PolicyPak Technology Briefs

Application Configuration Management (ACM) Report 2014-15

Jeremy Moskowitz,
Group Policy MVP
www.policypak.com
Phone: 800-883-8002

Executive Summary

>75% of organizations surveyed are trying to create desktop and security standards.

>80% of organizations say they've had users try to work around IT's security standards and settings.

>80% of organizations reported unwanted calls to the support desk, asking for help to resolve users' own self-inflicted issues.

>66% of organizations say that it takes them more than 30 minutes to address and fix an undesired, user-made change.

Contents

Introduction

IT goals: Stable, secure & cost-effective

In any IT organization, the most important goals are:

- Keep systems **stable**,
- Keep systems **secure**, and to
- Keep the **costs** of implementation, maintenance, support and migration costs as **low as possible**.

To accomplish these goals, most IT organizations endeavor to establish standard sets of system configurations. If a system is in a known state, this optimizes the system productivity, minimizes troubleshooting efforts, and meets security requirements.

IT really has two "realms" of systems:

- Servers and such where users don't get to generally touch:

Only IT has access to manipulate the configuration and security of the systems they manage. These systems largely stay secure once set because no one except administrators are manipulating them.

- Client systems (physical desktops & laptops, or virtual VDI and RDS sessions):

With end-user systems, IT has to contend with the fact that the user has anywhere from limited to complete access to change the configurations and security settings established by IT. The secure, consistent, and productive working environment they require can be "worked around" quickly by regular end-users.

How Application Configuration Fits Into The Picture

Applications are not only the medium by which users accomplish their work; applications can also serve as a conduit by which malicious code can enter, infect, and spread throughout a corporate network.

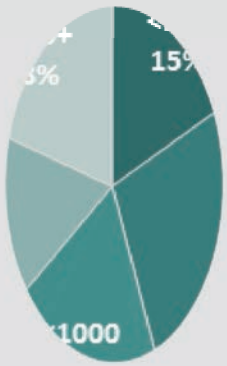
While IT takes steps to establish application configuration standards, users often, accidentally or maliciously, modifying IT's desired settings.

In the "best case", this increases IT's support costs when users call the help desk, or, at worst, it increases the potential for the introduction of malicious code, possible data breaches, loss in corporate reputation, and loss of revenue, personal information and corporate secrets.

Application Configuration Management (ACM) tools do exist to both establish and enforce productivity and security settings within applications, but they typically lack the depth and breadth required to actually have a positive impact on the environment.

About the Survey

Company size distribution: how company size breaks out within the survey.



PolicyPak Software, inc. surveyed 710 IT professionals about the current state of ACM, asking about the environments they support, the tools they use to manage application configurations, the effectiveness of those tools, and the resulting impact on IT.

Company Size

This survey saw responses from organizations of every size, ranging from the small business with less than 100 users, to enterprises with more than 5000.

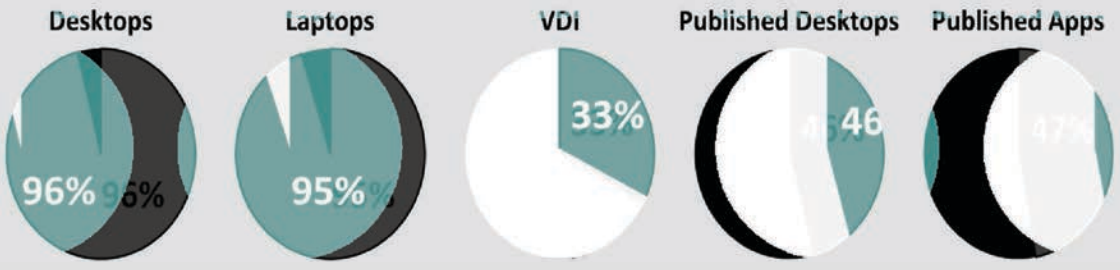
No matter the size of the organization, we found that every organization had some level of application configuration management issues, and were trying to address them. The chart alongside shows the breakdown of respondent organization sizes.

Clients Managed

The chart below shows the percentage of organization supporting each type of client today.

Unsurprisingly, smaller organizations showed measurably lower use of VDI or published environments to facilitate access to corporate applications or data.

Who supports what: the different type of client machines supported.



PolicyPak
WHAT YOU SET IS WHAT THEY GET.

The Ever Changing State of the User Environment

Making Applications Changes - Everyone's Doing It

Users making changes:

over **80%** of organizations need to deal with application issues stemming from unwanted user-led changes.

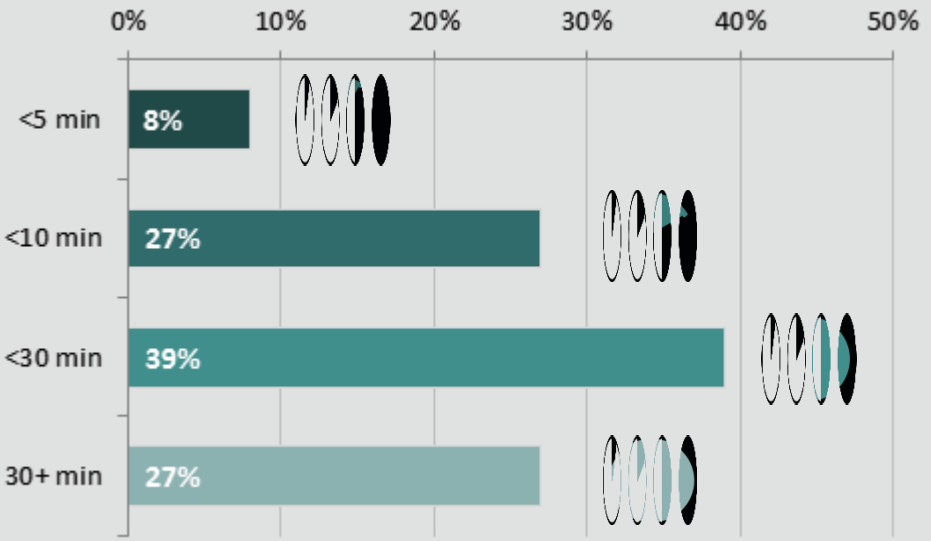
Organizations want users to accomplish their work efficiently and effectively. However, the lack of security settings, or an inability to enforce application configurations can leave users able to either intentionally or inadvertently modify their own settings.

Our survey reported that user application misconfigurations resulted in **83% of organizations** getting unwanted calls to the support desk, asking for help to resolve their self-inflicted issues.

Enterprise-sized organizations showed the highest response of user-generated issues at **88%**, with small businesses being slightly less prone to user-generated issues at **78%**.

Even Simple Changes Are Costly

User app issues take time: over half of organizations report taking over 30 minutes on average to fix user application configuration issues.



On average:

18 min /event

$9 /event

The vast majority of organizations (**63%**) take over 10 minutes to address simple user environment changes, as shown in the chart above, with the average amount of support time needed of more than **18 minutes**.

PolicyPak
WHAT YOU SET IS WHAT THEY GET.

Given that the average salary of the Help Desk / Users Support role in IT is $57,127 annually[1], it costs IT organizations **an average of nearly $9** to address user change issues, with 27% of organizations spending **more than $14 per issue**.

Not included in the survey is the amount of productive time lost (also known as "down time") as the end-user waits for IT to actually come around to troubleshoot and fix the issue. Again, in some cases, the resolution time (once begun) can stretch to *longer* than 30 minutes, making each user-caused issue even more costly to the company overall.

Users Put Company Security at Risk

Security at risk:

over **75%** of organizations reported issues with users circumventing security.

A user can't distinguish between a setting that impacts only the configuration of the application and one that will impact the very security of their environment. For example, a simple misconfiguration in browser security settings intended to allow a favorite website to run properly can instead permit untrusted websites to wreak havoc.

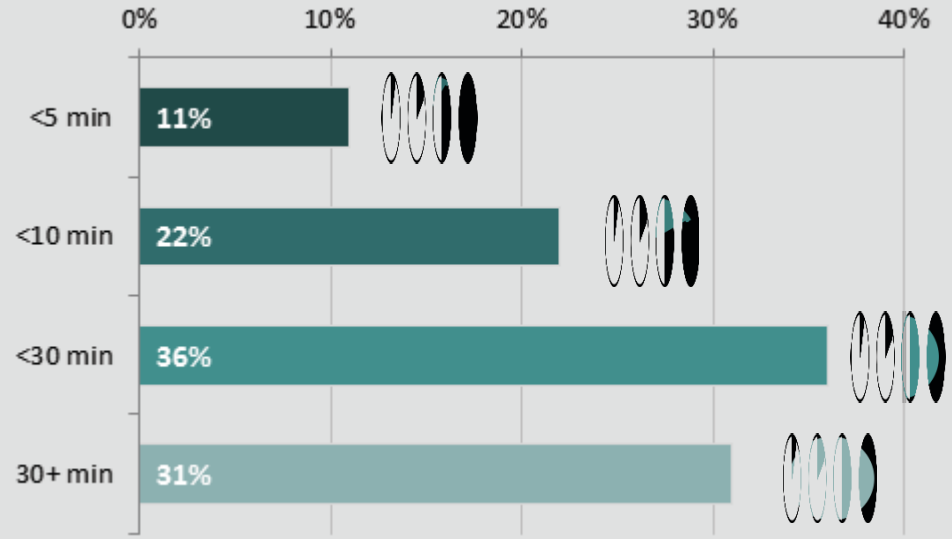
Our survey reported **78% of organizations** expressing that they had experienced end-users making application changes **specifically meant to circumvent security settings intended by IT**.

Larger organizations are most susceptible with over **88%** of those organizations with 5000 and more users experiencing the problem: the larger the organization, the bigger the problem.

[1] Redmond Magazine 2013 Salary Survey

Security Changes are Equally Costly

User app issues take time: over half of organizations report taking over 30 minutes on average to fix user application configuration issues.



The survey study found that *resolving* security settings issues take longer than application configuration settings issues.

A full **two-thirds** of organizations take more than 10 minutes to address security issues, as shown the chart above.

Support *costs* per issue were found to be similar to that of fixing non-security changes made by users. Considering 8 out of the top 10 threat actions causing data breaches[2] are malware, users manipulating sanctioned security settings pose a real threat to organizations, with potential costs far greater than just the 30 minutes spent reapplying a security setting.

[2] Verizon 2014 Data Breach Investigations Report

Managing Application Configurations

While it's evident that users are making changes which could negatively impact security and productivity, IT is still taking strides to address the problem.

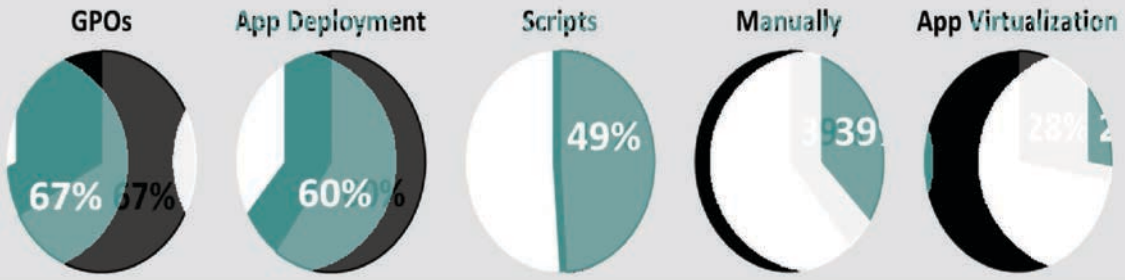
The best organizations are not idly sitting by: they are creating standard application and security configurations and working to establish and maintain standard user environments.

Deploying Applications: A Standard Practice

Every organization participating in the survey indicated that deploying applications is a priority. Group Policy and App Deployment solutions topped the list to initially get software "out there", as shown in the chart below

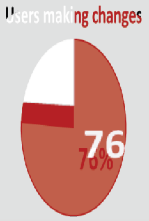
Deployment is an often-used point in time to establish configurations as part of the deployment.

Application deployment:
the most commonly used methods of deploying applications.



Keeping a Standard Configuration

Widespread standardization I:



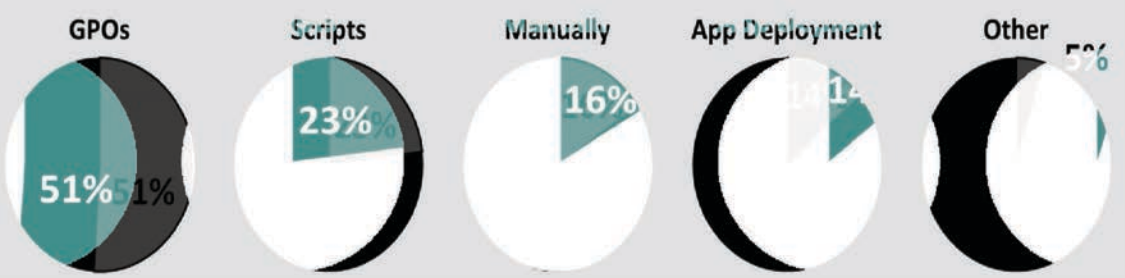
over **75%** of organizations reported establishing and maintaining standard *application* configurations.

Not every organization chooses to use deployment as the point in time, nor method, to deploy standard configurations. **More than three-quarters of organizations are concerned** with establishing and maintaining a standard configuration, as reported to our survey. But **only 14% utilize app deployment** as the medium by which to push out configuration settings, as shown in the chart below.

This isn't surprising, as application deployment solutions are focused on one thing – deployment. To *maintain* a standard configuration, solutions that *enforce* a configuration repeatedly, like Group Policy, are a better choice. So it came

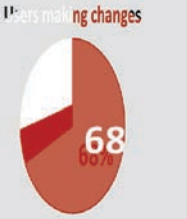
as no surprise that **over half of all organizations surveyed are using Group Policy** to maintain configuration settings, also shown in the chart below.

Keeping up to date: the most common methods for updating application *configuration* settings.



Locking Down Application Security

Widespread standardization II:

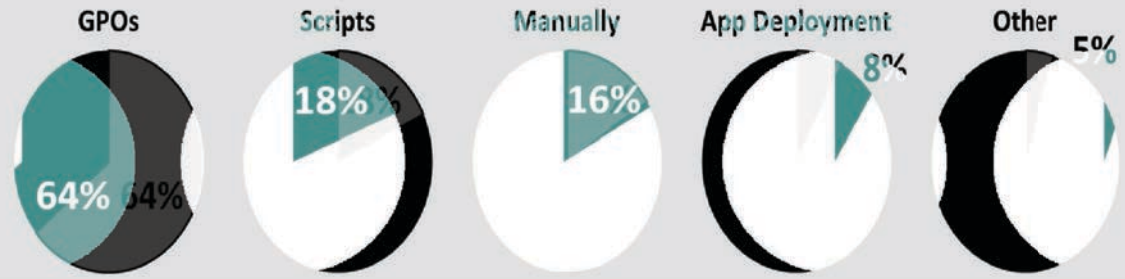


over **65%** of organizations reported establishing and maintaining standard *security* configurations.

With malware attacks on the rise, and web browsers and email being the highest targets, organizations are taking steps to address these concerns by maintaining standard security settings. Surprisingly, **only 68% of organizations are imposing security-related settings** (less than their standard application setting counterpart), according to our survey report.

Not surprising, organizations are utilizing the same solutions to implement security settings, as they are application settings. Group Policy topped the list at 64%, as shown in the chart below.

Keeping up to date: the most common methods for updating application *security* settings.



PolicyPak
WHAT YOU SET IS WHAT THEY GET.

Reportcard: Is IT Winning the ACM Battle?

It's obvious IT organizations are taking steps to attempt to address Application Configuration Management issues around both application and security settings. Both manual activity, as well as the use of automated solutions are used, signifying the importance to security and lowering the cost of support.

It's equally obvious that users are still able to make modifications that are having a tangible impact on support costs, and an intangible impact on the state of security within an organization.

The question, then, becomes *If IT is establishing ACM, then why are users able to still make changes?*

The answer is that IT *can't* restrict user changes within applications.

Here's a quick Q &A to help understand the ACM challenge for technical managers:

Q: Why isn't Group Policy enough by itself to establish and maintain ACM?

A: Because Group Policy can only manage what it can manage.

Group Policy does a great job for the settings "in the box", such as desktop look and feel and security settings. But when it comes to managing applications, the app itself must be "Group Policy aware" to be fully managed.

Only a handful of some Microsoft applications and those applications that store their configuration in the proper places in the registry are fully supported. Therefore, applications which don't store their configurations in a way Group Policy can fully manage (such as Firefox, Flash, Java, OpenOffice, Skype, Chrome and even pieces of Internet Explorer itself) and many registry based applications are vulnerable because there's no Group Policy-way to manage them and maintain settings. For a video to articulate the problem, see http://www.policypak.com/video/uk23jwvjm-c.html

Q: Why aren't Application Deployment tools (specifically MSI packaging tools) enough to establish and maintain ACM?

A: Because MSI packaging tools only deliver settings one time.

MSI packaging tools have a better ability to initially rollout deep settings within an application, but have no ability to *enforce* those settings once deployed.

Once the "one time" delivery has occurred, users are free to work around anything set in the box.

Q: Why doesn't VDI help with ACM?

A: Because VDI doesn't prevent users from making changes once they're in their own session.

Even if you give users a brand new desktop each and every time they log on, users can then configure settings however they want.

VDI solutions from vendors like Microsoft, Citrix and VMware all have ways to help when users make sanctioned changes to applications. They store when a user changes an application setting, so it's a seamless experience for the next VDI session.

But none of the solutions can restrict users from making changes, which is a demonstrated source a rise in support costs and a lowering of the organizations security posture.

Final Thoughts

The reality for IT organizations is that they *are* making an attempt.

But without a solution to implement, maintain, enforce, *and* restrict the changing of settings, IT is simply losing the battle.

For more information on to actually deliver, enforce, maintain, and remediate application settings, which will ensure end-user compliance and security, see the ACM solution at www.PolicyPak.com which works alongside your existing Microsoft, Citrix, and/or VMware investment.