Security vs. Flexibility: Must IT Management Choose?

Whitepaper

June 6, 2008

Intelligent Solutions for ABSOLUTE Control

www.faronics.com

Tel: 1-800-943-6422 ▪ **Fax:** 1-800-943-6488

Tel: +1-604-637-3333 ▪ **Fax:** +1-604-637-8188

Security vs. Flexibility: Must IT Management Choose?

Your organization already has a CCM tool. But is it enough?

By Jeremy Moskowitz. Moskowitz, Inc., Microsoft MVP

Executive Summary

IT Managers are tasked with making the desktop environment more secure and locked down to a uniform corporate standard, yet flexible enough to handle the myriad of exceptions that arise across the enterprise.

Centralized Configuration Management (CCM) tools are great, especially in environments with branch offices. But CCM tools can't do the big job of making your environment inherently more secure or more flexible.

This paper focuses on how IT Managers can leverage CCM tools along with other techniques and tools to have it all: security, a uniform standard, and flexibility when needed.

Challenge

As an IT Manager, your job is split in two. On the one hand, you're asked to keep the company's desktops (or laptops or whatever types of client computers individual employees use) and servers secure. On the other hand, you're asked for systems that can be agile and work flexibly with the business as specific exceptions arise.

This isn't an easy order. A secure desktop, for instance, can be so secure that it's unusable—and no one wants that. A system that's too flexible likely means that there are no standards at all.

There has to be a way to achieve a balance here. The challenge is simple: can a desktop (or a server) be made more secure, and still remain flexible for the end user?

"The challenge is simple: can a desktop or a server be made more secure, and still remain flexible for the end user?"

Of course, IT Managers have the organization's best interests at heart. The corporate policies are usually generated from the "top down," meaning that the corporate standards dictate fairly strict **Processes, Protocols, and Procedures** (PP&Ps). These PP&Ps are put in place for good reasons. The benefits of well-heeled PP&Ps are numerous and include:

- Reduced cost for deployment: A standardized desktop means one image to deploy and one image to update in the future.
- Shorter troubleshooting time: A standardized set of applications is ideal because the help desk and desktop support staff can be immediately aware of what's placed upon any given desktop.
- Greater ease in bringing on new support staff: With the high turnover rate in the IT department, the IT Manager doesn't need to spend weeks training support staff on different types of desktop systems. In an environment where all desktops are the same it's easy for a new staff member to pick up where the last staff member left off.
- Best practices for the organization: Years of working together as a team can establish some specific applications and configurations that are optimized for the company.

Unfortunately, in the real world, one singular standardized desktop that fits everyone is simply not possible. Moreover, although it's true that PP&Ps can be put into place, branch offices oftentimes do not rigorously adhere to agreed-upon corporate standards. The common list of reasons for user or branch office non-compliance to corporate PP&Ps are:

- Increased need for self-autonomy: The absence of IT staff at a branch office means that support could be limited, or at least have the *appearance* of being limited.
- Self-regulation: Secretive projects (i.e. skunk works projects) by their very nature may need to deviate purposefully from the corporate standard.
- Unforeseen user demands for flexibility: A user in the field may specifically need an additional non-standard application to perform one task or to land that one additional client, or to work alongside another company.
- Lack of understanding of the business directive: Staff may not understand that PP&Ps are in place for their own good and to lower overall costs. Staff can see them as barriers to getting their jobs done (or worse, barriers to playing games).
- Just plain resistance: Staff may actively avoid conforming to PP&Ps because "they don't want to." They might feel as if their work is "more important" and "more specialized" than other parts of the company. This kind of issue usually requires the most support help of all.

Corporate offices can struggle to enforce PP&Ps, but can they always be successful?

Unfortunately, the answer is usually "No." The corporate offices often lose the battle of having their PP&Ps upheld uniformly, ceding power to the branches and tolerating less-than-ideal configurations, hit-and-miss security, sub-par uniformity, and inconsistent best practices.

With so many challenges, how can corporate IT Managers bridge the gap between ensuring and enforcing corporate standards and providing a system that maintains its flexibility and practicality at the periphery?

It starts with a **Centralized Configuration Management** (CCM) tool. Many organizations use a CCM tool to do the grunt work no one likes to do. Instead of running around from desktop to desktop, the CCM tool can save time by doing the dirty work of deploying software and patches, updating desktops, gathering statistics, and a hundred other tasks that would otherwise overwhelm an IT Manager and the staff. CCM tools allow IT Managers to take back some of the time that would have been allocated to maintenance tasks and frees them up to focus on more strategic work.

A good starting point for control consists of tools like:

- Microsoft's Group Policy (built into Active Directory)
- Microsoft System Center Configuration Manager (formerly SMS)
- Novell ZENworks
- LANDesk Management Suite
- Tivoli
- OpenView
- Altiris
- BigFix
- LanRev

There are many others, but these are among the most popular.

> "Although some CCM solutions perform patch management, there's simply no "magic button" in these tools that can be pressed to make the desktops "more secure."

Although CCM tools are great at automation, they do not do as well at making the environment inherently more secure. Although some perform patch management, there's simply no "magic button" in these tools that can be pressed to make the desktops "more secure."

Some more modern CCM tools now contain a "desired state" reporting and management method. This feature is intended to help the administrator control computers to a specific set of defined criteria. Unfortunately, CCM tools are far from perfect, and are sometimes used as reporting tools to simply express how far from the baseline a desktop has traveled. Moreover, it's not always easy to make exceptions for flexibility. A "desired state" is a fixed goal, and configuring alternatives from the desired state can be challenging. Additionally, in the worst case, if a desktop with a desired state becomes corrupted beyond repair, there is no way to return back to that desired state — no matter how much the administrator wishes for it to be so.

For these reasons, CCM tools are not enough to provide absolute certainty of the configuration state of a desktop. Organizations need to adopt and implement blended solutions that combine CCM tools with an additional way to positively guarantee the end state of a desktop, and the ability to quickly refresh it if it strays too far from the corporate standard.

> "A drift in standard causes stability degradation and the need for the desktop to be re-imaged back to the baseline — only to see a repeat in the cycle again."

Only then can IT Managers have confidence that their corporate directives are being honored and adhered to. This has a direct benefit on the bottom line. It simply costs less if you know precisely what to expect on end-users desktops. Less to troubleshoot, less to install, and less to maintain.

Also, ensuring that your solution works across multiple heterogeneous systems is more important than ever. With Windows, Macintosh, and Linux operating systems on corporate desktops (sometimes both or all three on some people's machines), the savvy IT Manager will ensure that the flexible and secure solution works across all platforms the company uses today and tomorrow.

By keeping in mind some of the trouble points presented here, you'll be well on your way toward achieving that secure, managed, and flexible desktop.

For the rest of the paper, we'll examine some common scenarios IT Managers face and how to minimize the exposure you'll face. Then, we'll wrap up our discussion with some ways you can work around these issues, without sacrificing flexibility or security.

The Desktop Pain Cycle

IT Managers are up against an issue called the "Desktop Pain Cycle." The situation can show up anywhere, but we'll highlight some common areas that most IT Managers run into time and time again, detracting from "real" IT management duties, consuming time, and causing frustration for the whole department, and, of course the end user as well.

In all cases, it starts when the user acquires a new desktop. This can be a repurposed computer, or a computer that comes in from the manufacturer. In most cases, the desktop is scripted or imaged to an installation. Indeed, that installation is usually a well-defined corporate standard. However, because of the specific business need that desktop is destined for, that corporate standard simply cannot be adhered to for very long. Over the long haul, that drift in standard causes stability degradation and the need for the desktop to be re-imaged back to the baseline — only to see a repeat in the cycle again.

Scenario 1: Scholastic Student or Corporate Training Labs

Student labs from elementary school to college face some of the toughest abuse. Additionally, corporate employees can sometimes act in inappropriate ways when they go to training. That's because students usually have a huge amount of free time on their hands. This can happen before or after class, or during lab time. Even with some of the best security, there is often a way to get a "toe hold" into the system and have students install the software they want. In doing so, that software degrades the experience for all subsequent users. Moreover, the whole point of student labs is to produce the same experience over and over again, regardless of the user on the desktop. So the next student's experience on that

desktop is reduced, and could mean a loss of productive learning time for that next student. Therefore, in most cases, Scholastic Student and Corporate Training labs often fail to meet the very goal they set out to achieve. In the end, these desktops are in constant need of re-imaging or re-scripting to return the desktop back to the baseline. CCM tools by themselves are of limited usefulness here. On the one hand, you might be able to use it to scan for software that isn't corporate-sanctioned, but it might be hard determining who precisely is installing the software because these desktops are used by so many different individuals.

Scenario 2: Test Labs / Quality Assurance

Corporate test beds (also known as test labs or QA labs) are also under a huge challenge. In these situations, computers are constantly being torture-tested with new software to see if it will fit a business need. These computers often go through lots of loading and unloading of software, various configurations, and trials and errors. Ultimately, their destiny is to be constantly re-imaged or re-scripted to return the desktop back to the baseline. CCM tools can re-image desktops here, but only if they're part of the CCM system. Oftentimes, test bed machines are exempt from CCM systems, because their constant re-formatting can introduce database consistency errors within the CCM system.

> "All users need computers that can fit their work patterns and not introduce pain into their work processes."

Scenario 3: Standard Corporate Desktop and Specialized Desktops

Many organizations have two types of users: users who are too fearful to make any changes to their desktops or to explore features (for fear they'll "break" something), or users who are openly brazen and actively load games, surf dangerous websites, or install their own non-sanctioned software. Companies rarely have "middle ground" employees who are both computer savvy and won't try to install extra software on their desktops. The problem is generally widespread. On the one hand, as previously expressed, additional software is often needed in the fringes of the organization to handle non-standard tasks: barcode scanning, lab sample measurements, mixing stations, shop floor duty, and other items. Sometimes these systems interface with the CCM tool, and other times they are exempt for fear that the CCM administrator himself or herself might make an erroneous change to these desktops, causing downtime for the organization.

Scenario 4: Traveling Users

Traveling users are the most autonomous users and oftentimes manipulate their computers far away from corporate reach. Installing software and manipulating configuration settings can be common, because there is little "checking in" with the corporate infrastructure. CCM tools by themselves have limited value here, because remote client computers are often the most vulnerable to image drift. Sometimes, these computers need to be returned to the office for a fresh installation, taking hours or days of productivity away from the traveling user.

The Other Side of the Desktop Pain Cycle

The Desktop Pain Cycle also includes the end-user frustration that results from rigidity. Although it's true that desktops can be locked down inside the image with scripting or via Group Policy, desktops need to be flexible enough to perform some tasks — even tasks that the creators of the image didn't originally consider.

The lack of available customization can be very frustrating to end users because it forces the user to work the way someone else expects them to work, not the way they are most productive. Additionally, for special needs individuals, a too-tightly restricted desktop can be incredibly frustrating. All users need computers that can fit their work patterns and not introduce pain into their work processes.

Therefore, a good starting point must be a middle ground in lock-down versus flexibility.

Gaining Control with Flexibility

Having a CCM tool in place to reach out and configure any damaged desktops is an excellent first step. However, with most of these tools, although it can be straightforward to install and remove software that's maintained within the CCM system, it's much more difficult to remove software that a user or local administrator has installed. Some (but certainly not all) CCM tools have the ability to restore the operating system back to the corporate baseline. Even then, however, many times an administrator (or thoughtful friend of the IT department) is asked to ensure that a desktop has loaded properly. And even then the desktop needs to be tweaked back to the specific function it was performing before the issue.

The good news, however, is that having a CCM tool in place can at least give the IT department a repeatable procedure to return a desktop back to the corporate standard. This doesn't really take into account the particulars that must be performed *after* the desktop is restored back to the baseline. But at least it's a good start.

And, if your IT department has Linux and Macintosh machines, there are CCM systems that can integrate to those architectures, giving you a singular unified starting procedure for all systems: Windows, Linux, and Macintosh.

Additionally, having one standardized restore procedure brings another advantage. When support personnel turns over, there can be a standardized set of troubleshooting procedures (per architecture) before the final step to use the CCM to perform the restore. If someone is having a desktop issue and the primary support person is absent, an available support person can work through a standard, documented set of troubleshooting guidelines—it's an easy last resort to return the desktop back to the original state. Again, because the CCM tool controls the restore, the process you perform for a Windows desktop is exactly the same for both Macintosh and Linux.

Increasing Your System Flexibility without Sacrificing Security and Corporate Standards

This section written by Faronics and Moskowitz, Inc.

Just having a CCM tool is a good first start. The CCM tool can restore desktops back to a set baseline, but in doing so, it doesn't take into account the applications, settings, and personalization inherent to many of your company's desktops.

What you need is a way to increase your flexibility without sacrificing security and corporate standards.

Finding tools that specifically work with your CCM investment can be a challenge. You could always hand-code your own process, but that approach is time consuming and ultimately more expensive because of overall maintenance.

> "Faronics' software, Deep Freeze, has one main goal: flexibly preventing some system changes while allowing others."

A better approach is to work with a vendor who knows the CCM business. Faronics' software, Deep Freeze, has one main goal: flexibly preventing some system changes while allowing others. If a desktop strays from the set standard, it will be restored to its original state upon restart. What's more, Deep Freeze can be controlled using the same CCM process you use today, and it can be performed against Windows, Macintosh, and Linux desktops. No longer will you need to re-image desktops and "start over." Instead, you'll "Freeze" the desktop at the point you want (manually, or using your CCM tool) and Deep Freeze will do the rest. Deep Freeze will make sure that all changes to a computer are temporary for only that session, which means that computers will never stray away from their baseline configurations—making them virtually indestructible while still allowing users the ability to save their documents, pictures, emails, and data.

There are also dedicated Deep Freeze plug-ins for LANDesk Management Suite and Novell ConsoleOne to allow IT administrators to manage Deep Freeze deployments through the native Novell and LANDesk toolset. Deep Freeze can easily be integrated with other CCM applications, such as BigFix, OpenView, or Tivoli, through its command-line support.

Results of Using a CCM Tool with Deep Freeze

A CCM tool is great. But it doesn't prevent a desktop from straying from its baseline. And a CCM tool can be challenging when it comes to managing exceptions. Using a CCM tool with Deep Freeze, however, means an entirely new world is available to you.

Using the same CCM processes and procedures you have today, you can manage dozens to thousands of desktops and ensure that corporate standards are enforced, and exceptions can be made. If users have their desktops stray too far from accepted standards, you can use your CCM tool in conjunction with Deep Freeze to revert the desktops back to the agreed-upon standards.

Moreover, you can configure your desktops in a very flexible fashion, where some users have different standards than other users (even on the same computer). This gives you the flexibility you want and the security you need. The overall reputation of IT management will improve because the security procedures will be enforced, even if there's a particular need for flexibility.

Ultimately, you'll drive toward more efficient, cost-effective IT management. Downtime for re-imaging will fall significantly, because it's always the same, repeatable process to get the desktop back to the agreed-upon baseline.

"Using the same CCM processes and procedures you have today, you can manage dozens to thousands of desktops and ensure that corporate standards are enforced, and exceptions can be made."

About the Author

Jeremy Moskowitz, MCSE, MCSA, and Group Policy MVP is the Chief Propeller-Head for Moskowitz, Inc. as an independent consultant and trainer for Windows technologies. He runs www.GPanswers.com, a community forum for people to get their toughest Group Policy questions answered.

Mr. Moskowitz can be found speaking at IT conferences and inside corporations all over the world and has authored or co-authored many books, including his latest two, *Group Policy: Management, Troubleshooting and Security* (Sybex), and the new *Creating the Secure Managed Desktop: Group Policy, SoftGrid, Microsoft Deployment Toolkit and Management Tools*, both with content available as eBook downloads from GPanswers.com/books.

Since becoming one of the world's first MCSE, he has performed Active Directory, Group Policy, and Windows infrastructure planning and implementation for some of the nation's largest organizations. Jeremy frequently contributes to Windows IT Pro Magazine, REDMOND Magazine, and Microsoft TechNet Magazine.

Jeremy teaches Group Policy intensive training and workshop classes recommended by Microsoft.

Learn more at www.GPanswers.com/workshop.