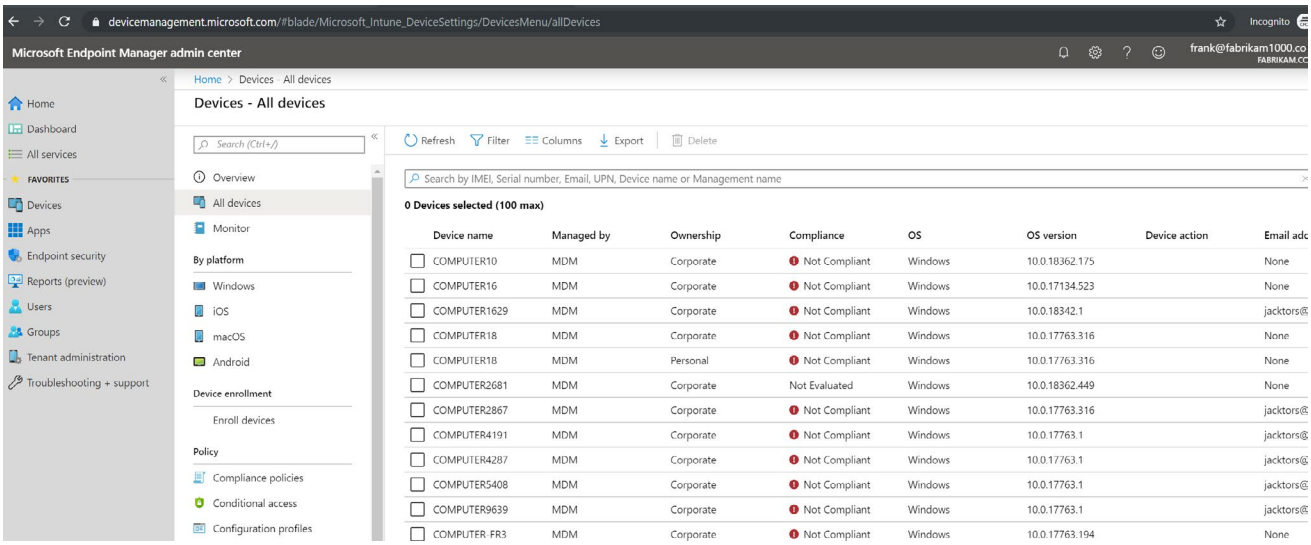
Why Microsoft Endpoint Manager Admins Need PolicyPak

PolicyPak®
SECURING YOUR STANDARDS™

In case you did not know, a significant merger was recently announced — not a merger between two companies, but of two technology management solutions within Microsoft. In recognition of the hybrid network architectures that so many companies contend with, Microsoft is rebranding ConfigMgr and Intune into one unified solution called Microsoft Endpoint Manager (MEM).

You can see a screenshot of MEM in Figure 1. An admin can now use their Intune web console to manage machines that are cloud-only with Intune, managed with ConfigMgr, or both.



With a unified view of both systems, Microsoft hopes to provide greater clarity to what has been a confusing state for so many organizations. In this paper, we examine the ramifications of this unified tool beyond its rebranding purposes and discuss how third-party solutions such as PolicyPak are required when managing and securing Microsoft-based enterprises.

Before we go there, let us look at how we got here.

MEM = Microsoft System Center Configuration Manager + Microsoft Intune

The Two Available Roads for IT Managers

Not too long ago, Windows-based enterprises arrived at a fork in the road, and IT managers have been struggling ever since with which one to take. One is a familiar road. It's one that utilizes on-premise administration tools such as ConfigMgr or Group Policy to manage AD environments. The other leads to that mystical place called "The Cloud." It is a place where we manage users and devices that reside in Azure AD, managed by MDM portal solutions like Intune.

So which road does one take?

The familiar road is a comfortable one. It is tried and true and has served Windows Admins well over time. However, it lacks the flexibility and scalability that companies urgently need as they attempt to digitally transform their organizations to attain greater agility, transparency, and empowerment.

The other road is the one less traveled, at least for now. At the rate that companies are rapidly migrating business-critical services to the cloud, however, it is rapidly expanding into a superhighway. Internal IT and Business leaders are seeking to integrate cloud intelligence to automate tasks and enhance the experience of their customers.

Microsoft now believes that regardless of which road one chooses, many arrive over time at the same destination. Microsoft expresses that there is a cloud-only management solution with Intune and Microsoft 365 at the center.

Few IT and business leaders doubt this inevitability, but transitioning to a cloud-centric universe is challenging, and it can be reasonably expected to take many years to get to the destination.

While the process of "lift and shift" certainly sounds easy, the process of migrating your on-prem IT estate to the cloud without having to re-structure your environment simply is not realistic. While in some ways we live in a "copy and paste" world, the reality of transitioning to the cloud for companies with legacy-strapped environments is proving to be a challenging endeavor for all but the smallest of companies.

The Promises of Microsoft Endpoint Manager

While Microsoft's plan may be for everyone to migrate their enterprise to the cloud, they have recognized that the majority of companies cannot migrate overnight. Microsoft VP Brad Anderson acknowledged this in a recent statement:

> *"Modern management does not mean cloud-only. It does not mean a migration away from ConfigMgr or migration to Intune."*

Significant innovative changes rarely occur overnight. Instead, they progress incrementally. Yes, companies may indeed arrive at the cloud as their eventual destination, but they do so at their own pace. For instance, some customers have more than 2,000 apps deployed, managed, and updated by ConfigMgr. They also have made significant investments in their ConfigMgr infrastructure. The truth is that the impending fork in the road referenced earlier cannot be an "either-or" decision. Instead, these roads run parallel to one another until the day arrives in which companies can consider abandoning their on-premise AD environment.

That is why Microsoft has now chosen to combine Intune (cloud management) and ConfigMgr (big boy management tool) under one umbrella. Microsoft Endpoint Manager is the convergence of Intune and ConfigMgr functionality and data—plus new intelligent actions.

Intune has been rebranded as Microsoft Endpoint Manager Microsoft Intune (MEMMI). ConfigMgr is now known as Microsoft Endpoint Manager Configuration Manager (MEMCM). Those organizations that do not currently utilize ConfigMgr will not witness any immediate changes other than the name change. However, current ConfigMgr customers will get an Intune license, giving them the ability to manage Windows 10 devices (phones and iOS devices are not included). This gives admins the ability to view their mobile devices, and ConfigMgr controlled PCs, within Intune.

There will be no more having to bounce repeatedly back and forth between interfaces throughout the course of the day. Note that you will need an Azure P1 license for your users.
MEM is a modern comanaged system solution for your Windows 10 devices designed to manage the modern workplace of today. Microsoft is emphasizing that this is a comanaged solution that is not a temporary or transitory solution. Says Anderson once again,

> *"... this vision includes both ConfigMgr and Intune,"*
> *"Co-management isn't a bridge; it's a destination."*

In other words, it's okay to be on-prem, and it's okay to be on the cloud, and it's a lot simpler to deal with this duality with MEM.

Upcoming Innovation in Microsoft Endpoint Manager

The benefits of this new co-managed solution go far beyond branding and licensing simplification. Microsoft will unveil a stream of new tools and components through MEM. For instance, Microsoft will soon release a "CSE TOOL," which customers can add-into any MDM deployment (not just Intune) and will accept some directives and poke at SOME Microsoft Group Policy CSEs. Initially, this will include:

A. DRIVE MAPS

B. NON "MICROSOFT POLICIES KEYS" IN REGISTRY

C. AUDITING

Microsoft will likely increase the CSE TOOL coverage over time, and other MDM providers (Workspace One, Citrix CEM, etc. . . .) can hook into it and do "more Group Policy-like things," using MDM as the transport. This means that the engineering on CSPs can grow over time, while admins continue to use some of their Group Policy know-how.

Microsoft will also be releasing an add-on to MEMMI, which will allow customers to import their GPO backups and into MEMMI for evaluation. If any settings are supported in MEMMI, they will be converted from their Group Policy settings to something that MEMMI can deliver via MDM CSPs.

All of this is further indication that Group Policy is here to stay because they cannot rip out the "Group Policy guts" within a Windows client or server and have the CSE Tool continue working.

Microsoft has already stated that bringing over the bulk of Group Policy operations is not part of Intune's design goals.

So, being conscientious of what is possible in Group Policy and MDM land will be required for a long time in making important decisions about what to do about that gap.

It is a big deal that the cloud is now brought down to ConfigMgr because the cloud means intelligence. There are currently over 190 million devices managed by Intune and ConfigMgr.

That gives Microsoft cloud-scale-learned insights that customers can then leverage to improve the end-user experience. MEM will be introducing an array of intelligent actions that will give admins granular analysis as well as new comparative insights to their environments versus others.

One example of this is Productivity Score. Productivity Score will allow organizations to evaluate their employee and technology experiences in measurable metrics that internal IT can use to justify the value that it brings to the organization. From the perspective of the user experience, it will quantify how people are collaborating on content, developing a meeting culture and communicating with one another. Real measured results concerning these types of user experiences can offer insights into how to enhance the user experience and increase productivity. The technology experience will provide insights into assessing policies, device settings, device boot times, application performance and security compliance.

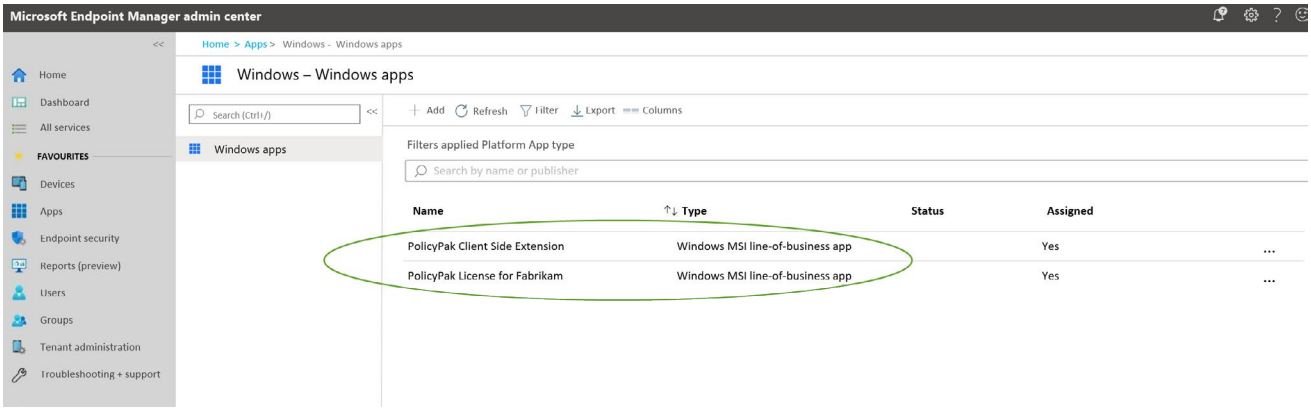
Using PolicyPak to Augment Microsoft Endpoint Manager

If you are accustomed to having access to the more than 10,000 real Group Policy and Group Policy Preference settings available in Windows Server AD environments, then Intune (or any MDM) will end up being a bit of a disappointment. MDM solutions such as Intune do offer some key advantages over Group Policy and Group Policy Preferences, such as the ability to manage devices off-premise and remote wipe mobile computers believed to be compromised.

Still, the disparity between the two with regards to configurable settings is immense. In order to fill this gap, enterprises will be required to augment MEM with PolicyPak to attain the best of both worlds.

PolicyPak has the PolicyPak Group Policy Edition (aka On-Prem Edition) and also the PolicyPak MDM Edition, which are licensed together. Therefore, no matter which road you're on now or what road you're headed toward, the PolicyPak solution works with you.

The PolicyPak "moving part" (called a Client Side Extension) and the PolicyPak License file are simply MSI files that are easily deployable using MDM (ConfigMgr or Intune), as seen here.



Once PolicyPak is deployed, you can receive PolicyPak directives from Group Policy or MEM (ConfigMgr or Intune.)

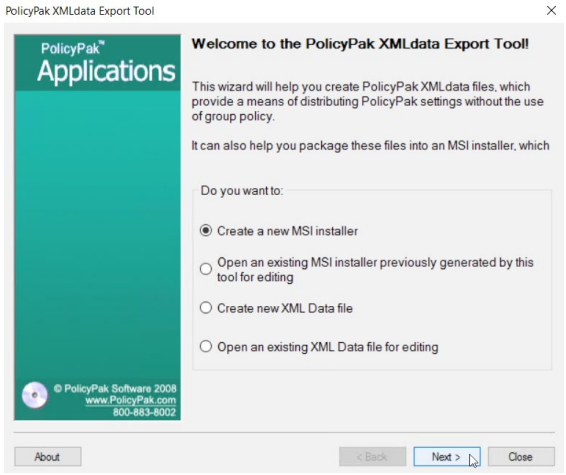
PolicyPak: Migrating existing on-prem Group Policy settings to MEM

Because MEM cannot deploy all the Group Policy and Group Policy Preferences settings that customers want (nor is it a design goal of MEM to do so). This leaves a gap for customers to fill. Thankfully, it's quite easy to use PolicyPak to export existing Group Policy settings and enable them for use with MEM.

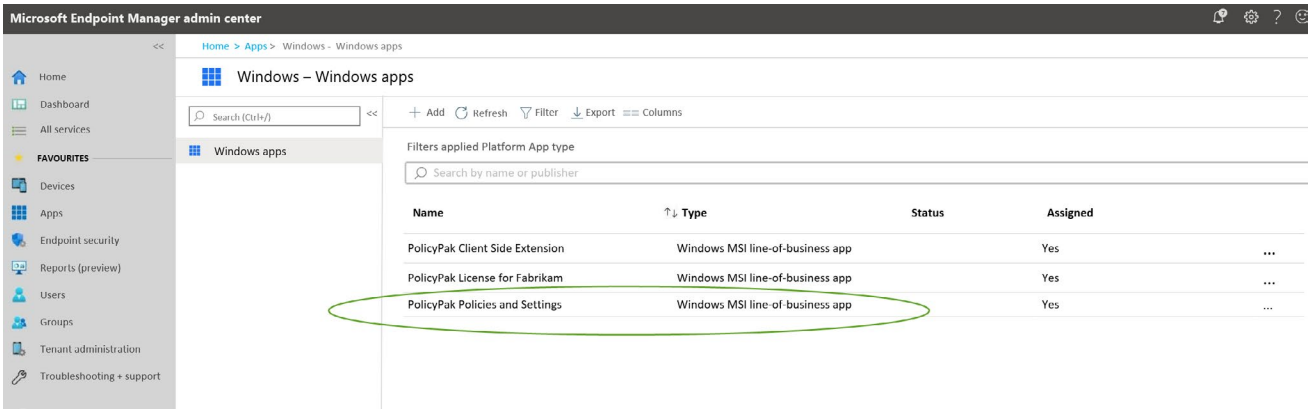
PolicyPak has three components that let you export existing on-prem Group Policy settings:

- PolicyPak Admin Templates Manager lets you export Microsoft Group Policy and third party ADMX settings.
- PolicyPak Security Settings Manager lets you export Microsoft Group Policy Security settings.
- PolicyPak Preferences Manager lets you export Microsoft Group Policy Preferences settings.

Once exported as XMLs, you can wrap up the settings as an MSI file using the PolicyPak Export Tool, as seen in Figure X.



Once wrapped up into an MSI, the previously exported settings can be deployed as an MSI via MEMMI, as seen here.



For a quick overview video of exporting on-prem Group Policy items and using them with MEM, see this video: https://kb.policypak.com/kb/article/482-policypak-and-microsoft-intune/

PolicyPak: Beyond just Group Policy to MDM Migration
(and used for ongoing management)

Yes, PolicyPak is often used to fill the important gaps that many enterprises need to fill within their MDM environments when migrating GPOs. Beyond the gaps between Group Policy and MDM, what else does an MEM administrator need?

Just because you're leaving the bonds of on-prem behind, doesn't mean that your security and management challenges magically fade away.

Immutable Windows Truths

- Your apps are your still your apps.
- Your users are still your users.
- Your browsers are still your browsers.
- Windows is still Windows.

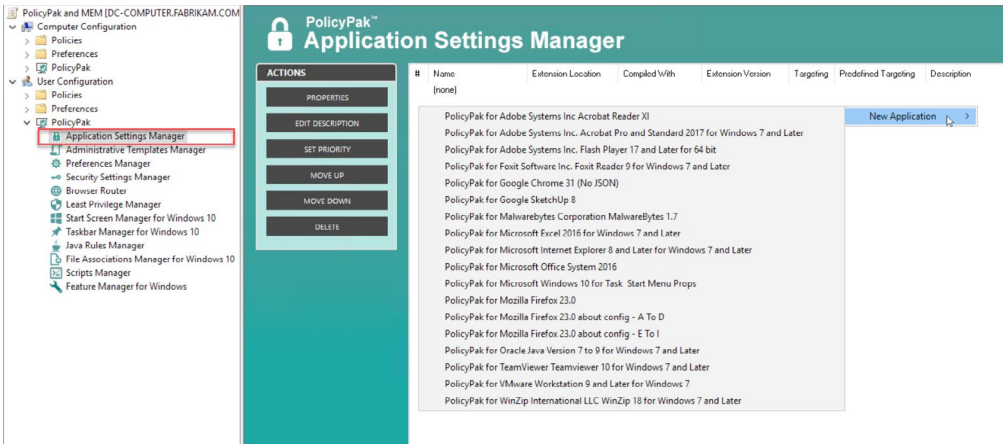
Let's see how PolicyPak can help you on-prem, in the cloud, or both.

Your Apps are Still your Apps: Manage them with PolicyPak Application Manager

No matter how you deploy and manage Windows, you'll always have applications to manage on Windows 10, and users are going to want to work around your IT standardized configuration.

The PolicyPak Application Manager enables you to deliver and enforce configuration settings for third party applications. The PolicyPak Applications Manager provides group policy settings for some 500 applications, including Firefox, Java, Flash, IE, and Adobe products.

PolicyPak Application Manager can ensure optimal application experiences for your users every time. It can also eliminate gaping security holes that these settings can create, if left accessible to standard users, by locking them out.

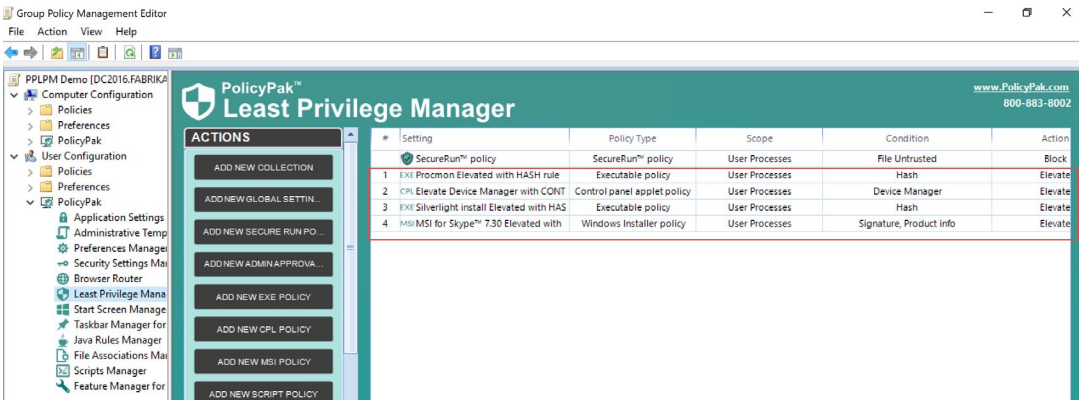


You can manage your applications on-prem, via GPOs or ConfigMgr, or export these settings for use via MEMMI.

Your Users are Still Your Users: Manage them with PolicyPak Least Privilege Manager

Your users beg to be local admins to run key applications. Without local admin rights, some applications won't run, install, or upgrade.

PolicyPak Least Privilege Manager enables you to remove local admin rights safely, yet enables applications to run as designed. You can see PolicyPak Least Privilege Manager with application elevation and whitelisting rules as seen here.



You can see a quick demonstration of how to enable standard users to install MSI applications and overcome UAC prompts when needed **(Click Here)**.

Users continue to download unknown files from the Internet. This makes it drop-dead easy for the bad guys to get a toehold on one machine, or worse, your whole network. PolicyPak provides one-click whitelisting to stop a huge array of malware attacks.

To see a video demonstration of a PolicyPak SecureRun™ check, **click here**.

We've only scratched the surface of the potential of PolicyPak Least Privilege Manager.
A couple other capabilities worth noting include:

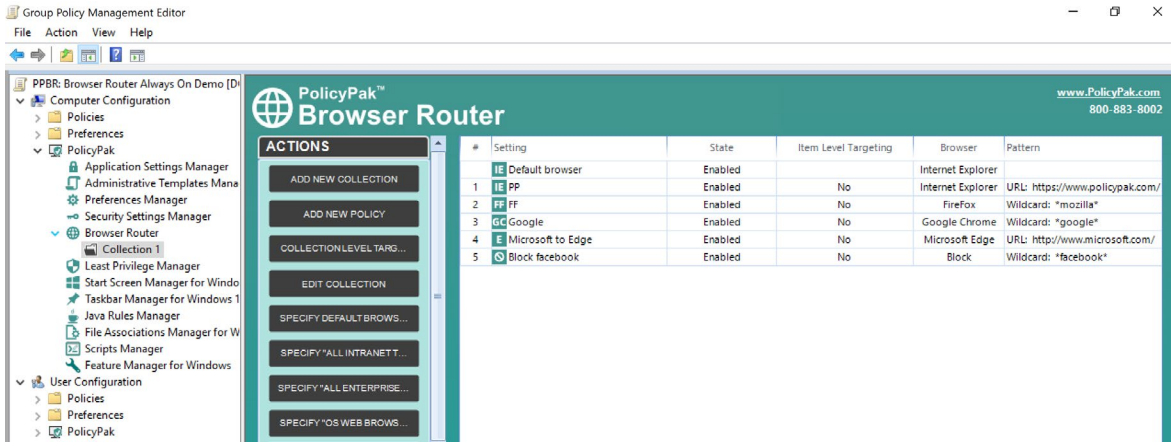
- Give standard users access to certain Control Panel applets (**Click here** to see a video demonstration of this capability).
- Overcome Network Card, Printer, and Add/Remove Programs UAC prompts (**Click here** to see a video demonstration of this capability).
- Block or allow Windows Universal applications (**Click here** to see a video demonstration of this capability).
- Performing "Over the phone" approval for elevation (**Click here** to see a video demonstration).

Again, all policies created by PolicyPak Least Privilege Manager can be delivered through MEMCM, MEMMI, or Group Policy. Computers can be domain-joined or even non-domain-joined.

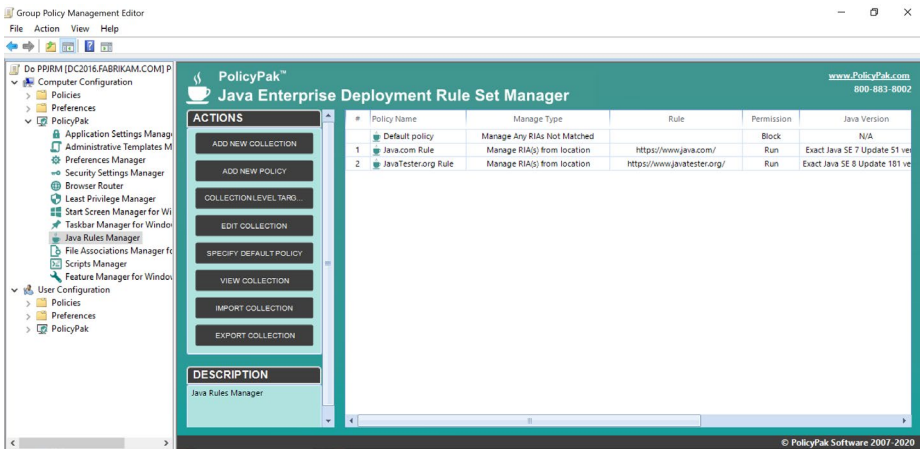
Your Browsers are Still Your Browsers: PolicyPak Browser Router and PolicyPak Java Rules Manager

Your organization may depend on certain websites that may only work on a certain browser, maybe even an older version. Once your machines are rolled out, how can you make some websites open in Chrome, others in Edge, others in Firefox, and others in Internet Explorer? And if you change your mind about what the default browser should be (perhaps migrating from IE or Chrome to Edge Chromium), how would you do this?

PolicyPak Browser Router helps you get a handle on your multi-browser environments by allowing you to map designated websites to the desired browser. It also lets you dictate a specific Default Browser so users are not prompted (and help desks are not called). You can see the PolicyPak Browser Router configured as seen here.



Moreover, how can you manage Windows machines when they need security plus to access Java applications? Java Rules Manager lets you map the right website to the right version of Java via the Deployment Rule Sets. It will block the unknown Java applets with untrusted websites while allowing th e good ones to work with the Java you already have. Configuration to lock down Java can be seen here.



Windows is still Windows: PolicyPak Start Screen & Taskbar Manager, PolicyPak File Associations Manager and PolicyPak Feature Manager

Once you have your Windows 10 machines rolled out and "out there," what happens when corporate needs change and applications are upgraded, added or removed? With PolicyPak, three features work together to ensure that the Windows 10 environment is managed dynamically, on-prem or via MEM.

POLICYPAK FILE ASSOCIATIONS MANAGER:

Quickly map which application to open with which file type, and keep these associations applying even if the user changes them or the computer goes offline. You can see the PolicyPak File Associations Manager configured below. (**Click here** to see the power in a video.)

POLICYPAK START SCREEN & TASKBAR MANAGER:

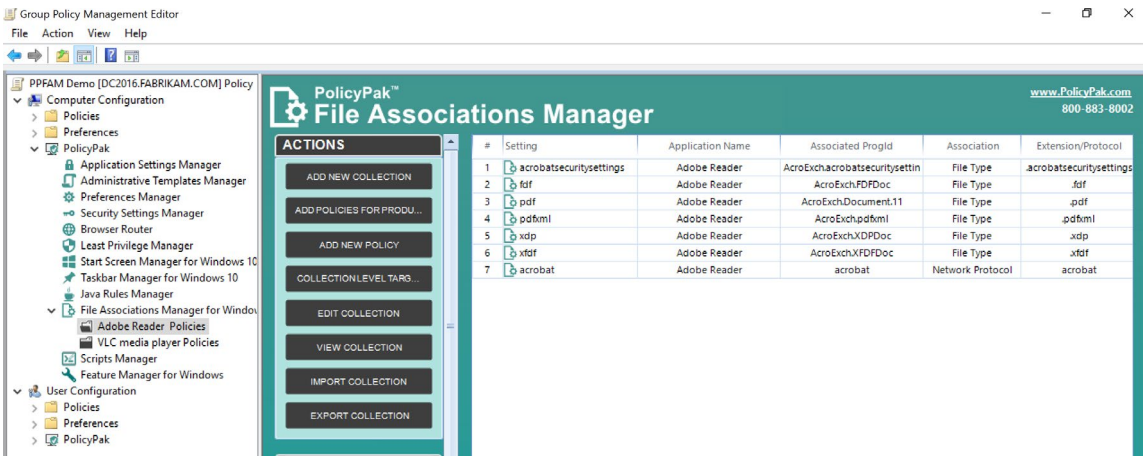
Take total control of your users' Windows 10 start screens and taskbar. Place Windows Desktop, Windows Universal apps, and Edge tiles into your desired start screen groups and keep them locked down so users cannot alter them. You can easily pin or remove applications from the Start menu or Taskbar. (**Click here** to see the power in a video.)

POLICYPAK FEATURE MANAGER FOR WINDOWS:

If you roll out machines with Autopilot, you don't have to take Windows' default feature set. PolicyPak Feature Manager lets you dynamically configure your desktops with the exact features you want in real-time once the policy is applied. All of this happens in the background, and reboots can be postponed to an opportune time. (**Click here** to see the power in a video.)

POLICYPAK SCRIPTS MANAGER:

Yes, Intune lets you deploy scripts, so long as they are PowerShell. PolicyPak Scripts Manager lets you run PowerShell, JavaScript, Visual Basic, and Batch scripts and target your users or computers. Run scripts with user or system rights, interactively or silent. You can even specify the "On" and "Off" script. (**Click here** to see the power in a video.)



All roads lead to PolicyPak

No doubt, MEM will bring much-needed functionality and provide necessitated clarity and simplicity when it comes to management and licensing. Even more importantly for Microsoft, MEM will encourage enterprises to accelerate their move to the cloud.

Although it will take time, maybe many years, Microsoft will increase Intune coverage for some Group Policy settings, but still, others might never make it into the cloud.

In the meantime, PolicyPak will continue to fill this gap, as well as provide you with other must-have tools to ensure that the user's desktop experience is optimized and secure.

While MEM may address the impending fork in the road for so many enterprises, it has never been a problem for PolicyPak customers.

Regardless of which road you take, PolicyPak is ready to work on-prem or with MEM.

ABOUT THE AUTHOR

Jeremy Moskowitz is a 15-time Microsoft MVP for endpoint management and enterprise mobility using Group Policy and Modern Device Management. Jeremy's published works include Group Policy: Fundamentals, Security and the Managed Desktop (Copyright © 2015 by John Wiley & Sons., Indianapolis, Indiana) and MDM: Fundamentals, Security and Modern Desktop (Copyright © 2019 by John Wiley & Sons., Indianapolis, Indiana). Jeremy Moskowitz is the CEO and head instructor for MDMandGPanswers.com, which has enrolled over 16,000 students and is the founder of PolicyPak Software, which manages and protects nearly 2 Million endpoints worldwide.

ABOUT POLICYPAK SOFTWARE

PolicyPak is a modern desktop management solution for on-premises, MDM, and cloud. PolicyPak enables enterprise IT teams to easily configure, deploy, and manage policies that keep users and computers secure and productive regardless of location. Unlike other management options, only PolicyPak allows Windows administrators to lock down, customize and target settings for local admin rights, applications, browsers, Java, the Windows 10 Start Menu and Taskbar, File Associations, scripts, and more. PolicyPak can also consolidate the number of GPOs in a Windows environment and migrate GPOs to MDM. Whether an organization relies on traditional management tools like Active Directory, Group Policy, and ConfigMgr, modern tools like Azure AD and MDM, or no management tool at all, PolicyPak delivers the settings they need to be successful today and in the future.