

## WHY WINDOWS POWER POLICIES ARE NOT ENOUGH FOR EFFECTIVE POWER MANAGEMENT

*By Mike Jager, Verismic ([www.verismic.com](http://www.verismic.com))*

Power management is becoming a buzz-phrase in the IT world which frequently brings with it an inevitable haze preventing corporations from being successful in reducing energy costs and consumption. We all watch the news each day and realize energy costs are increasing in the midst of these difficult economic times, and as could be predicted, corporations are looking for any successful methodologies to reduce these costs. However at the same time rarely will executive management endorse any power management initiatives without solid assurance end-users productivity will not be negatively impacted.

While attempting to meet these goals one specific question arises time after time; 'Why are the integrated power management features of Microsoft Windows not enough?' To be honest, over ninety percent of my client meetings either start or end with that question, and rightfully so due to a decade of confusion and misinformation regarding Microsoft Windows native power management abilities.

Power management really is quite simple, so much so that it can be boiled down to three key areas that if mastered will yield significant annual savings.

- Knowledge and visibility regarding behavior of **your** end users
- Flexibility of power management scheduling capabilities
- Enforcement of desired power management settings

Before we dive into these three areas let's clear the air now at the very beginning:

Microsoft Windows (of any version) is not 'lacking' in power management visibility and behavioral knowledge reporting. Nor is it falling short in providing flexibility of power management capabilities. Finally, Microsoft Windows and/or Active Directory's missing enforcement arm should not be seen as a dreadful oversight as they were never designed to be used as a successful corporate power management solution. Therefore it would be unfair and dishonest to say it was lacking in these three key areas.

## Knowledge and Visibility of End User Behavior

This is one of the largest missing puzzle pieces causing power management initiatives to fail. Corporations that attempt to implement power policies based on mythical 'best practices' comprised of scheduled power events such as standby/hibernate and most efficient triggers will fail. To understand why one must realize that successful power management is not based on a workstation's power consumption, rather the behavior of the humans using them. Therefore you need an extremely detailed level of visibility into your end-user's inactivity. This includes knowing:

- How much inactivity do you have in your organization?
- When does that inactivity occur? (don't be fooled into believing it is only after hours)
- Where does this inactivity occur? (inactivity varies for every single end-user)
- What is the nature of the inactivity?
- What is the time slice breakdown of the inactivity? (duration of inactivity periods)
- What is your acceptable inactivity 'cost of doing business' (how did you make this decision?)

Without visibility into the behavior of your enemy you can never win the war, and when it comes to power management inactivity is your enemy. All of these questions are impossible to answer from anywhere within the desktop Microsoft Windows operating system or Active Directory. Putting aside the fact there are no reporting capabilities whatsoever within Active Directory, these measurements are not tracking in any form.

## Flexibility of Power Management Scheduling Capabilities

This key area makes incredibly logical sense. Once you have critical visibility to target your enemy (inactivity) you need the proper tools with enough flexibility for useful and responsible power policies. As mentioned earlier this is not possible with either Microsoft Windows or Active Directory. In fact, if you are near your PC, take a break right now from reading and open your Power Options under Control Panel. Ask yourself these questions while looking through the settings:

- Am I capable of setting unique power actions for different days of the week?
- Am I capable of setting unique power actions for different hours of the day?
- Am I capable of mixing standby/hibernate/power off settings throughout a flexible policy?
- Am I capable of predicting whether the power settings I choose will be successful before enabling them?
- Am I capable of pulling a report to ensure my computer has been enforcing my settings? (since inactivity does suggest you will not be present at all times)

Since inactivity is based on human behavior it will always be highly dynamic, not static 24-hours a day, 7-days a week. Therefore you need a solution which will provide the highest level of flexibility.

Even though you will find the answer to these questions is 'no' while on your workstation, perhaps you are under the impression your IT department does have these capabilities within Active Directory behind the scenes? This would be another great set of questions to ask of your IT team to start a productive conversation between executive management and technical staff.

Again this is not a shortcoming of Microsoft Windows or Active Directory, they were never designed or meant to be a power management solution.

## Enforcement of Desired Power Management Settings

Now is the final of our three key areas to successful power management. When looking at power management, this article has explored both why most corporations fail despite the best of intentions, and how to overcome the lack of visibility/information in this increasingly common battle. Now staff needs to understand the enforcement, how does an organization use the critical intelligence about their environment and enforce the desired power behavior without negatively impacting end-user productivity. To that end, review one final round of discussion-provoking questions for you and your IT department:

- How do I ensure enforcement has 'common sense' to place end-user needs above all else while still accomplishing my power management goals?
- How do I ensure critical running applications are protected from power actions?
- How do I know workstations are behaving as desired? (without walking around at midnight)
- How do I report to executive management on power management success?
- How do I review, understand and report our success is not due to undesired impact to end-user productivity?
- How do I know when it is time to periodically review power management policies for beneficial adjustments?

It would be impossible to say which one of these questions is most important when it comes to enforcement; this is when the rubber meets the road. A power management solution can have a million bells and whistles but if it cannot deliver on enforcement all the visibility in the world will be of little value to you and your IT Department.

The last question usually provokes an interesting discussion. Why would power management settings need to be reviewed? Remember the reoccurring point in this article: power management is behavior, not technology. People change, job roles change, corporate work environments changes and therefore the behavior contributing to power management success or failure will also change. It will be critical to observe through reporting if there are reductions in power management effectiveness over periods of time and act accordingly to adjust power management policies.

Remember, power management is not a 'project', it is an ongoing operational model and as such should be treated as any other system or operating procedure within the organization. If reviewed quarterly, bi-annually, or annually responsible parties can be assured of continued success in power management.

To summarize, successful power management is absolutely an obtainable goal, in spite of the fact that so few actually achieve it due to a lack of understanding. Consider each of these three areas and realize if power management is approached with the correct strategy each area and the overall goal can be reached.

Also, when discussing these areas with your IT department, do not be surprised or disappointed if they cannot answer many of the questions above with tangible reports or evidence – they are not to blame. Your IT Department can accomplish very little utilizing only Microsoft Windows and Active Directory.

I'll leave you with a final and all too familiar comment we've all been told in our lives...always use the right tool for the right job else you're only going to make things worse.