PolicyPak Manifesto: Why PolicyPak Exists and Its Top Superpowers

PolicyPak doesn't have to exist. But then over two million Windows PCs would be less secure and less managed, and administrators wouldn't be able to do their jobs to make Windows more secure and managed.

PolicyPak instantly makes your Windows system more secure while keeping your applications, browsers, operating system security settings and data governance settings in compliance. PolicyPak becomes a supercharger for your existing investment in Active Directory & Group Policy for on-prem users or your existing MDM service like Windows Intune for remote users. If you have no infrastructure at all, you can use PolicyPak Cloud as your supercharger.

In this paper, we will share with you our PolicyPak's superpowers so you can decide if you want to supercharge your Windows settings and security management via Group Policy, MDM or PolicyPak Cloud.

> *"To protect our resources, we must implement a number of federal security mandates. Not only does PolicyPak make it easier, but in some cases, we would have no way to implement the mandated settings without it."*

- Jamie Hosley
Computer Specialist, Desktop and Device Engineering Solution Delivery,
US Department of Veterans Affairs

PolicyPak®
SECURING YOUR STANDARDS™

PolicyPak Policies: Where the Superpowers Begin

PolicyPak's Policies add on to Windows management where Group Policy and MDM simply cannot. Said another way, if Group Policy, MDM, or an RMM tool could do what PolicyPak could do, then PolicyPak wouldn't need to exist. However, since they cannot, PolicyPak becomes an important tool for your PC management.

In Table 1, you can see a summary of PolicyPak's Policies.

Table 1: PolicyPak Components

PolicyPak Policy	Summary
Least Privilege Manager	Eliminate local admin rights and block malware.
Device Manager	Block USB & CD-ROMs from malware and data exfiltration.
File Associations Manager	Map extensions to applications (PDF to Acrobat and more).
Feature Manager	Add/Remove Windows 10 / Server Features on Demand
Start Screen & Taskbar Manager	Place and lock application icons.
GPO Compliance Reporter	Ensure your GPOs are effective on endpoints.
Application Settings Manager	Secure Browsers and applications (Firefox, Java, etc).
Browser Router	Map websites to specific browsers .
Java Rules Manager	Map websites to specific Java versions.
Software Package Manager	Deliver and Remove Windows Store applications.
Admin Templates Manager	Reduce GPOs and eliminate loopback.
GPO Export Manager	Export all GPOs for use with non-domain joined machines.
Scripts & Triggers Manager	Run interesting scripts when you need them
VPN Manager	Set up VPN and Always-On-VPN Connections
RDP Manager	Deliver .RDP files to users for remote work

PolicyPak: Understanding and Choosing your Edition(s)

PolicyPak enables you to increase your coverage for your on-prem and remote work scenarios. You can choose from three editions of the product.

Below is a quick cheat-sheet to enable you to decide which version or versions you need. For additional information on choosing an edition, you can go to the PolicyPak purchasing page for a detailed video and solution matrix.

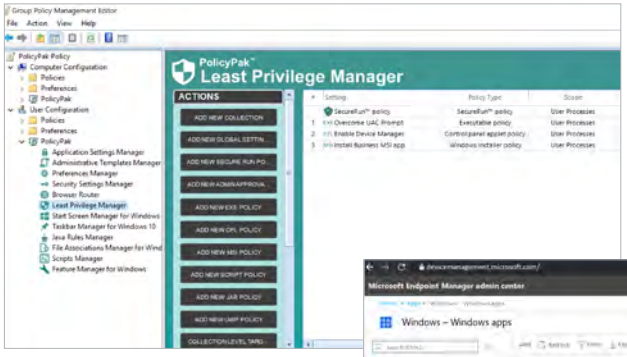
PolicyPak
Enterprise Edition
comes with every Pak, every solution, and priority support – everything is included.

PolicyPak
Professional Edition
is flexible, extensible, and completely customizable - designed to grow as your needs change.

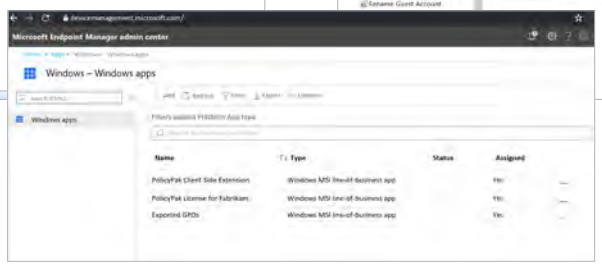
PolicyPak
SaaS Edition
is 100% cloud with monthly or yearly billing – ideal for MSPs, IT teams, and managing non-domain joined computers.

In the figure below, you can see PolicyPak utilized with how your IT department already works.

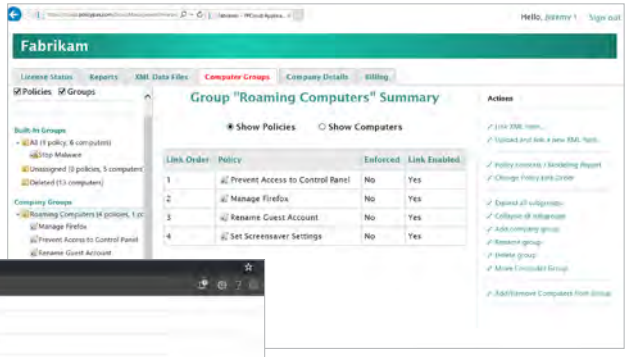
PolicyPak's superpowers originate in our Policies, but instead of describing each one-by-one, in the following sections we'll investigate the results you can expect to see by using PolicyPak, such as increased security and better system management.



PolicyPak integrated with Active Directory & Group Policy.



PolicyPak integrated with Microsoft Endpoint Manager (MEM) (or any MDM service.)



PolicyPak Cloud delivers settings if you have no infrastructure at all.

Figure 1: PolicyPak Editions work the way you already work.

PolicyPak: Top Security Superpowers

In this section, we'll review the top ways to increase your security – things that Group Policy, MDM, or an RMM tool simply cannot. We'll see how PolicyPak can:

- Remove local admin rights
- Automatically block ransomware and unknown-ware
- Automatically block USB & CD-ROMs for inbound ransomware and outbound data exfiltration
- Take control of Java websites
- Manage and secure your browsers
- Manage and secure your applications and middleware

Let's see how these items can increase your security to your on-prem and remote workers.

"I like PolicyPak because it's very lightweight. Just add to Group Policy (or MDM) and go! It just works with what you already have, is very powerful and very easy to use."

- James Rankin
Citrix CTP, VMware vExpert, Formerly known as "AppSense Bigot"
james-rankin.com, @james_rankin

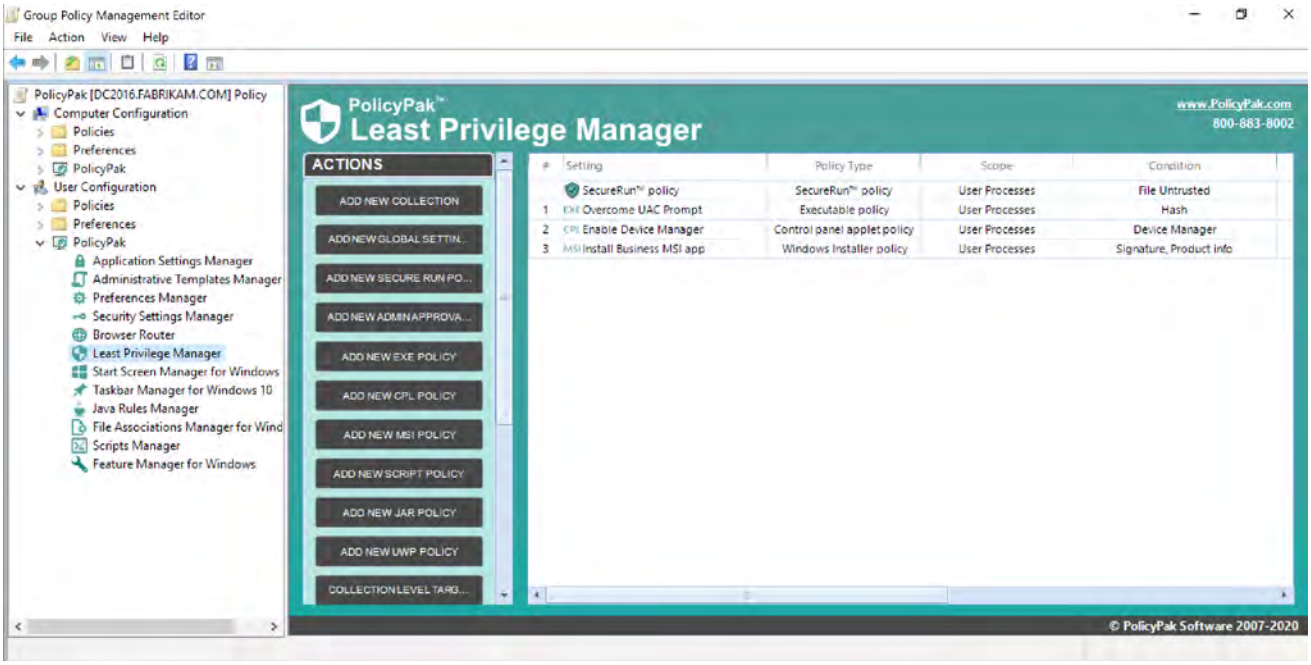
Security Superpower #1: Remove Local Admin Rights

Microsoft recommends restricting local administrator accounts on workstations and servers. This advice has been around since at least 2004 from this Microsoft blog post. Local admin accounts are what the SANS Institute refers to as the "keys to the kingdom." Hackers and bad guys need those accounts to embed your machines with their malicious code. Once a beachhead is established, they can then carry out their missions. Yet, IT admins routinely give away these keys to the kingdom.

According to a 2018 survey of 500 organizations conducted by PolicyPak and MDMandGPanswers.com, the number one reason why enterprise admins assign local admin rights to machines is to enable end-users to install applications which require local admin rights to install. Other top reasons include overcoming UAC prompts when running older software and/or managing operating systems.

With PolicyPak's Least Privilege Manager, you no longer need to give away local admin rights. PolicyPak's Least Privilege Manager enables you to make rules to overcome UAC prompts for Standard Users, enabling them to do their job, without you needing to give away control. Simply create the rules you need, like what's seen in Figure 2, and your Standard Users are up and running, overcoming UAC prompts in no time flat.

Figure 2: Creating rules in PolicyPak Least Privilege Manager to overcome UAC prompts



"I knew I had a hard job ahead of me to eliminate admin rights in an effort to better protect the company. Now I am simply flat-out more secure, with happy users, who can download and run sanctioned web conferencing software, update their own drivers, or install our home-grown software (that constantly changes). Never before have I used a product like PolicyPak Least Privilege Manager that was as easy to use as the demo indicated… it worked exactly like the videos on the website!"

- Jeremy Friesen
IT Network Administrator
Geoprobe Systems

Additionally, with PolicyPak Least Privilege Manager, you can enable users to perform three very special functions:

- Install their own local printers
- Change their network card settings (e.g. DHCP to static IP)
- Uninstall specific software

These tasks are only available when the user is an admin. But with PolicyPak, you don't have to give admin credentials to do these admin-like things. With the 2011 "Printnightmare" patches, Microsoft has even locked "Click to Print" such that only local admins may install network printers. PolicyPak customers already have the "get out of Jail free" card to enable them to move onward.

You can see how PolicyPak overcomes the Printnightmare problem in this video.

In Figure 3, you can see the PolicyPak Least Privilege Manager Helper Tools which can be made available to users to overcome these very real challenges when you remove local admin rights.

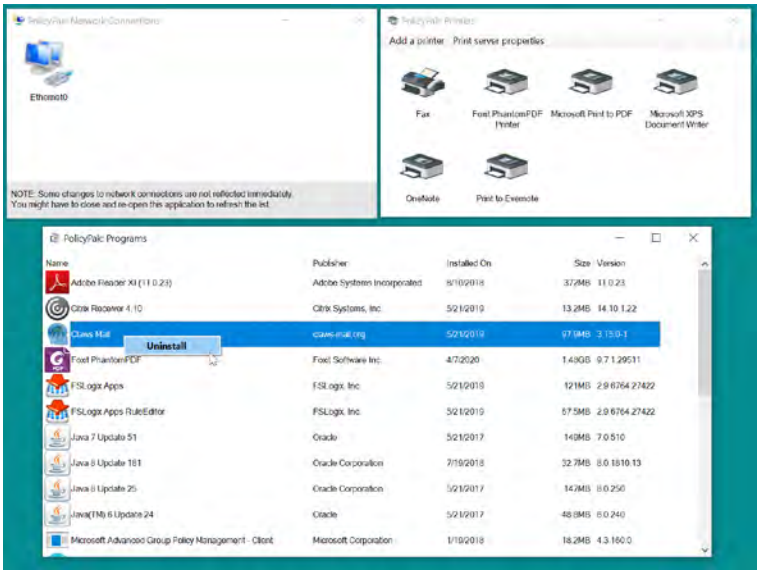


Figure 3: Enable Standard Users to install local printers, change network card settings, and uninstall software.

Security Superpower #2: Automatically Block Ransomware and Unknown-ware

Users love to click on things. And when they do, programs launch – good, sanctioned programs and, evil, unsanctioned programs. The last thing you want from a user, whether on-prem or remote, is for them to click on something unsanctioned and for the whole computer to be locked up like the scenario depicted in the screenshot in Figure 4.

Figure 4: WannaCry presentation to the end-user after he or she clicks on malware.

Inside Windows, Microsoft provides a decent whitelisting solution called AppLocker. AppLocker can work for some small environments, but there are some challenges. The main challenges are:

- AppLocker is not available for the Pro editions of any of the Windows operating systems.
- It can easily be subverted by anyone with admin rights to their device.
- It requires constant care and attention by an already over-extended staff.
- You cannot specify user and computer side policies.

This is where PolicyPak can step in. The table below compares the functions of PolicyPak's Least Privilege Manager to AppLocker.

Goal	Microsoft AppLocker	PolicyPak Least Privilege Manager
Prevent users from running naughty items	Yes	Yes
Enable transition from Admin users to Standard Users	No	Yes
Prevent users from executing malware	Partial	Yes
Once admin rights are removed, elevate applications and situations	No	Yes

Table 3: Comparison of PolicyPak to AppLocker

The biggest issue with AppLocker is managing the rules. Ask any AppLocker admin, and they will profess that their whole day revolves around dealing with AppLocker exceptions. Conversely, with PolicyPak Least Privilege Manager and SecureRun™, applications are automatically locked down based on the file owner.

In Figure 5, with PolicyPak SecureRun™ on the job, you can see that the sanctioned Adobe Reader app is able to run. But unknown apps and scripts are automatically blocked.

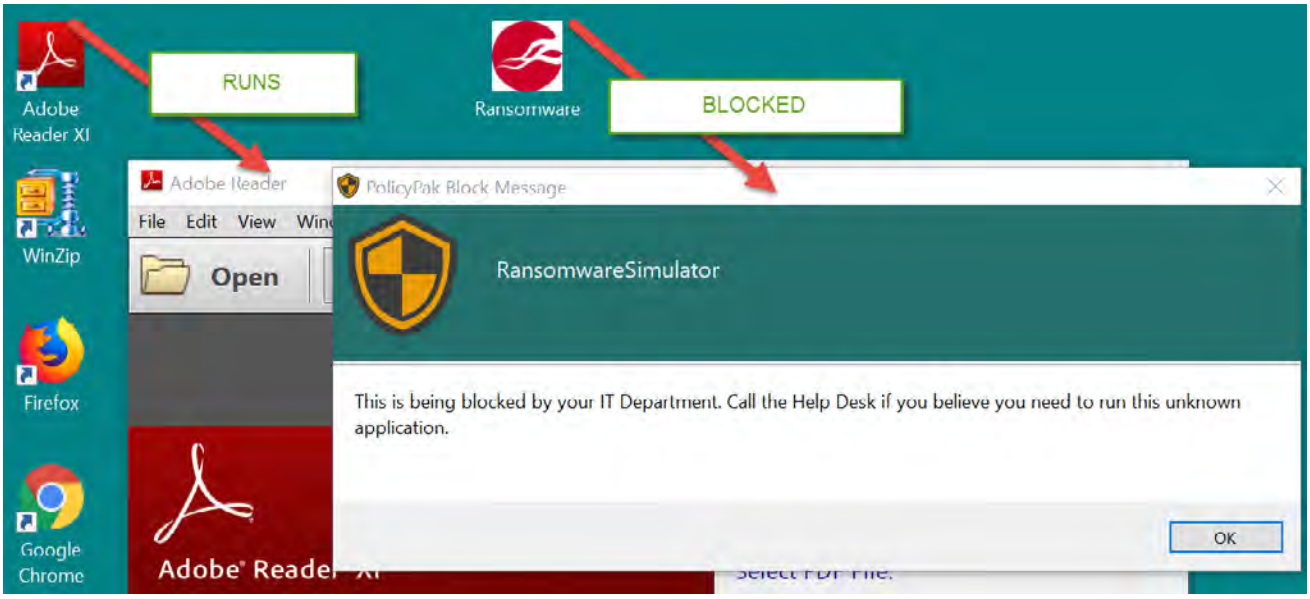


Figure 5: PolicyPak SecureRun™ allows all sanctioned apps, and blocks anything unknown

"We tried using Whitelisting products in the past; but the time and effort to get it to work was truly draining. I love the ability in "one click" to authorize everything that I installed (and permit to run), but block running everything else that users might try to run on their own.

"We were able to get PolicyPak Least Privilege Manager with its SecureRun™ working in under a day. We started testing the Friday it was released, pushed it out the next Monday.

"Couldn't be happier with my PolicyPak investment. Thanks!"

- David Hoffman
Network Administrator Northwest Area Foundation

Northwest Area Foundation
Reducing Poverty. Building Prosperity.

Security Superpower #2: Automatically block USB & CD-ROMs for inbound ransomware and outbound data exfiltration

Half of people plug in USB drives they find in the parking lot. And 68% took no precautions when doing do. This is according to a study by Google researchers where the details can be found here.

Don't be the victim of Ransomware or another kind of attack by this vector.

PolicyPak Device Manager will universally block USB sticks and DVD/CD-ROMs, then give you the controls you need to allow just who needs access to just the devices they need. So when you supply USB sticks which are always encrypted, you know those are exactly the ones they'll use, and no unusual or foreign ones.

Likewise, stop any undesired data exfiltration. Sanction just the right people with the right level of access for specific USB sticks. Enable a highly secure team to read your sanctioned USB sticks, but not write to them.

With PolicyPak Device Manager you can be in control of USB and DVD/CD-ROM access. In Figure 6 you can see how to create a Global Settings policy which will universally block; plus make rules about who can use what devices.

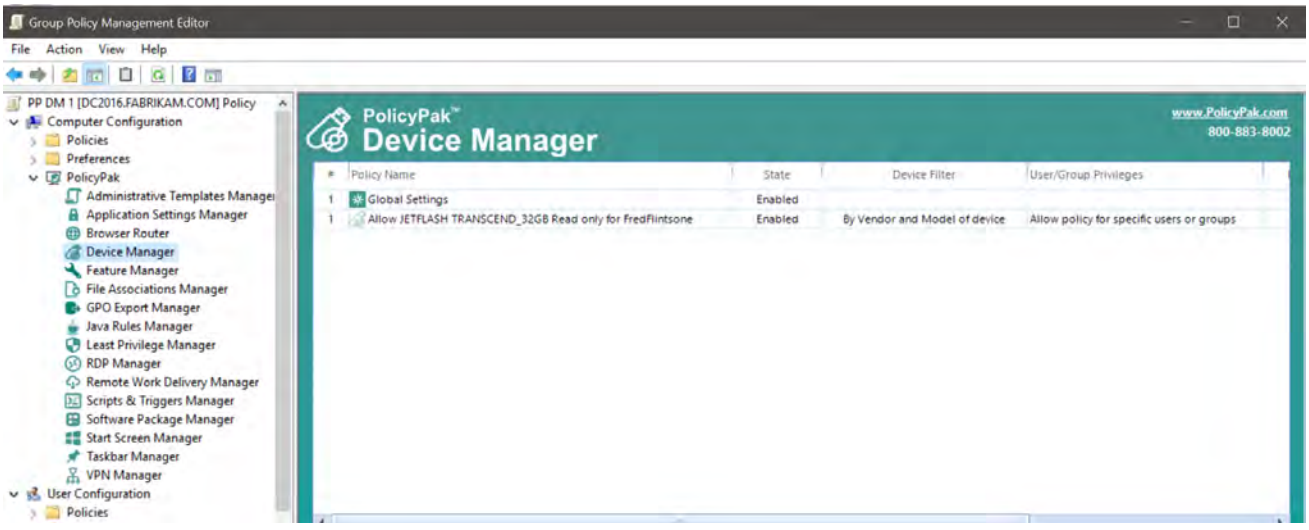


Figure 6: PolicyPak Device Manager will block USB and DVD/CD-ROMs but allow specific users' access as needed

The result of managing the device can be seen by the end user with a customizable message in Figure 7. Unsanctioned devices are blocked; allowed devices get specific Read, Write or Execute access.

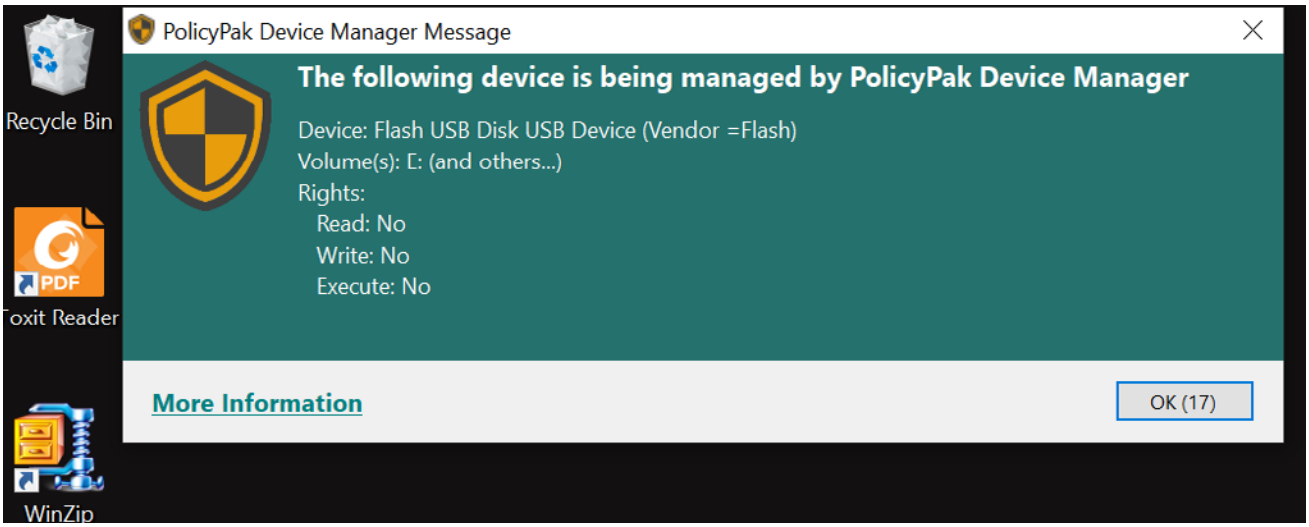


Figure 7: PolicyPak Device Manager makes your endpoints more secure blocking unknown devices

Security Superpower #3: Take Control of Java Websites

Unfortunately, you can't make Java magically go away. You can try, but in the meantime you will still have a few big problems:

- How do you guarantee Java websites use the best version of Java for that application?
- How do you have the latest Java on your machines for security?
- How can you block unknown and unsanctioned Java websites?

With PolicyPak Java Rules Manager, you can do all of these. PolicyPak Java Rules Manger enables you to map particular key websites to use particular versions of Java. Without PolicyPak Java Rules Manager, all Java websites will simply use the latest version of Java on the machine. This can cause websites with Java applets to fail. With PolicyPak Java Rules Manager, you can have the latest version of Java on the machine for security, while having older versions of Java available for compatibility, as shown in Figure 8.

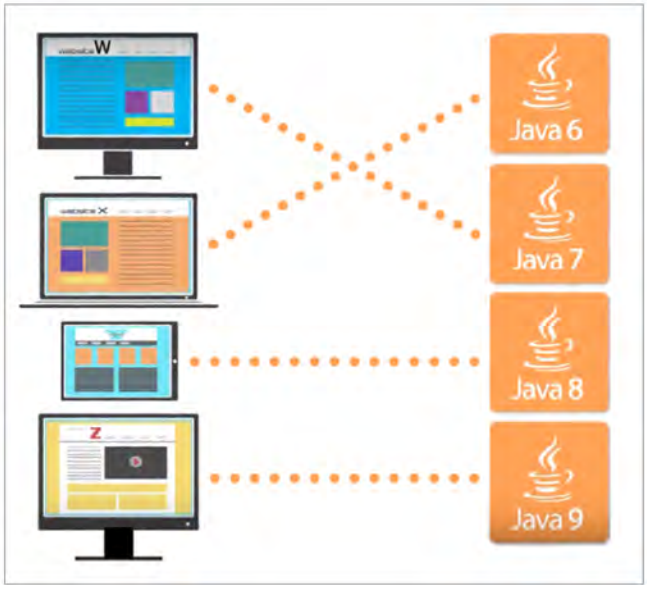


Figure 8: PolicyPak Java Rules Manager easily maps websites to particular Java versions.

In the example in Figure 9, there are three rules:

- Block any Java applet which isn't expressly allowed
- Map Java.com to Java 7 U 51
- Map Javatester.org to Java 8 U 25

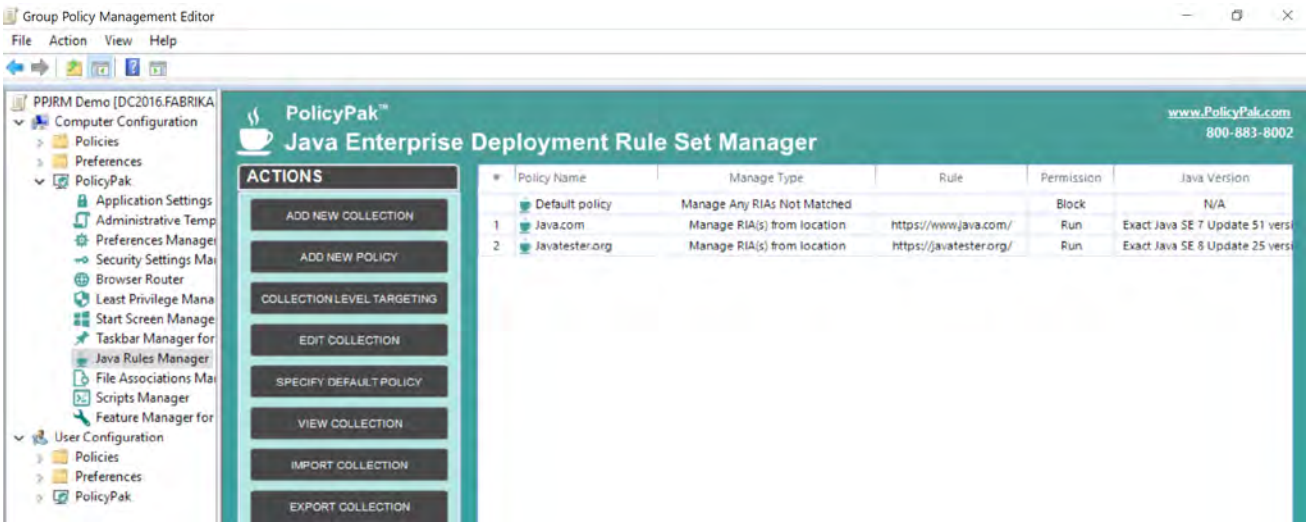


Figure 9: Using PolicyPak Java Rules Manager to block unknown Java applets and map specific versions of Java to specific websites

The result couldn't be simpler. As seen in Figure 10, when Java runs, it is then directed to use the correct version of Java. And if the website is unsanctioned, the Java applet is blocked.

In this way, you increase your security and also your compatibility.

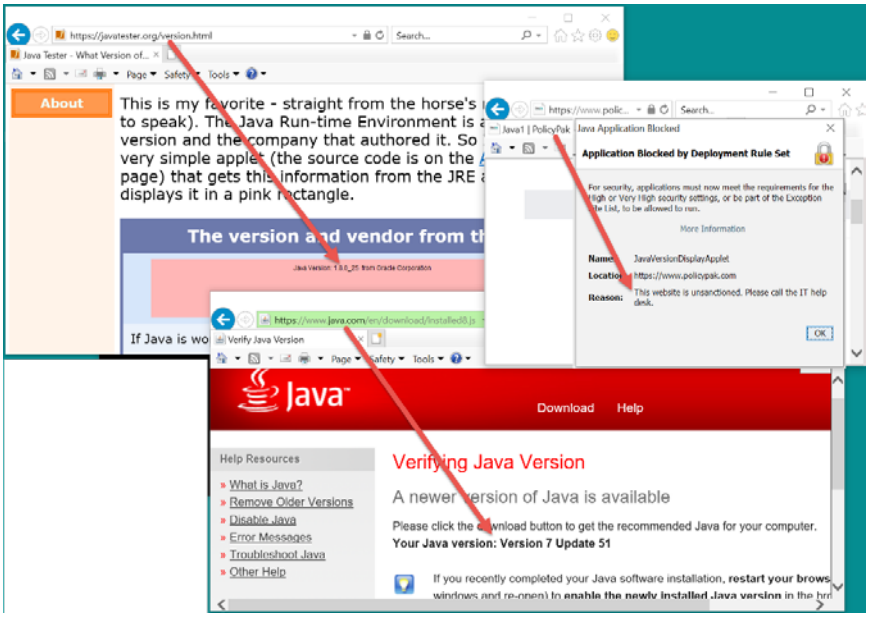


Figure 10: PolicyPak Java Rules Manager result: Mapping certain websites and blocking others.

RTC GROUP

PolicyPak
SECURING YOUR STANDARDS.

"We had a situation in which there was a new Java release that wasn't working with our application so we needed an updated Pak. I emailed support at 5:00 p.m. in the UK, and when I came in at 8:00 a.m. the next morning, the work was done. With each issue I've had, the response from PolicyPak has always been fast, and professionally handled."

- Justin Taylor,
Group Information Technology Manager, RTC Group Plc

Security Superpower #4: Manage and Secure Your Browsers

Microsoft's worldwide application compatibility lead, Chris Jackson, wrote a seminal blog post entitled "The perils of using Internet Explorer as your default browser." The basic gist is simple: Use IE only when you must because other browsers are more modern and are tested to meet modern standards.

Even though Microsoft is sunsetting Internet Explorer the application, you will still need to manage the "IE Mode within Edge" plus Edge, in addition to Chrome and/or Firefox still required for some websites.

You know that some websites only work perfectly with the right browser. You wouldn't want to utilize your Google services with Firefox or Internet Explorer. And you know your timecard or in-house application only works with Internet Explorer (or IE Mode within Edge.)

Additionally, you may want to block students or employees from browsing nonessential websites, like Facebook.

With PolicyPak Browser Router, you can quickly and easily make routes to specific browsers for specific websites. In Figure 11, you can see the main idea behind PolicyPak Browser Router.

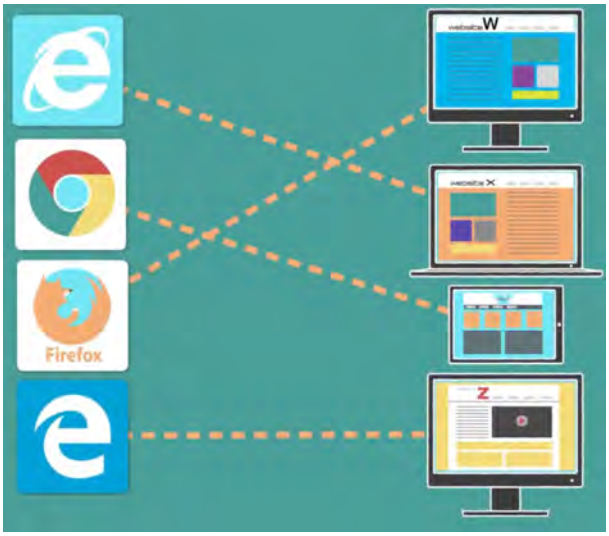


Figure 11: How PolicyPak Browser Router enables the most secure browser per website.

Creating these rules to open specific websites in specific browsers couldn't be simpler. It's equally easy to block specific websites (like Facebook, etc.) from all browsers. In Figure 12, you can see PolicyPak Browser Router with routes to use Chrome for "anything Google" and Edge for "anything Microsoft" and to block access to the Facebook site.

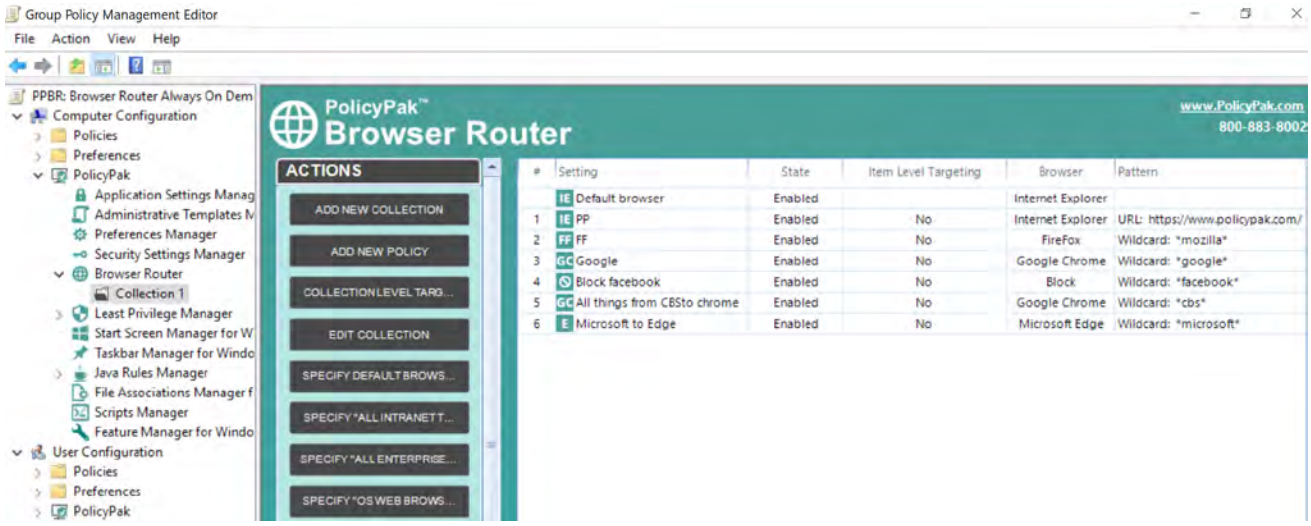


Figure 12: PolicyPak Browser Router routes and blocks websites as needed.

The result is that when users click on links from programs like Outlook, Teams, Acrobat, or from any browser, the right browser opens in the right website. In other cases, the website is blocked, depending on the settings you have created. You can see an example of this in action in Figure 13.

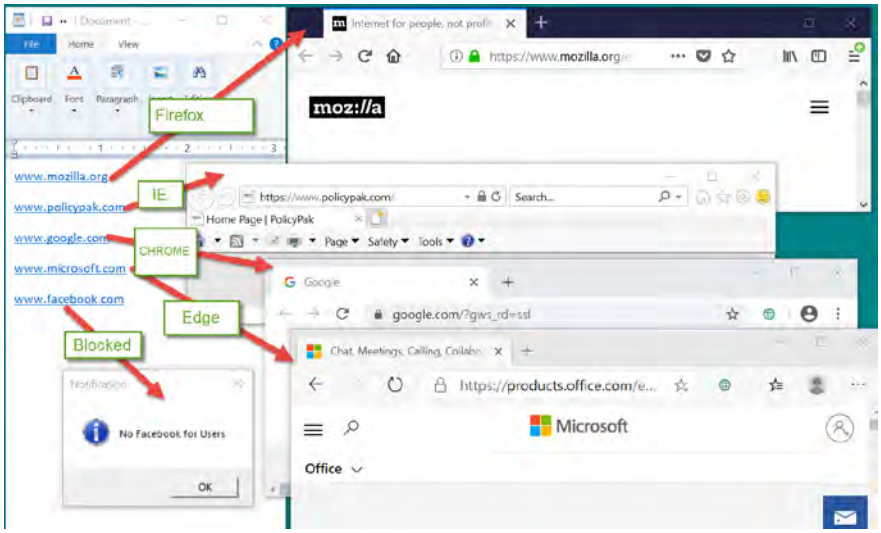


Figure 13: PolicyPak Browser Router opens the right website at the right time; or blocks it.

> *"By using PolicyPak Browser Router behind the scenes, we are able to ensure that when users open their banking website, it always opens in the CORRECT browser; not the browser they just happened to be using. This spares users from a lot of frustration, and has greatly reduced help desk calls."*

- Ernest Murray,
CTO and Co-Founder, Genuine Technology Group.

PolicyPak Browser Router can dictate a user's default browser (so, no more annoying pop-ups and/or calls to the help desk). Additionally, when sites are routed to Internet Explorer, the IE Document and Enterprise Mode can be set on the fly. You can then route sites to Internet Explorer (the full application) or IE in Edge mode.

In short, you already have multiple browsers: Edge and IE. And if you even more browsers, you can secure and manage all of them with PolicyPak Browser Router.

Security Superpower #5: Manage and Secure Your Applications and Middleware

You know you need to improve security for applications and browsers. A key instance would be the need to remove insecure protocols from your applications and network.

But your applications are already on the desktops and rolled out to end-users. How can you globally remove insecure protocols from applications plus also tighten up inherent security holes in your applications and browsers?

You can start by looking at the guidance from the Defense Information Systems Agency (DISA) in their Security Technical Implementation Guides, or STIGS as seen in Figure 14.

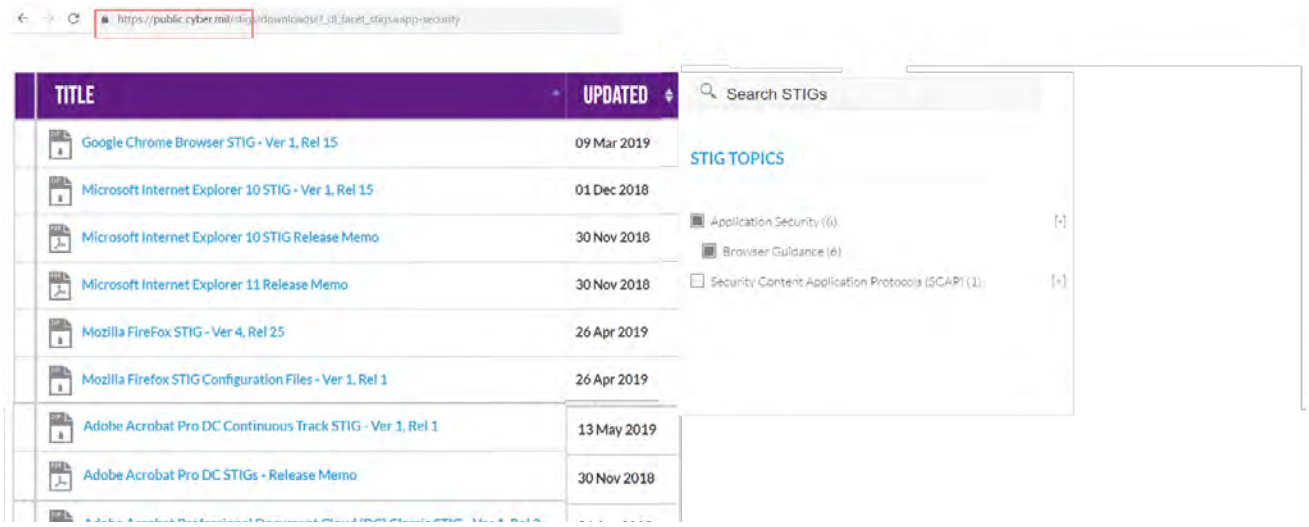


Figure 14: Guidance from Security Technical Implementation Guides.

But how do you quickly implement them and report on their efficacy? You could implement their settings by pre-populating the settings into your image or performing the work with scripts. Or, you could use PolicyPak Application Manager to take this advice and deploy it directly to your machines, even when the advice changes from time to time.

In Figure 15, we're using PolicyPak Application Manager to remove and block insecure protocols, while forcefully requiring the most secure protocol.

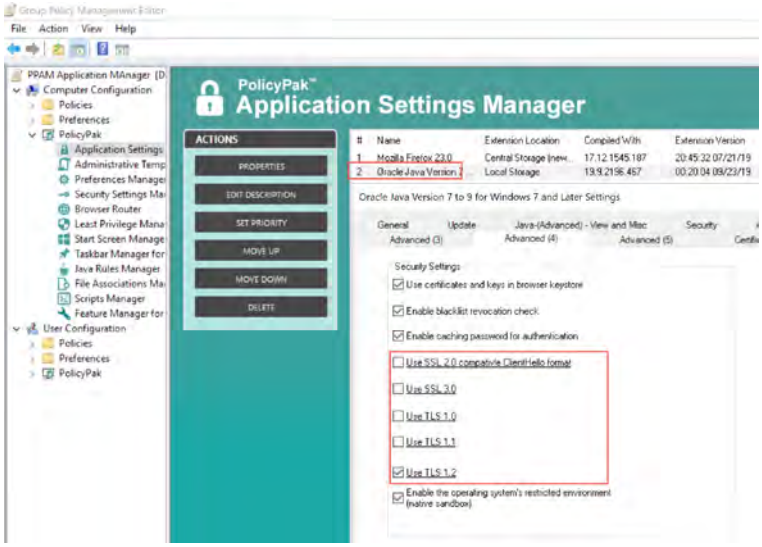


Figure 15: Use PolicyPak Application Manager to set nearly any application or browser security setting.

The result is that your browser, middleware, and any other application is instantly more secure, as seen in Figure 16.

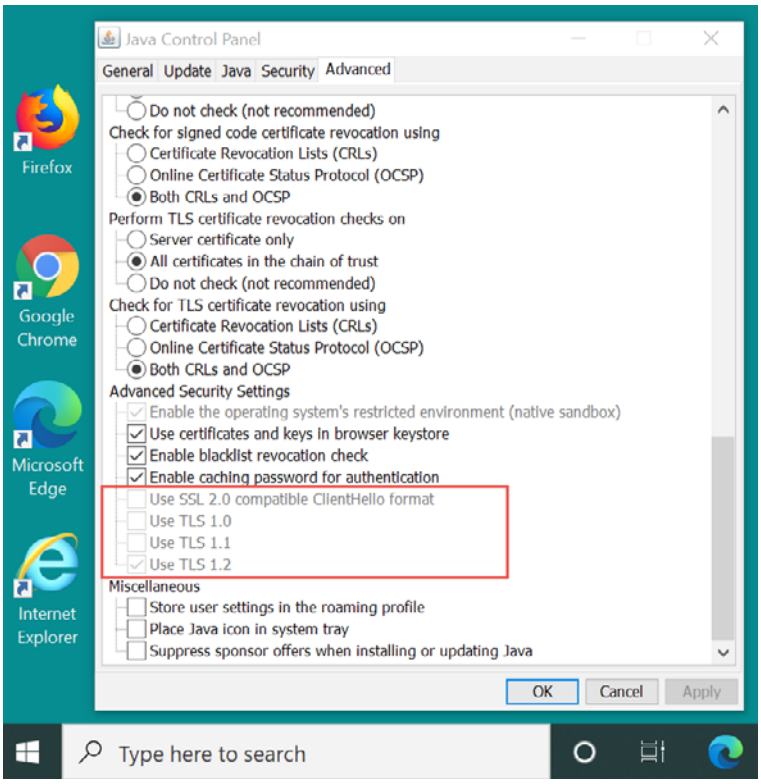


Figure 16: Securing Java security settings with PolicyPak.

> *"We originally started using PolicyPak as it was the only solution that we found that would allow us to manage Firefox within the enterprise. Even with Firefox's own policy settings, PolicyPak still beats that, hands down, with thousands of Firefox settings to configure. Beyond Firefox, we are now using PolicyPak to manage Java, Adobe products, and so much more! Best of all, with our existing Group Policy experience, we already know how to use it. PolicyPak is quickly becoming our primary means of implementing new settings with Group Policy here at TIAA."*

- Michael Patrick,
Senior Engineer - IT, Unified Client Infrastructure Engineering

TIAA

PolicyPak: Top Windows Management Superpowers

Beyond what PolicyPak brings to increase security, it also enables superpowers where Group Policy, MDM, and other products simply cannot go. In-box Management from Group Policy and Microsoft Endpoint Manager can only go so far. With PolicyPak, you're able to both secure, and standardize, your environment.

Expert Opinion: Take a second and think of something you wish you could do in Group Policy but currently can't. Whatever you thought of, I would be willing to bet that PolicyPak can handle it!

- Joseph Moody
Microsoft MVP

Users want to be productive on-prem and when doing remote work. With PolicyPak, you're turbocharging the systems you already use, not replacing them. PolicyPak's Policies work for your team wherever they are, so you know they can be both secure and productive.

Windows Management Superpower #1: Deploy any Group Policy Setting (or PolicyPak Setting) Over the Internet (via PolicyPak Cloud or via Your MDM)

Group Policy is Microsoft's best toolkit for keeping your machines managed and secure. The problem is that there's no way to get real on-prem Group Policy settings to your remote and non-domain joined machines. But with PolicyPak, you can.

Those who are used to the extensive settings and feature coverage of Group Policy need to bridge the gap in some way. As many MDM admins will tell you, a blocker to using their MDM service is the need for parity between their on-prem Group Policy settings and their MDM service.

If you use PolicyPak Cloud or PolicyPak MDM, you can export existing Group Policy settings (ADMX, Group Policy Preferences, and Group Policy Security settings) and get those deployed to your remote machines. Additionally, all PolicyPak settings (like those discussed earlier and those discussed later in this paper) can also be exported this same way.

In Figure 17, you can see how to export existing Group Policy settings for use with PolicyPak Cloud and PolicyPak MDM.

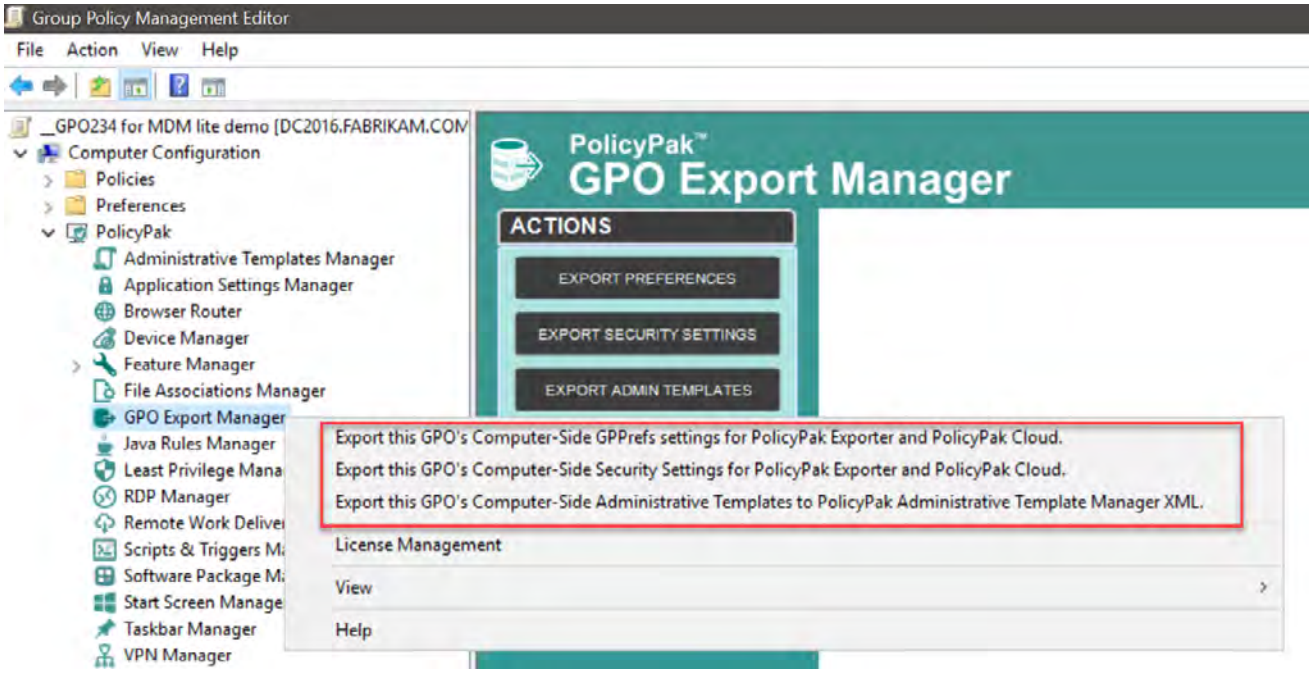


Figure 17: Exporting Group Policy settings for use with PolicyPak Cloud or PolicyPak MDM.

Then, use PolicyPak Cloud (Figure 18), or PolicyPak MDM (Figure 19) to get those settings deployed.

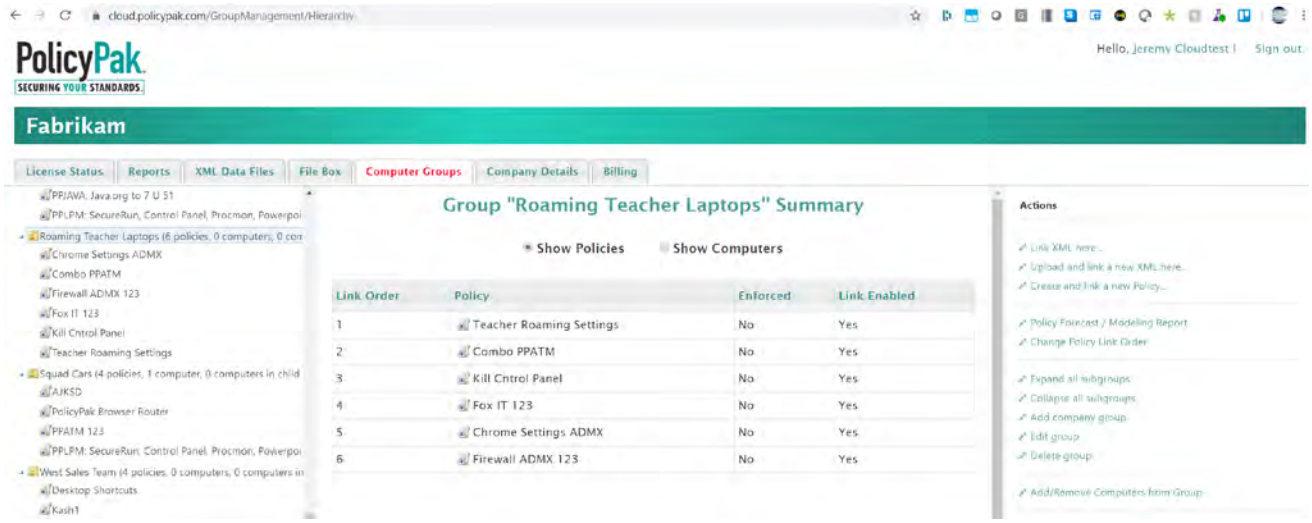


Figure 18: Using PolicyPak Cloud to deploy PolicyPak and Group Policy settings.

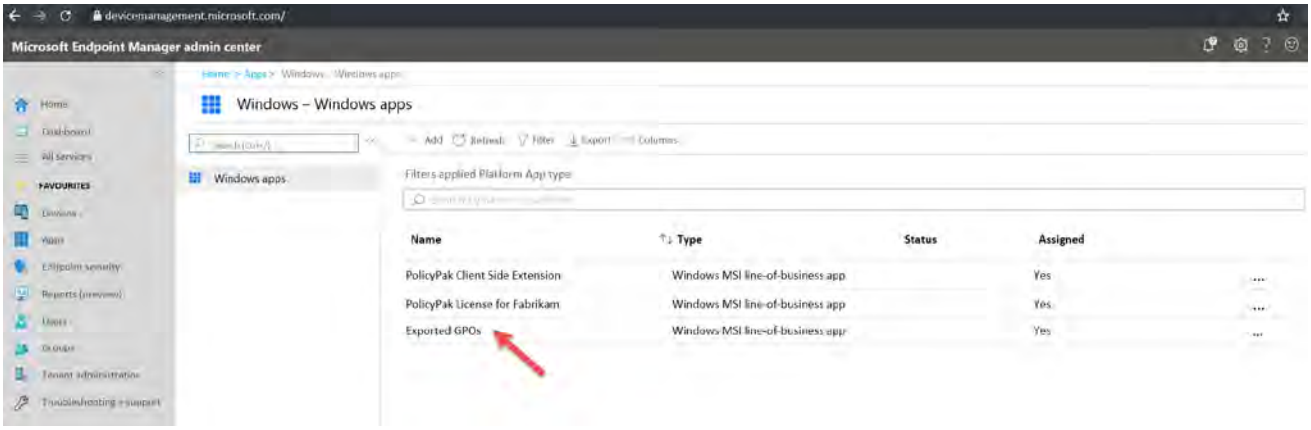


Figure 19: Deploying PolicyPak and real Microsoft Group Policy settings with your MDM service like Microsoft Endpoint Manager.

Windows Management Superpower #2: Configure File Associations, Start Screen, and Taskbar Exactly How They Should Be

Using Windows shouldn't be like navigating a mine field. It should be easy for your end-users to do their jobs. But there are three areas of constant challenge for the IT admin to configure for the end-user:

- Windows File associations
- Windows Start Screen
- Windows Taskbar

Let's start by saying that there is an "in the box" way to manage the Windows file associations, Start Screen, and Taskbar. The process of managing these settings via Microsoft's method is arduous, time-consuming, and inflexible. Here's what's involved:

- Create a golden machine with all of the necessary applications preinstalled.
- Configure required file associations, Start Screen, and Taskbar settings by making the associations. Put the icons into your allotted Start Screen and Taskbar configurations.
- Use PowerShell to export the file associations and Start Screen (and Taskbar) layout XML files.
- Use Group Policy to ensure that designated computers utilize the XML file.

When you need to update an application or add a new application (deploying via Microsoft Endpoint Manager or any other method), your IT team then needs to:

- Rebuild the golden computer.
- Reperform the file associations.
- Replace the Start Screen and Taskbar icons into groups.
- Rerun the PowerShell commands to reexport XML files.
- Redeliver those settings via Group Policy and deploy to all computers again.

Moreover, this system only really works when every computer gets the exact same configuration. If you have any variation, you need to perform the process THAT many more times for each variation. You need a solution that is flexible, dynamic, and adaptable to your ever-changing environment. There's a better way to manage file associations, Start Screen, and Taskbar with PolicyPak.

Managing Windows File Associations

Establishing the right file associations doesn't have to be insanely difficult. When you use PolicyPak File Associations Manager you can set file associations simply and easily to ensure your users open the right applications with the right extensions, as you can see in Figure 20.

Figure 20: The right File Associations you desire.

Then, PolicyPak File Associations Manager will automatically detect what software is installed for each user and set the right file associations. It couldn't be easier. PolicyPak File Associations Manager works with desktops, laptops, Citrix & RDS, Windows Virtual Desktop, and anything else.

Each user gets exactly the right file associations at the right time based upon their needs. Specify your apps, like what's seen in Figure 21, and PolicyPak File Associations Manager does the rest.

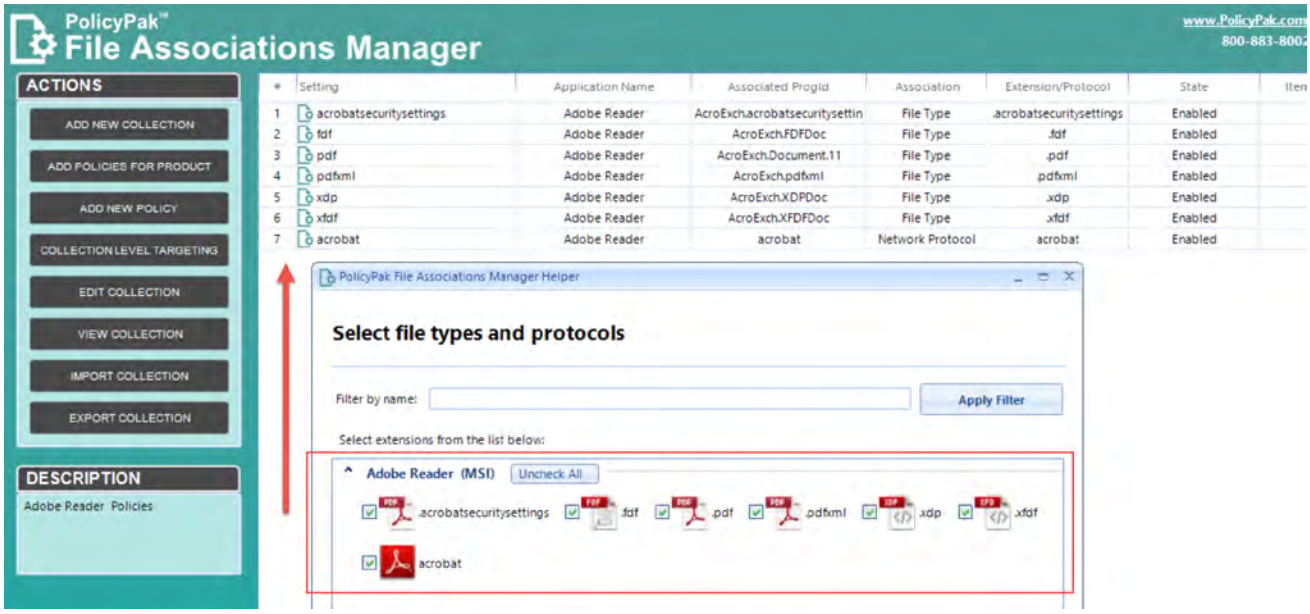


Figure 21: Selecting file associations with PolicyPak.

Managing Windows 10 Start Screen and Taskbar

Users want to be as productive as they can, as fast as they can. When you deploy software, it appears on the left side of the Windows 10 Start Screen, but there's no way to broadcast your software deployment to them on the right side of the screen. Moreover, the users' default start screen is a mess, as seen in Figure 22.

But your applications (and/or users' desires) should be quickly organized for a fast startup. The last thing you need from a user on-prem or remotely working is a helpdesk call just because they cannot find the application they know they need to use. Figure 23 shows how PolicyPak Start Screen & Taskbar Manager can nicely organize both the Start Screen and the Taskbar.

> *"We use PolicyPak Start Screen & Taskbar Manager to quickly control our Windows 10 Start Screen. We used to bake our Start Menu into the configuration, but as programs updated over time, icons would disappear and users started calling us. After an hour of installing and working with PolicyPak, we rolled out a nice and organized Start Menu look to all our users for our Windows 10 project."*
>
> - David Ganger
> IT Manager Mid-City Supply Co., Inc.

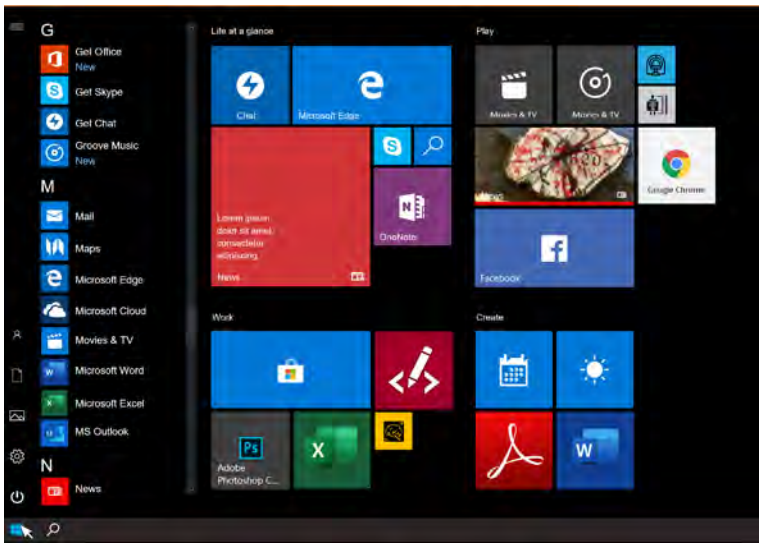


Figure 22: A user's Start Screen & Taskbar without PolicyPak Start Screen & Taskbar Manager.

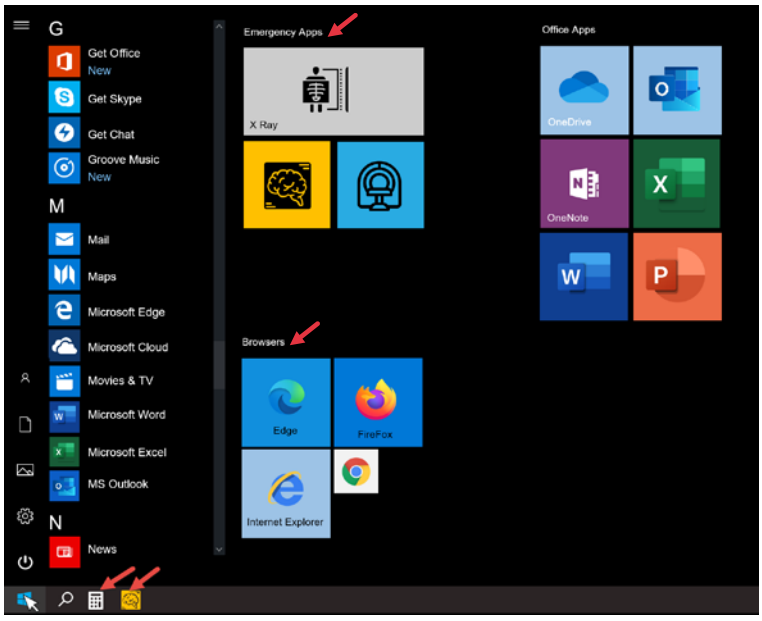


Figure 23: A user's Start Screen & Taskbar after PolicyPak Start Screen & Taskbar Manager has been used.

PolicyPak has impressive capabilities that fill very real gaps and make any Windows desktop admin's life a lot easier.

- HELGE KLEIN
Citrix CTP, VMware vExpert, Microsoft MVP Creator of Uberagent & Delprof2

Win 10 Management Superpower #3: Deploy (and remove) Software
(Great for Remote Work Users)

Working from anywhere means you need to deliver software and keep it updated.

When duty calls, use PolicyPak Remote Work Delivery Manager and PolicyPak Software Package Manager to do just that.

In Figure 22, we can see we're delivering a new application which is staged on Amazon S3 (or other web-based storage) to our remote team.

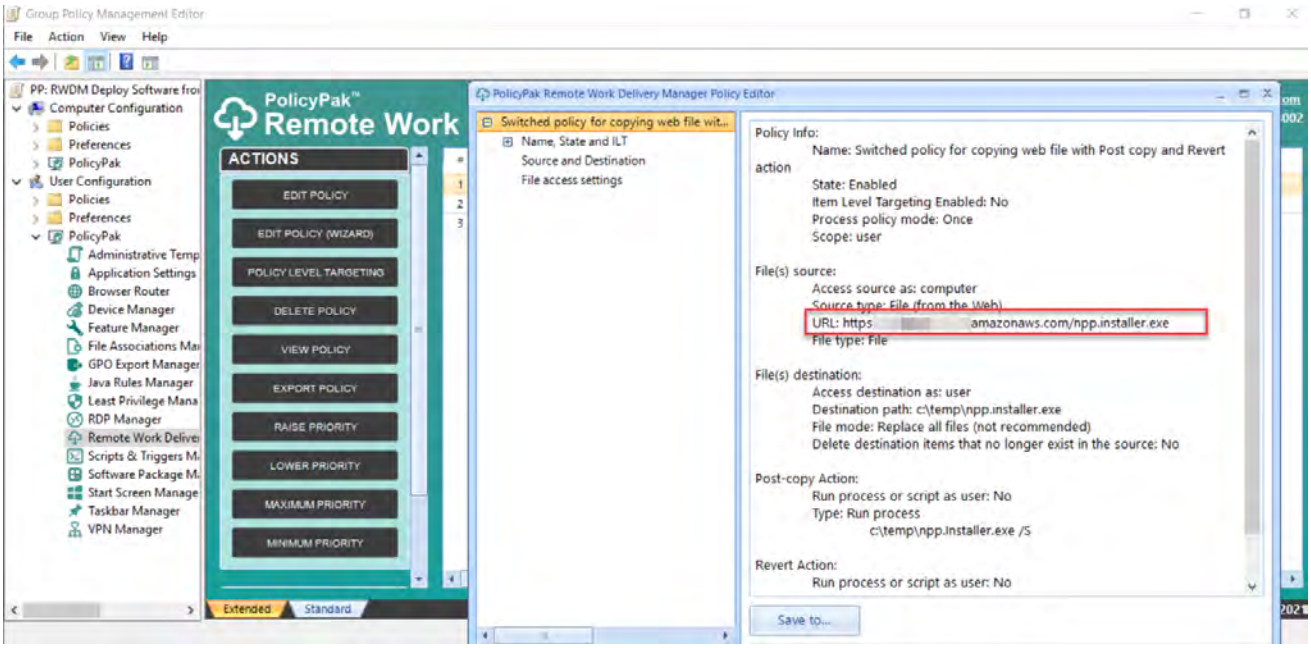


Figure 24: Installing software to remote users from Amazon S3 or Azure storage.

You can also use PolicyPak Software Package Manager to install required business applications from the Windows Store, and yet remove any unwanted applications like Candy Crush. Both policies are shown in Figure 25.

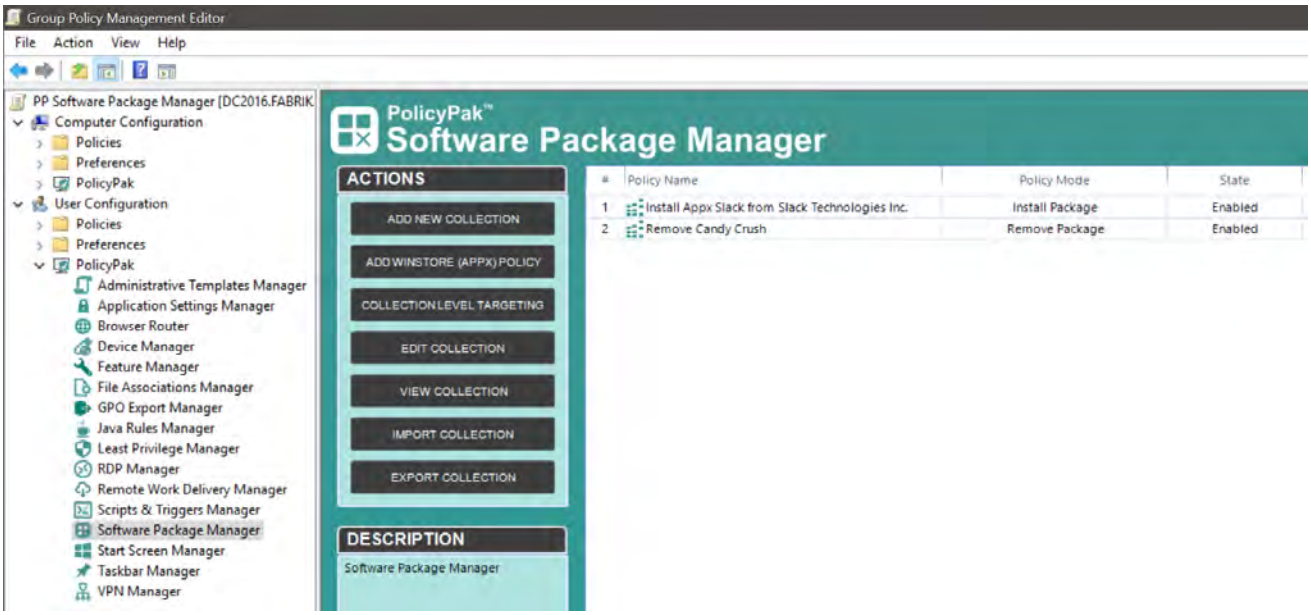


Figure 25: Using PolicyPak Software Package Manager to install and remove Windows Store applications.

In this way, you can fine tune exactly what end users should and shouldn't use: on-prem or out in the field.

PolicyPak is probably the best kept secret of the decade. It's simply a 'must have' for any RDSH admin.

- ERIC HAAVERSTEIN

Citrix CTP, Microsoft MVP, VMware EUC Champion XenApp Blog

Windows Management Superpower #4: Consolidate GPOs and Target Settings, Get Faster Logins

Less GPOs at login means a faster login time. PolicyPak enables you to consolidate GPOs and to target the settings within them to specific users and computers. In the example in Figure 26, there are 16 GPOs across four divisions, with four cases for each division.

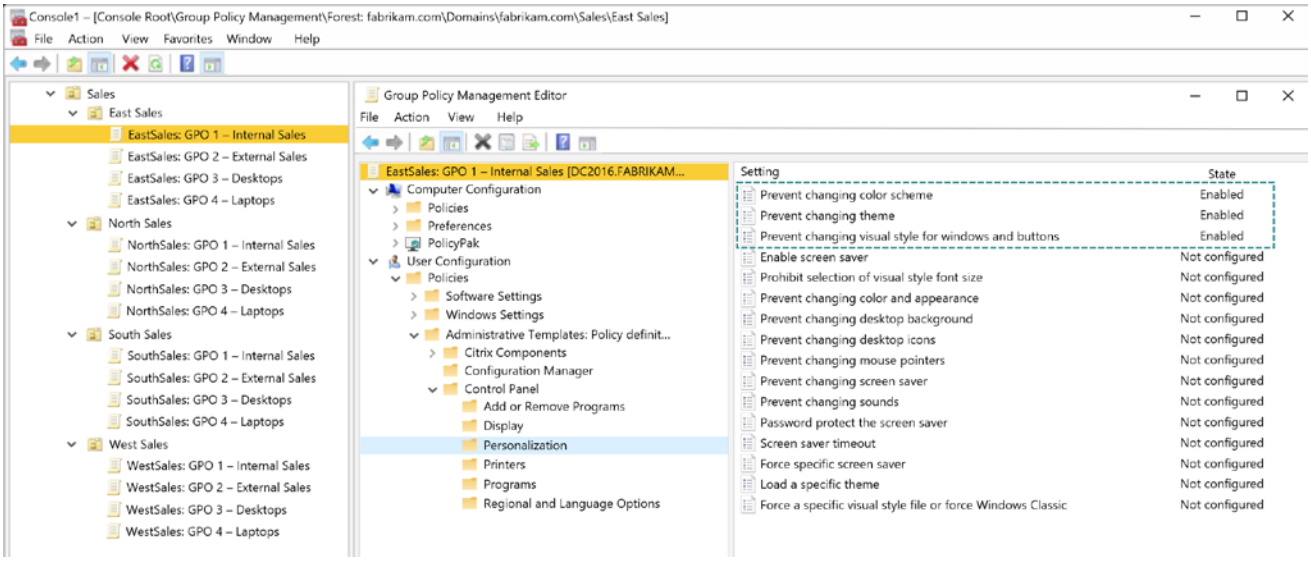


Figure 26: Without PolicyPak, you have too many GPOs linked to users or computers which can lead to long login times.

With PolicyPak, you can use our Group Policy Merge tool which lets you read existing GPOs and consolidate them. You can see an example of this in Figure 27.

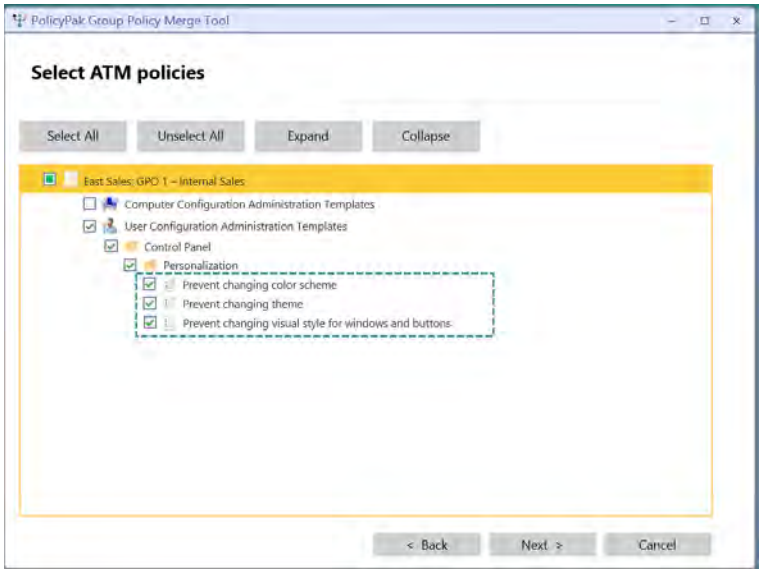


Figure 27: Using the PolicyPak Group Policy Merge Tool.

The result in Figure 28 is one GPO to replace all sixteen, with each GPO nestled into a Collection which will only apply to the right people at the right time.

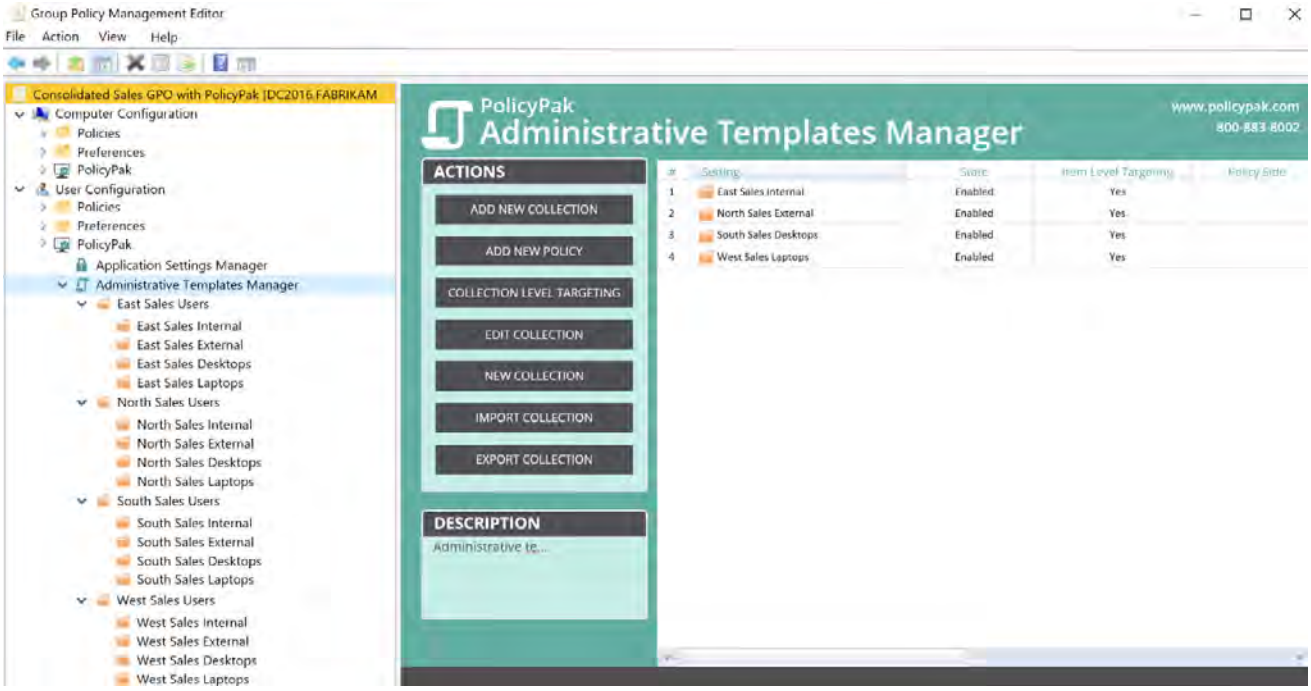


Figure 28: Consolidated GPOs after merging with PolicyPak Merge Tool.

Windows Management Superpower #5: Works With What You Already Have (and Will Have in the Future), Experts Love It, and Customers Love It

PolicyPak's biggest superpower is that it works with whatever you have today. PolicyPak will work with practically anything:

- Desktops & laptops
- VDI
- Windows Virtual Desktops
- Microsoft FSLogix
- VPN
- Group Policy & Microsoft AGPM
- Citrix
- VMware Horizon
- VMware Workspace ONE
- Microsoft Endpoint Manager (SCCM and Intune)
- On-Prem Active Directory or Azure Active Directory
- Application virtualization and layering

Final Thoughts

You wanted to know what PolicyPak's superpowers are and why PolicyPak needs to exist. The answer is simple: Windows 10 needs more management than Group Policy, Microsoft Endpoint Manager, or other tools can provide.