Manage multiple browser environments
- Manage multiple Java environments
- Manage Windows 10 File Associations
- Manage Windows 10 Start Menu
- Deploy any script throughout your MDM service
- Manage Windows Features and Optional Features

In the following sections, we show how PolicyPak MDM Edition can augment and improve the scope and power of your MDM service.

Simplifying Your Transition from Group Policy to MDM

If you want your MDM to deliver real Group Policy settings, PolicyPak MDM Edition makes it easy.

First off, editing is simple. You start by using the tool you know, the Group Policy Management console seen in Figures 1, 2, 3 and 4.

Then it's easy to configure Windows Security settings, Group Policy Preferences settings, or Administrative Templates settings. Additionally, you can leverage any existing third-party ADMX templates you're already using, expanding your management potential to hundreds of additional applications.

Once PolicyPak is installed on your management station, it merely integrates with the GPMC which is shown in Figure 5.

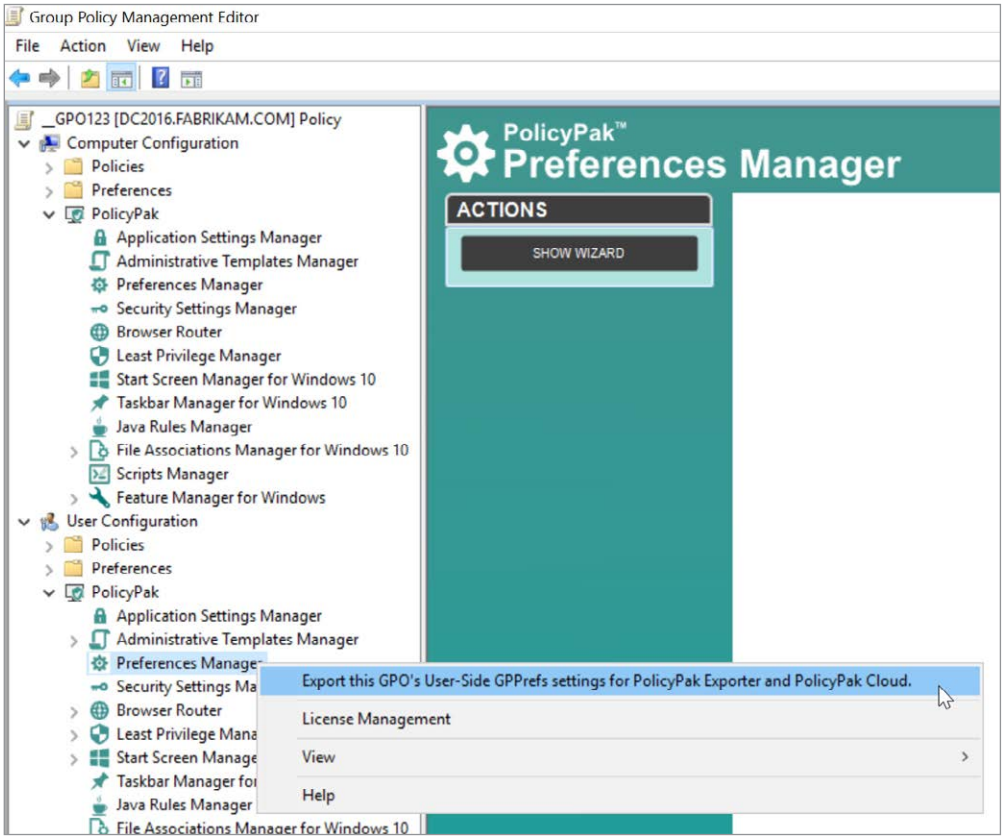

Figure 5: PolicyPak editors inside the Group Policy editor

Then you're ready to create real Microsoft Group Policy settings (or any extra PolicyPak settings) as usual within the Group Policy editor. When you're ready to deploy these settings via MDM, here's the process:

1. Upload the PolicyPak License and PolicyPak Client-Side Extension into your MDM service as .MSI files (you only need to do this once).
2. Export those the settings as .XML files using the GPMC.
3. Wrap up those .XML files into an .MSI file with the PolicyPak Exporter utility.
4. Upload the .MSI to your MDM service as an app.
5. Upload the PP license and Client-Side Extension.

You can see the result of these steps with MDM services like Workspace One and Microsoft Intune in Figures 6 and 7 respectively.

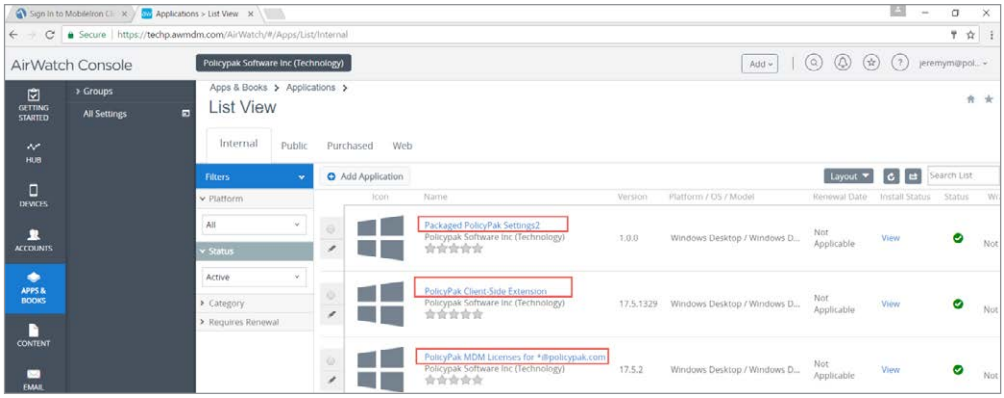

Figure 6: PolicyPak Client Side Extension, PolicyPak Licenses, and PolicyPak Settings uploaded into VMware Workspace One (formerly AirWatch).

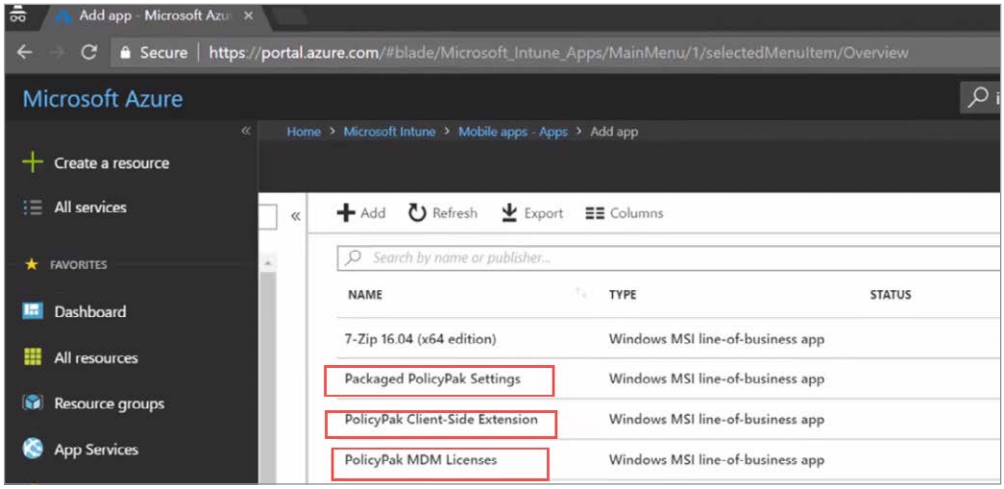

Figure 7: PolicyPak Client Side Extension, PolicyPak Licenses, and PolicyPak Settings uploaded into Microsoft Intune.

For demonstrations of how to apply real Microsoft Group Policy Settings in Intune, Workspace One, or to your MDM service, see the videos on this page: https://www.policypak.com/products/mdm-edition.html.

Establishing Least Privilege Best Practices and Extending the Power of Windows Autopilot

When you use Windows Autopilot to provision a new machine, the user on the device may be set up as a Standard User or a Local Admin.

Yes, it is easy to simply "give away" local admin rights for someone who is a standard user. But this is well known as a poor practice which lowers security and makes it easier for malware and malicious code to permeate your enterprise devices when users download anything using their admin rights.

That's why it is so important to enforce the principle of Least Privilege, which limits the damage of a compromised user account. However, how do you allow users to install approved applications or access allowed Control Panel applets if you strip them of local admin rights?

With PolicyPak, this is drop-dead easy. PolicyPak enables users to elevate applications as needed, perform installations, or bypass UAC prompts. Other actions that require local admin rights (where they shouldn't be given) would be installing printers, managing network cards, or uninstalling applications.

PolicyPak allows standard users the ability to complete administrative tasks without you having to hand over the keys to the castle—your full local admin rights. With PolicyPak, you can merely create settings, as shown in Figure 8, and choose what kind of permission you wish to grant.

Perhaps you want to provide standard users access to Device Manager (to update drivers) without having local admin rights, or enable that user to add printers. Similarly, you could allow users who are on the road to be able to download and maintain the latest version of iTunes or other sanctioned software.

The first step is to create a policy using PolicyPak Least Privilege Manager like what you see in Figure 8.

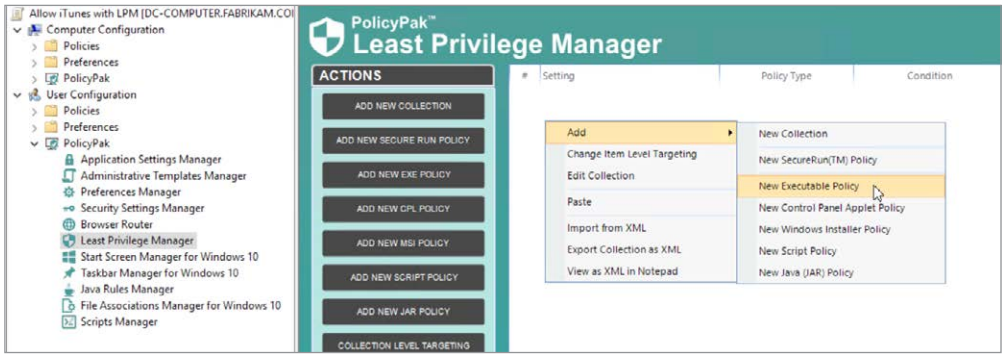

Figure 8: Creating a new PolicyPak Least Privilege Manager executable policy

Then, you can export the .XML, convert it to an .MSI and deliver it to your users using your MDM service.

For a video overview of Using Least Privilege Manager to elevate applications for standard users, see the following video: https://www.policypak.com/video/policypak-mdm-using-least-privilege-manager.html.

Preventing Malware on Your MDM-enrolled Machines

Many companies are turning to application whitelisting as a way to combat malware. Traditional whitelisting requires you to update the whitelist continually. A better approach is to allow or prevent access to applications based on who owns the application installation file.

PolicyPak SecureRun™ utilizes this approach. Applications that were not correctly installed by the admin, in-house software deployment tool, or your MDM service will just not run—unless the Admin says these applications are permitted. If an active user is not on the SecureRun Members list, PolicyPak Least Privilege Manager blocks all attempts to run or install any unapproved applications under that account. You can see the default members of the Secure Run Policy in Figure 9 and are able to add additional members as needed.

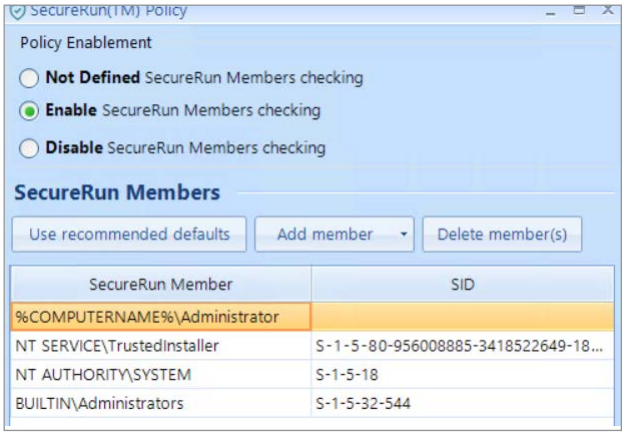

Figure 9: Defining who can (and cannot) run software helps you block malware attacks.

Again, once you create a policy, export it, wrap it into an .MSI, and upload it to an MDM service, you can then deliver and target the policy as you wish. This process applies to all policies created and used alongside PolicyPak MDM Edition and your MDM service.

For a video overview of how to isolate malware using PolicyPaK SecureRunTM, see the following video: https://www.policypak.com/video/policypak-mdm-using-least-privilege-managers-securerun-feature.html.

Managing Multi-browser Environments

Dealing with multiple browsers is a nightmare. Every browser wants to be the default, which drives your users crazy with pop-ups. Then there's the age-old problem of website incompatibility: not every web page renders as expected in all browsers. Users invariably choose the wrong browser for your company's go-to applications. If only there were a way to add order to all this madness.

Quiet the users and helpdesk tickets once and for all with PolicyPak Browser Router. PolicyPak Browser Router can enforce which browser is the default for your users, and put a stop to the endless prompts. The process is as easy as making a policy and clicking your desired default browser, like in Figure 10.

Figure 10: Use PolicyPak to define the default browser

Merely enforcing the default browser for users doesn't solve all the problems though. Again, some websites work better utilizing specific browsers. PolicyPak Browser Router offers URL assignment capabilities so that specific websites are launched only into specific browsers. Maybe you want:

- Your users' G-Suite portal site to always open in Chrome.
- Your IT team's Azure management console to always utilize Edge.
- Your users' timecard application to open in Firefox.
- Your intranet applications to open in Internet Explorer.

By making a PolicyPak Browser Router policy, then delivering it through your MDM service, even if a user tries to open an application with the "wrong browser," the application will still open in the right one.

For a video overview of how to get control of your multiple browser desktop environments, see the following video: https://www.policypak.com/video/policypak-mdm-map-the-right-website-to-the-right-browser.html.

Simplifying File Association Management

What if you want specific file types to open with a designated file handler such as Acrobat Reader for PDFs or Notepad++ for .XML files? PolicyPak File Associations Manager allows you to assign an application to specific file types.

Savvy readers might note that this functionality is in the MDM CSPs. However, to use it, the steps are:

1. Build a golden image with all your applications
2. Export the mapping file with DISM
3. Edit the file for the specific handlers you want.
4. Convert to base 64
5. Make a custom OMA-URI.

What's more, the MDM CSP that performs this work attempts to make the same file associations to all machines that get the profile. So if your users have Acrobat Reader and Acrobat Professional, what will it do?

PolicyPak makes it easy. Again, it all starts with making a policy using the Group Policy Management Console, as shown in Figure 11.

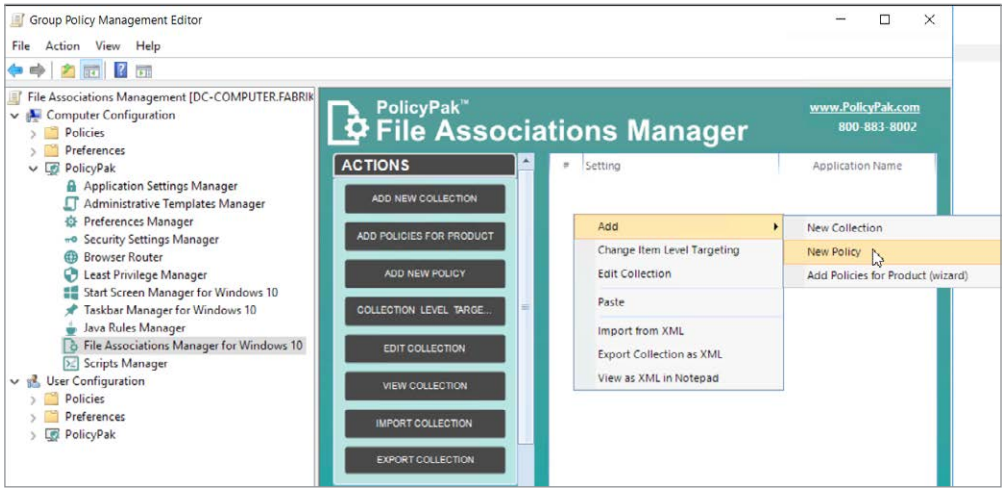

Figure 11: Using PolicyPak File Associations Manager to quickly create new associations

Then, the File Associations Manager can "detect" whether the application is actually on the machine before attempting to make the association. PolicyPak File Associations Manager easily handles multiple applications on the machine when they are vying for one association (remember our example of Acrobat Reader and Acrobat Standard are on the same machine).

For a video overview of how to ensure that all file types are assigned to the correct application, see the following video: https://www.policypak.com/video/policypak-mdm-file-associations-manager-helper-tool.html.

Start Screen and Taskbar Layout

To do so, you need to fully create (or re-create) a new machine and make a golden image. Then take that machine's hand-crafted start layout and export it as an .XML file. Then you need to import it into the Intune interface area, shown in Figure 12.

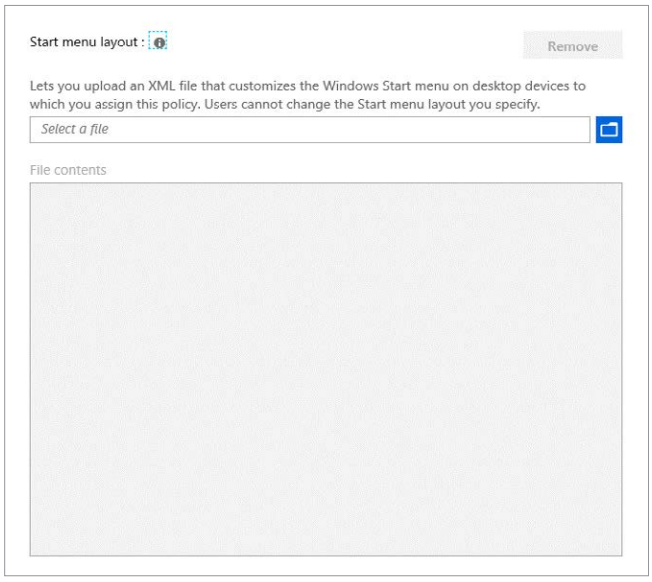

Figure 12: The Start Menu layout facility in Microsoft Intune.

This action works well when you need every Windows 10 device to get precisely the same applications.

In comparison, PolicyPak MDM Edition enables you to simply craft the layout with policy and export it, as shown in Figures 13 and 14.

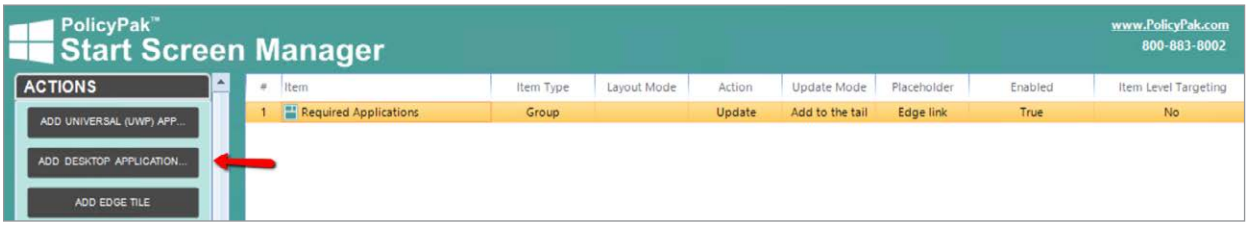

Figure 13: Quickly creating a crafted, flexible start screen with PolicyPak Start Screen & Taskbar Manager

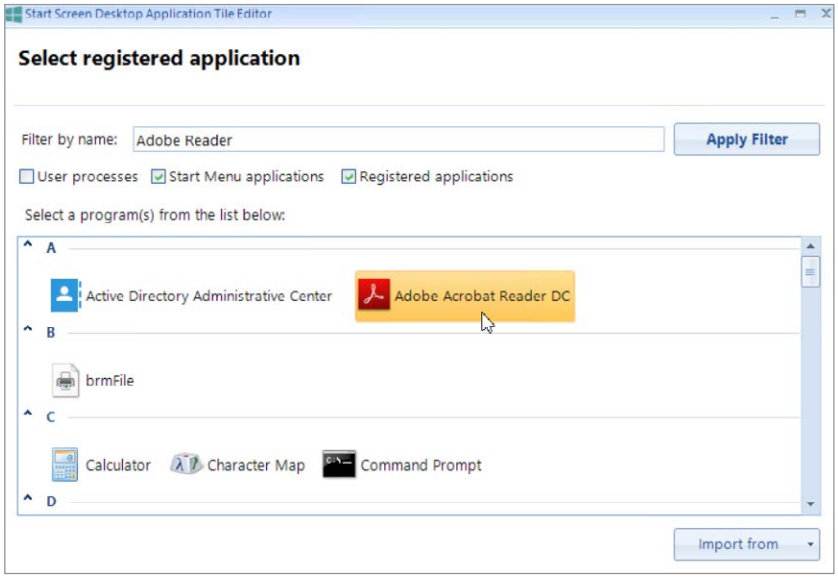

Figure 14: Selecting the application with PolicyPak Start Screen & Taskbar Manager

Because not every application is on every device, you can use PolicyPak's Item Level Targeting (ILT) to analyze what is installed on the Window 10 machine first, then present the correct Start layout, customized with only the applications and groups the user actually needs.

MDM's built-in Start Layout configuration facility has no ability like this. The result of using MDM's Start Layout configuration is that users end up with black holes in the groups, or groups that make no sense because the applications aren't on the targeted computer.

With PolicyPak MDM Edition it's unbelievably easy to dictate groups that have your Windows universal applications, desktop applications, or links to websites with Microsoft Edge.

For a video overview of how PolicyPak can help you regain control of the Windows 10 Start Screen for all of your devices managed by MDM, see the following videos: https://www.policypak.com/video/policypak-mdm-manage-the-windows-10-start-screen-like-a-boss.html and https://www.policypak.com/video/policypak-start-screen-manager-using-item-level-targeting.html.

Overcoming the Script Management Limitations of MDM

We have presented a lot of inherent challenges concerning MDM services, but the biggest one might be utilization of scripts. Because not every setting has a GUI, many MDM services are suggesting that IT admins leverage scripts to turn settings on and off, configure the operating system, and other items that "aren't ready yet" in MDM due to lack of CSP coverage. Therefore, scripts and MDM can be a necessary evil.

Depending on the MDM service you are using, there could be many limitations:

- Windows Intune only leverages PowerShell scripts (most existing scripts could be VB or batch file scripts.)
- For MobileIron customers, scripting requires a separate license.
- Scripts are typically run only once unless the script is updated.
- Scripts can only target computers, not users.
- The script must include all of the logic.
- There is no manual way to trigger the script to rerun.

Moreover, if you have existing VB scripts or batch files and want to target scripts at users, you're out of luck with your MDM service.

If we look at the Intune scripting interface itself, shown in Figure 15, it also doesn't offer many capabilities.

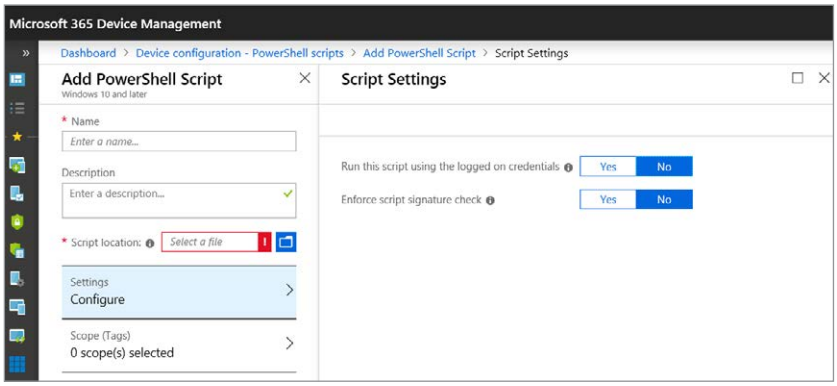

Figure 15: Microsoft Intune's PowerShell script delivery capabilities

With PolicyPak MDM Edition, you can forget about all of those crushing limitations. PolicyPak Scripts Manager enables you to:

- Works alongside any MDM service
- Target both the user and computer side
- Support multiple languages and file types, including .VB, .JS, .BAT, and PowerShell
- Apply the script more than once and retriggered whenever you want to
- Eliminate scripting size restrictions
- Deliver to kiosk machines which are Hybrid AD joined.
- Deliver scripts as needed for other unusual scenarios

Additionally, PolicyPak Scripts Manager provide a superpower that your MDM cannot offer. It can run a script when a condition is TRUE (or when the policy applies), then run a different script when that condition is FALSE (or the policy no longer applies).

What's more, you can use the granular powers of PolicyPak Item Level Targeting to target the exact machine, user, and circumstance for your scripts; for example, deploying it to Windows 10 laptop devices only, on a specific IP range, to a specific model of laptop.

In Figure 16, we've created a VB script to create a desktop shortcut for our users using PolicyPak Scripts Manager. First, we create a policy with the "On apply action" (as seen in Figure 16). Note the multiple script languages we can choose from.

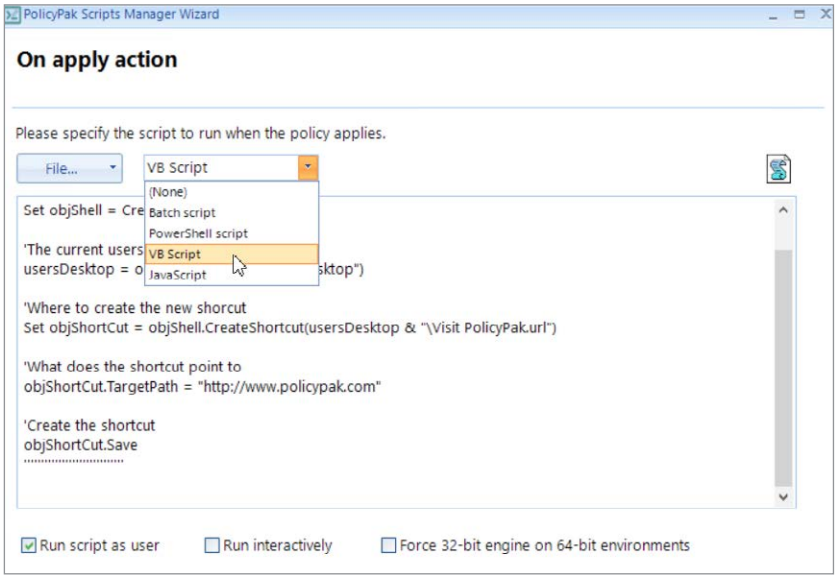

Figure 16: Delivering a script (of any kind) as an "On apply action" with PolicyPak Scripts Manager

Next, we place in the script that performs the revert action (which deletes the shortcut once the policy is out of scope) for the assigned users, as shown in Figure 17.

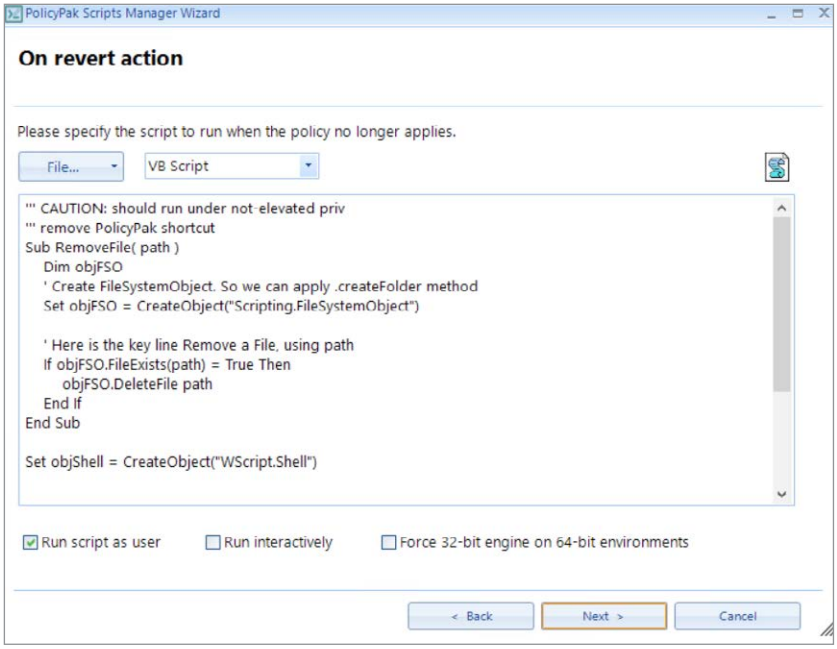

Figure 17: Delivering a script (of any kind) as an "On revert action" with PolicyPak Scripts Manager

Then we choose the run frequency for the script, shown in Figure 18.

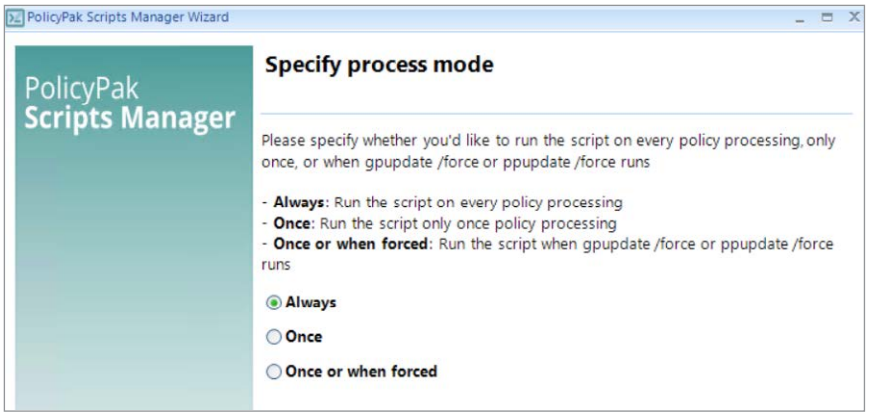

Figure 18: Choosing the run frequency of the script when deployed via PolicyPak Scripts Manager and your MDM service

Finally, we can add Item Level Targeting to apply the script according to our stated conditions, shown in Figure 19.

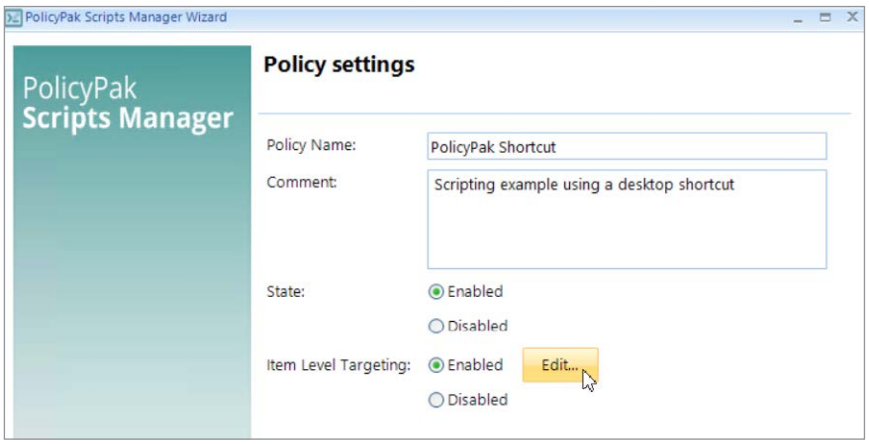

Figure 19: Using Item Level Targeting when deployed via PolicyPak Scripts Manager and your MDM service

In this case, we are going to choose users. Should a user leave the prescribed group, the revert script then runs and deletes the shortcut. Of course, ILT allows us to get far more granular than simple group assignment. We can target according to device type, IP subnet, operating system, computer name, and more, as shown in Figure 20.

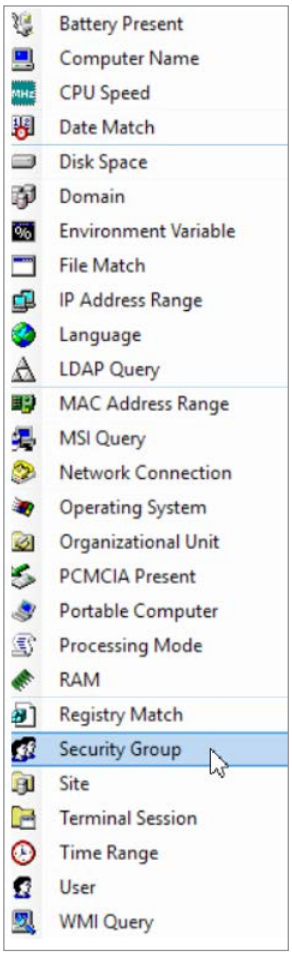

Figure 20: The PolicyPak Item Level Targeting options

For a video overview of how PolicyPak Scripts can significantly expand your scripting potential for whatever MDM service you presently have, see the following video: https://www.policypak.com/video/policypak-scripts-and-your-mdm-service-un-real-power.html.

Going beyond Autopilot to Add or Remove Features

Maybe you've investigated Autopilot with your MDM service. Autopilot enables an IT admin to deliver a fresh machine to an end user (typically from the factory) and Autopilot will make it ready for the user automatically. The MDM service downloads the .MSI or .MSIX applications, installs Office, lays down MDM policies, and so on, like what you see in Figure 21.

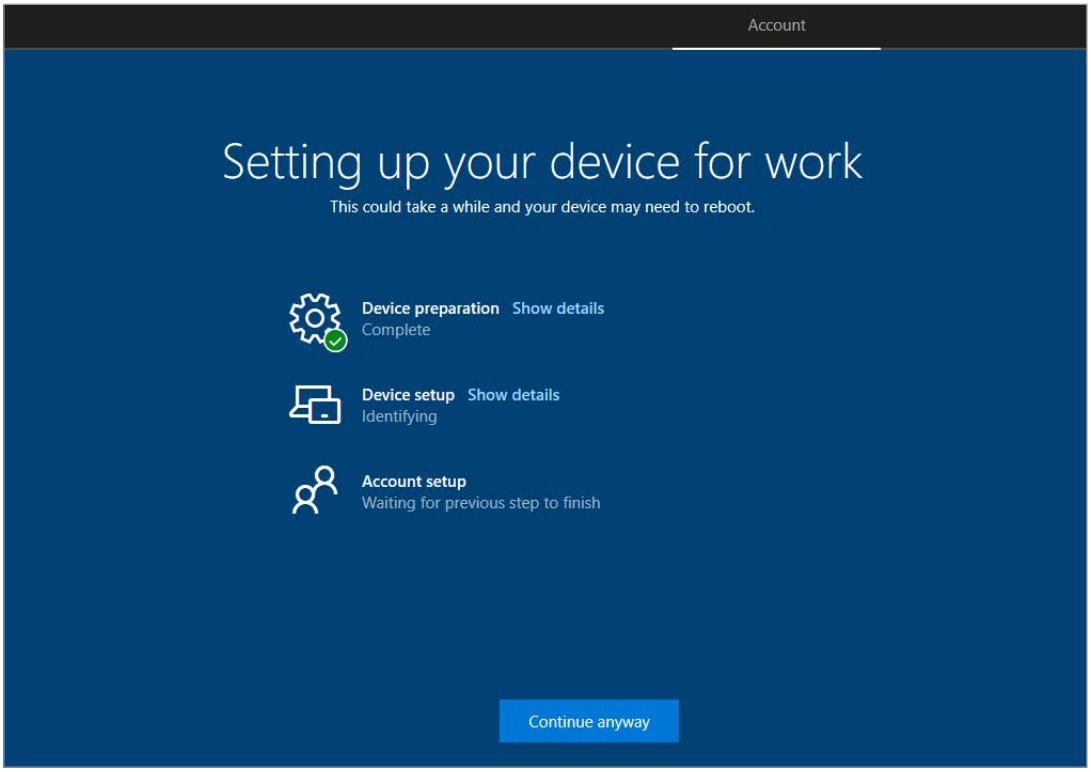

Figure 21: Autopilot setting up a new machine "Out of the box."

After Windows 10 is deployed (using Autopilot or otherwise), what happens when you change your mind and need to add or remove Windows 10 operating system features quickly?

Note that Windows 10 features split into two categories: Features and Optional Features, which you can see in Figures 22 and 23.

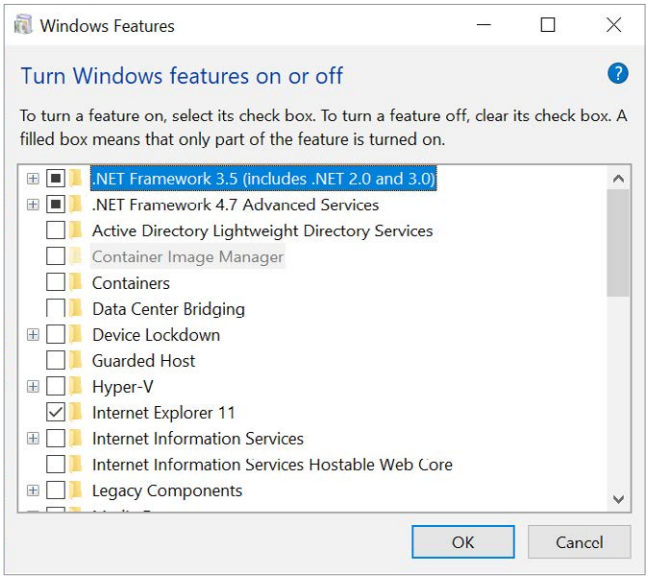

Figure 22: Windows 10 Features.

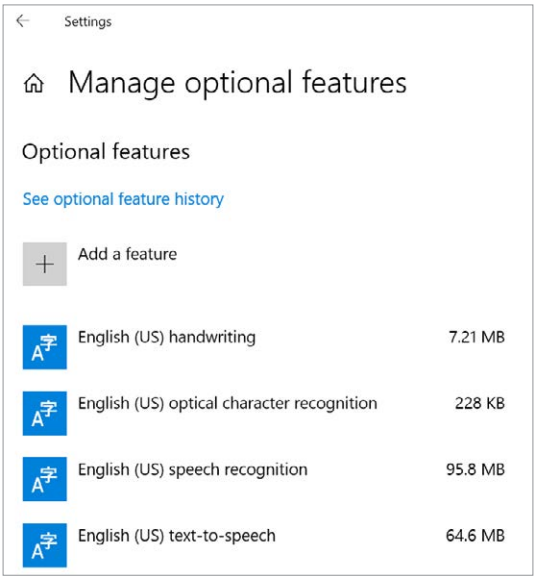

Figure 23: Windows 10 Optional Features

Installing or removing Features or Optional Features isn't directly possible with MDM. So if you're using Autopilot to deploy machines from the factory or your home base, then you have to figure out how to get your Features and Optional Features precisely tuned before that machine goes out the door.

However, if you're using PolicyPak Feature Manager for Windows with your MDM service, then this is, once again, drop-dead easy. Simply declare which Features and Optional Features to install or uninstall (remove), and that's it. You can see an example in Figure 24.

Export the settings and utilize within your MDM service, and your wish is granted.

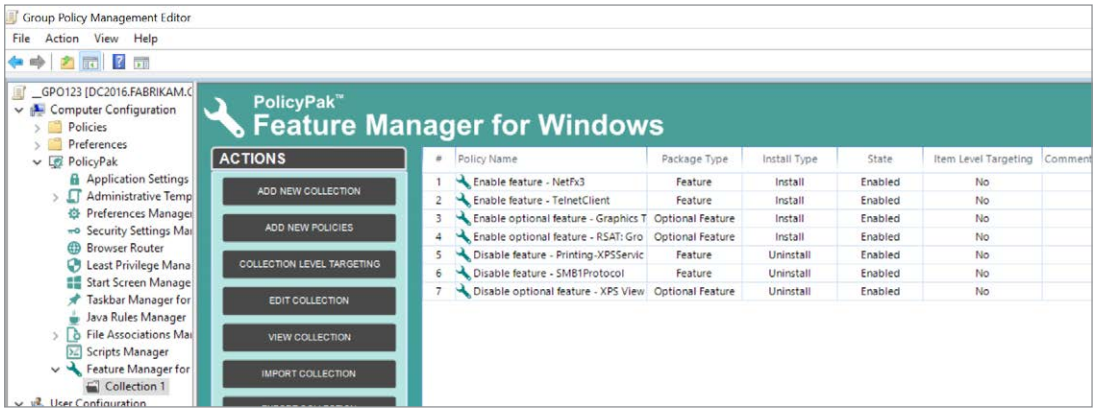

Figure 24: Quickly adding and removing features using PolicyPak Feature Manager for Windows with your MDM Service.

For a video overview of how PolicyPak Feature Manager for Windows can quickly and easily change the Features and Optional features on existing machines, or those recently deployed with Autopilot, see the following videos: https://www.policypak.com/products/feature-manager-for-windows.html.

WHY POLICYPAK AND WHY NOW

Whatever MDM service you currently use, PolicyPak MDM Edition can secure and manage the desktop beyond what you can do with your MDM service alone.

With PolicyPak MDM Edition, you can deploy real Microsoft Group policy settings to your MDM enrolled devices and selectively target them. You can easily import third-party ADMX files to give you near-blanket setting coverage over Windows 10, as well as over 400 applications.

There are also those extra settings that only PolicyPak can handle such as giving you full autonomy of the Windows Start Screen, managing application whitelisting with ease, and blocking malware that penetrates your multilayer security system. With PolicyPak MDM Edition, multi-browser environments are no longer a challenge, and scripting abilities are no longer constrained by the scripting engine your MDM provides.

We didn't build PolicyPak MDM Edition to replace your MDM, but rather to make it a whole lot better.

We recommended some videos throughout this paper, but for even more PolicyPak MDM Edition demos, head over to https://www.policypak.com/products/mdm-edition.html.

For a free trial of PolicyPak MDM, contact us at 800-883-8002, or head over to https://www.policypak.com/about-us/contact-us-for-a-trial-download.html.

PolicyPak®
SECURING YOUR STANDARDS.