



## What you should know about WMI based audits

*Facts behind so-called discovery audit products that promise install-and-go*

---

Microsoft put out a nifty tool some time ago called Scriptomatic on the MSDN website. With this tool you can poke around at the different things that Windows Management Instrumentation (WMI) can do and have it create VBScript you can cut-and-paste for your use. And it's pretty impressive stuff.

Since we started selling **E-Z Audit** in 2002 there have been more and more competing products that are, to be kind, little more than a bunch of WMI scripts taken from Scriptomatic or other sources and wrapped inside a usually amateur interface then presented as a true PC audit solution.

Well, no, they aren't.

First and most significantly, WMI based applications don't find *all* your program files, let alone *any* file on your PC like E-Z Audit can. Want to know about PDF files or image files? We find them, they don't. Some random .exe file copied directly to a hard drive? Sorry, no they won't see that.

This is a huge issue if you really want to know what's actually on your client PCs. An .exe file that was copied onto the hard drive from a USB drive or downloaded to it won't show up if that piece of software didn't come with an installer that actually obeys Microsoft recommended practices. You know, like malware or some dodgy piece of work you'd really rather not have on a user's PC.

But there are many other reasons that make the promise of 'install, discover, audit' less than promised. Here are just some:

- Have a lot of PCs on your LAN? Watch that LAN come to a crawl when hundreds or thousands of these WMI-based scripts start churning their way through your nodes. Our method scales way up and doesn't clog your network.
- Some software makes you change the Data Execution Prevention settings on your client PCs. Really? Think about that for a minute and decide whether this is really easy or even logical. This is impractical if not insane. We don't need this to happen.
- DCOM RPC problems. What's that? Try one of these and watch them happen. They are not fun to resolve. We couldn't care less – doesn't affect our software at all.

- You need to know the admin name and password for the local admin accounts for any PCs you are auditing. Maybe you do, maybe not, maybe there are dozens of them because you're a huge organization. For us, doesn't matter. Users can have limited user permissions and UAC turned on and it still works.
- Changes to firewalls on XP, Vista and Windows 7. Do you really want to create new Group Policy exceptions for one piece of software? And if you have other firewall products, then that adds even more complexity. We have no firewall problems – it just works.
- Some say agentless. Ok, but when that fails surprise there are 'fixes' that involve, that's right, agents to send out to remote PCs. And then have some hapless user somewhere open up ports on their servers. Our remote audits run without any of this nonsense. Try it at [www.pcauditsoftware.com](http://www.pcauditsoftware.com)
- When do these audits run? At set times, which of course have nothing to do with when PC are actually available to be audited and which mean repetitive audits that are unnecessary. We work on a schedule you set and PCs always get audited when they get back on-network, and no more than necessary.

Here's a piece from Microsoft on connecting to remote computers. It's a bit tedious and geeky but you can see from it that chances are very good that you will *not* just download-and-go like these products promise.

[http://msdn.microsoft.com/en-us/library/aa389290%28v=VS.85%29.aspx#configuring\\_a\\_computer\\_for\\_a\\_remote\\_connection](http://msdn.microsoft.com/en-us/library/aa389290%28v=VS.85%29.aspx#configuring_a_computer_for_a_remote_connection)

Does this mean WMI is a bad thing and we don't make use of it? Of course not. There are situations where it is a clean, easy and efficient tool. We just don't use it as a sole source of data gathering or even an extensive source for data gathering. And we do not rely on it 100% nor run it across your network.

And if the competing product you may have looked at is freeware, consider that not all freeware is created equal. Nobody creates freeware and spends money to promote it without some consideration of a payoff somewhere down the line unless it's some kid in their parent's cellar. And if that's the case, do you want to trust your audits to that?

Some with massive investor backing (and would they do that if there were no payoff?) are nakedly using you to get information about your computers and networks. The data may be "scrubbed", but at the end of the day you are sending details about your network to someone over whom you have no control to do what they want with that data.

Choose software that can actually deliver a true comprehensive audit that requires such simple IT admin tasks as creating a folder share and adding one line to a logon script. That's easy! Choose E-Z Audit, PC audit software made easy.