

The content in this preview is based on the last saved version of your email - any changes made to your email that have not been saved will not be shown in this preview.

## The Software Asset Management (SAM) Spotlight

For the Software Vendor, Software Licensing,  
and SAM/IT Asset Management Communities



### Windows 7 IT Asset Management: 'Locked and Loaded' ... and 'ITAM Consulting Notes from the Field'

January 2010  
Soft-Aid, [www.aid.com](http://www.aid.com)

#### In This Issue

[Windows 7 IT Asset Mgt.  
Notes from the Field. One  
Consultant's View.](#)

#### Quick Links

- [Soft-Aid Website](#)
- [Past Newsletters](#)
- [Archive of Past Slide Presentations](#)

#### Wit & Wisdom

***"It is one thing to show a [person] that he is in error, and another to put him in possession of the truth."***

**-John Locke**  
Philosopher (1632-1704)

#### Industry Studies and Stats **NEW!**

**Worldwide IT Asset Management Software 2008-2012 Forecast and 2007 Vendor Shares**, Frederick W. Broussard, IDC, Dec 2008 - IDC Doc # 215823, [More](#)

"IT organizations continue to need and use solutions that perform asset discovery and inventory ... basic asset information is even more critical as automation solutions embed asset discovery information within their operations, therefore offering streamlined operations to customers."

The Forrester Wave™: **IT Asset Life-Cycle Management, Q2 2009**, Forrester, [More](#)  
"The IT Asset Lifecycle Market will be worth \$1.04 billion in

#### Reading the IT Asset Management (ITAM) Tea Leaves.

#### Here comes Windows 7 ....

In our latest e-newsletter, we explore new IT asset management features in Windows 7 and then share 'notes from the field' in managing Software Assets.



#### Windows 7 IT Asset Management: 'Locked and Loaded' ....

I recently attended a great [Microsoft presentation on Windows 7](#) that touched on four new features that will help with IT Asset Management: (1) Applocker, (2) "Bit Locker to Go," and (3) "Windows XP Mode," and (4) DirectAccess.

Fortunately, whether to upgrade to Windows 7 is a clearer one than this chap's [decision matrix for Windows Vista](#) (very funny!). According to Michael Cherry, VP Operating Systems Research, Directions on Microsoft, "... I think Microsoft has got it right this time [with Windows 7]."\* Keep in mind, however, that no seamless migration path exists from Windows XP to Windows 7 which does not involve formatting or re-imaging the hard drive.

Applocker, "Bit Locker to Go," Windows XP Mode, and DirectAccess features are exclusive features of Windows 7. They do a good job of supplementing more traditional use of Active Directory Group Policies, which have been around for years and can restrict access to certain program groups, block installation of unauthorized software, etc.

#### What is Applocker?

AppLocker is a new feature of Windows 7 that allows one to restrict a program from running via Group Policy. It is comparable to-but better than-the Software Restriction Policies of former Windows versions, which are still supported in Windows 7 and Windows Server 2008 R2. Software Restriction Policies are not very popular among admins, because configuring them is time-consuming although it can easily be circumvented. AppLocker promises to address both downsides to Software Restriction Policies. A good list of Applocker benefits is [here](#).

According to Microsoft: "AppLocker supports multiple, independently configurable policies: executables, installers, scripts & DLLs. The multiple policies allow an organization to build rules that go beyond the traditional executable only solutions, providing greater flexibility and enhanced protection. For example, an organization could create a rule to "allow the Graphics Department to get updates directly from Adobe for Photoshop as long as it is still Adobe Photoshop version 14." This allows IT to retain control but empower users to keep their systems up to date based upon their business needs. In addition, each of these policies can be individually placed into an audit only mode allowing you to test your rules before they start blocking applications from running and potentially hurting end user productivity. AppLocker rules can be associated with a specific user or group within an organization."\*

#### What is "BitLocker to Go"?

2009, representing growth of 24% from 2008, down from 28% growth in 2007-2008." BMC, CA, LANDesk, BDNA, Eracent, HP, IBM, Novell, Service-now.com, Symantec, and USU are included in the report.

### "Does Virtualization Help with Regulatory Compliance?"

Daniel Schatz, 2009, [More](#)  
The survey aimed to provide a better understanding of security and regulatory challenges organizations face during their virtualization programs. Overall, there is a general uncertainty as to how virtualization might affect compliance with well known regulations like SOX, PCI, HIPAA and others. Consequently more than 25% of respondents mentioned some architecture or timeframe issues during their virtualization program due to compliance concerns. A surprising 13% even mentioned these concerns as one reason not to use virtualization technology in at least one area of their business. With respect to whether server virtualization had a positive impact on the organizations compliance management process a solid 30% confirmed this to be the case. According to the participants, the responsibility to ensure compliance of virtualized environments mainly falls on the Information Security department (73%), followed by Technology Operations (53%) and General Management (46%) (multiple selection possible). Even with the limited data gathered by this survey it becomes obvious that there is a wide range of views as to how virtualized environments can affect compliance requirements.

## Industry News

[See more Industry News](#)

"Microsoft's server chief talks cloud (Q&A)," 12/15/09, *cnet*, [More](#)

"Data breaches affect million state residents: credit cards, health records compromised," 1/3/10, *Boston Globe*, [More](#)

"Microsoft Taking Stock of Anti-Piracy Efforts: MS uses a day in December to highlight its ongoing efforts to stop illegal reproductions," *Redmond Channel Partner Magazine*, 12/10/09, [More](#)

"CIOs are more receptive than

According to Microsoft, "BitLocker to Go" gives IT administrators control over how removable storage devices (e.g. USB storage devices) can be utilized within their environment and the strength of protection that they require. Administrators can require data protection for any removable storage device upon which users want to write data, while still allowing unprotected storage devices to be utilized in a read-only mode. Policies are also available to require appropriate passwords, smart card, or domain user credentials to utilize a protected removable storage device."[\\*](#)

### What is "Windows XP Mode" for Windows 7?

Windows XP Mode allows one to run legacy Windows XP applications in a Windows 7 environment. It is one of Microsoft's desktop virtualization solutions and is built into certain editions of Windows 7. XP Mode is easier to install and configure than predecessor options in Windows Vista, which relied on Microsoft's Virtual PC product and was not natively incorporated into the operating system. Larger organizations that need centralized management of multiple PCs, however, should use Microsoft MED-V (Enterprise Desktop Virtualization, which is part of MDOP. Keep in mind, that Active Directory Group Policies do not apply to Windows XP Mode sessions so one's ability to control and deploy inventory agents to those sessions can be limited.

Three are other caveats: as our last newsletter touched on, one needs a virtualization ready processor to run Windows XP mode and it only works with Windows 7 Professional, Ultimate, or Enterprise editions. In addition, only the 32-bit version of Windows XP SP3 is supported in a Windows XP Mode session.

In November 2009, Microsoft released Windows XP Mode resources that installation instructions, release notes, and a guide for deploying XP Mode and scripts. In addition, there is a video that illustrates how to deploy XP Mode in corporate environments on the Microsoft web site.

### What is DirectAccess for Windows 7?

DirectAccess is a way for Windows 7 clients to securely connect to the corporate network from any location without any type of traditional VPN. This is relevant for IT Asset Management because it enables further ways for one to distribute inventory agents (or clients) to remote machines.

DirectAccess provides an encrypted bidirectional connection between the enterprise domain and the client device prior to the user logging on to the system, allowing admins to manage the remote machine via Group Policy and the like, just as if it were physically connected to the network. The connection is always on, so users don't have to remember to manually launch a [VPN client](#), and their applications, such as Microsoft Outlook and instant messaging, are always in communication with the corporate network. But there are many software and hardware requirements for DirectAccess ["that won't be seeing the light of day for a while."](#)

### Concluding Thoughts

The IT Asset Management options in Windows 7 (particularly when used in a Windows Server 2008 R2 domain environment) have great potential. As with all new technologies, fully incorporating some of these features into your environment takes careful planning. There are both pre and post requisites to using these technologies and they have their limitations as highlighted above.

### Other Microsoft Asset Management Technologies Include ...

Besides software and hardware inventory capabilities built in to Microsoft System Center Configuration Manager (SCCM) and Microsoft's Asset Inventory Service (AIS), Microsoft offers these other asset management technologies, which I shall briefly touch on.

APP-V or Application Virtualization solves application-to-application conflict issues within one's organization. Say, for example, one has a legacy line of business application that will not run on one's current operating system. Using Application Virtualization one can sequence those applications. One can stream them to the desktops within one's organization and there should be no conflict with the applications, as

ever to new software models -- and not because they're trendy," *InformationWeek Magazine*, 10/12/09 [More](#)

"When Things Go Wrong [with your SaaS Provider]," *InformationWeek Magazine*, 10/26/09 [More](#)

"Making Sense of Software Licensing [Event Recap]," Press Release from FAST Ltd, 10/13/09 [More](#)

[See more Industry News](#)

## Favorite Web Links

100 Top Movie Quotes (American Film Institute Top 100 Movies). [Link](#)

What does Google Suggest suggest about the state of humanity? [Link](#)

Nathan Myhrvold, former Microsoft CTO, is self-publishing a cook book with scientific underpinnings. He has built a laboratory kitchen, and does high-tech kitchen tinkering. [Link](#)

Earth's Weather ... Interconnected. [Link](#)

How dirty is your PC. Not as dirty as these. [Link](#)

Online Dating Advice: Exactly What To Say (and NOT to Say) In A First Message. [Link](#)

nothing is actually installed on the desktop. In short, the technology puts each app in its own "bubble" so they don't fight.

MED-V or Microsoft Enterprise Desktop Virtualization can be thought of as a more robust version of Windows XP Mode. Like Windows XP Mode, it enables you to solve application to operating system conflicts within your organization using virtualization technologies. But unlike Windows XP Mode, it provides centralized remote administration capabilities including Group Policies which is why larger organizations find it a better fit.

### Microsoft Software License Dependency Guide

In our [last e-newsletter](#), we touched on the dependencies between software and hardware and the role that IT Asset Management can play in ensuring that they are considered before performing software upgrades. I have since found a nice but dated list for Microsoft products. Microsoft's [Software Product License Dependency Reference Guide](#) is a list of Microsoft software and other associated Microsoft licenses needed to use that software. The list is useful from a licensing perspective (it shows licensing groups) but misses detailed deployment info such as the fact that [Office 2010 will be missing support for Windows XP 64-bit](#) and information on the virtualization desktop infrastructure (VDI) solutions.

### Of Interesting Note

As of mid-December 2009, the Microsoft Volume License Services (MVLS) and eOpen licensing management websites have been retired and replaced with the Microsoft Volume Licensing Service Center (VLSC). The VLSC provides, according to Microsoft, "a single, integrated portal for managing all Volume Licensing IDs, a simplified registration system, and an improved user interface that provides greater administrative controls." [More](#)

Thank you for reading.

All the Best!  
David Yashar, Managing Consultant  
[info@aid.com](mailto:info@aid.com)  
(voice) 781-569-0410



For a complete archive of past e-newsletters, click [here](#).

## Notes from the Field

### One Consultant's View. Getting a Handle on the IT Asset Environment.

#### ***Success is about the journey and the end-result!***

By Ilan Justh, [info@aid.com](mailto:info@aid.com)

So what do you do when you have been tasked with finding all of the hardware and software assets in a big corporation. I learned that preparation and following a methodical approach is the best route to success.

When working as the IT Asset Manager at a major art institute, one of my first tasks when brought on board was to create a master database of every technical asset owned by the organization which would be used to measure the value and ensure correct billings for our IT support contracts, to secure company property and data, and to ensure that the company's books accurately reflected what was deployed.

My first step was to determine what should be tracked and was considered an "IT Asset." I convened a meeting with the network and telecom groups, my direct manager, and others who had a vested stake in what we defined as an IT Asset (e.g. finance and legal).

The questions we posed to each other were many. They included: What

value might there be in tracking mice, external drives, keyboards, and sound items (speakers, microphones, etc.)? We viewed them as consumables at a low dollar and intrinsic value so we excluded them ... though anything with data stored on it would require follow-up. How about monitors? We debated this one and voted 'no' as well. The consensus was that the dollar value was below our financial threshold and also not worth repairing in case of failure. What remained were computers, printers and select external assets such as scanners (laptops of course being lumped into the first category) and phones. The telecom group opted not to have us inventory their equipment, while the network infrastructure group asked for the scope to include their servers, routers, switches, hubs, etc.

We had some inventory data though it was incomplete and inaccurate. The quantity did, however, help us estimate project time and help me in creating a project schedule. We figured out what data to log by producing a master list of previously scanned Windows devices and commercially licensable software on them and made determinations from there.

After further assessing how we might impact user groups during their working hours, we were nearing the point where teams could start searching for missing assets. We had yet to get departmental manager buy-in but had secured that of senior management. We needed the support of these managers because we would be touching EVERY machine. So we supplied them with key milestones and project dates and more information on our intent, the risks and fall back plans, and put a person in charge to answer their ongoing questions. We also let them know that we would be visiting EVERY machine and that our job would be easier if users turned off their machines and provided any sign-on passwords (in case we had to power on their machine).

We provided each team leader adhesive asset labels as the chance of finding items missing tags or tagged assets that weren't in the inventory was high. Of course we found assets in both categories. To speed things up, and aid in difficult accessibility issues, we wanted to use bar codes on each label. Each team had a scanner unit assigned to them and was trained in use. Details do matter. We even got a few mirrors that were flexible and had extension wands to reach behind devices (yes they did get used).

We debated whether to do anything else to the machines because it this exhaustive approach would only be repeated in batches in the future. We opted not to because the project already had an expansive scope. Lab equipment and stand-alone machines were the only ones we MIGHT need to touch but after considering the highly sensitive data and applications on them, we opted to exclude them (for now) from scope

Items without a tag had new bar code labels attached and were noted on our asset report sheets. If assets were already in our 'master' list then they were checked off. Secondary devices were noted as child assets to their parent computer. Printers had their queue names noted (when they were network connected) and also had their physical locations shown. We didn't just note this on the spreadsheet. We also placed the information on blueprint maps we got from the facilities group. This last set of information became critical to a follow-on printer project that I [described in a separate article](#).

Data was taken off the collected sheets and logged into our database which ensured that it has the most up-to-date data available. We concentrated on discrepancies and verifying associations between child and parent devices. After a couple of months passed, we finally had completed the inventory process. We had over 6100 units and discovered we had about 80 devices that we still could not find. Our goal was a complete inventory and while one might claim that there could be diminishing returns with locating those machines, we opted to pursue them in the hopes they might also shed light on gaps and holes in our processes and policy adherence.

We became detectives and found innovative ways to locate these assets. Our first assumption was some of them were properly disposed of or not tracked as such. Sure enough, our data disposal firm confirmed this which brought us down into the <50 range. Next, we looked at asset information we had on the devices.

In many cases we had ownership or location information even though it was dated. Many users recalled seeing or having those parts in their

possession but could not recall where they went. Some disposed of them on their own which was unauthorized. Others had stored them in storage closets "as emergency back-ups." We made sure to advise them of company policies on storing and securing IT assets which involved using the help/service desk. We secured what we could find and adjusted our support contracts accordingly, which was a nice 'win.'

We next visited technician work areas and discovered old machines and other bits and pieces stashed away. We marked all of these units as 'stored' rather than 'deployed'. We were now in single digits. The last step I took actually caused a few raised eyebrows in the network sector! I searched the company's email archives as well as the network storage array. I STRONGLY suggest you consider the relevant privacy and security issues before doing this. Sure enough, I found email messages that a couple of units had left with former employees and a printer had been lent by the marketing team to a publicist in New York.

Our project was nearing completion. Of the 6,100 items we either discovered or were in our original inventory figures, we were down to 7 missing devices and had added a few more. Luckily none were of any significant monetary value so the Company wrote those off and we were done with our baseline assessment. We had created a solid starting point that was used to ensure future inventory changes would go against a known accurate database with data points that were helpful. We were able to reduce and renegotiate our support contract, make smarter decisions on which printers to deploy, and make wiser decisions about who received what notebooks and desktops in the future.

Our master view of company IT assets also provided the data center team immeasurable value since they did not know what servers were in their environment, their locations, and the software loads. They used this data to assess their own strategies and operational processes around backups, load balancing, contracts and usage.

-----  
For more information about the privacy and security of your information, please read our Privacy Policy at: <http://www.aid.com/legal/privacy.htm>. This Newsletter is subject to our Terms of Use as listed at <http://www.aid.com/legal/termsfuse.htm>.

You should not rely on this E-Newsletter for legal advice or opinions. INFORMATION PROVIDED IN THIS E-NEWSLETTER IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND. The reader assumes the risk as to the accuracy of any information presented.

Copyright © 2010, Soft-Aid Inc. All Rights Reserved (but feel free to copy it, post it, quote it, think about it, and forward it to others so long as Soft-Aid and its web site [www.aid.com](http://www.aid.com) are mentioned as originators and copyright holders).

### [Forward email](#)

#### ✉ **SafeUnsubscribe®**

This email was sent to [dyashar@aid.com](mailto:dyashar@aid.com) by [enews@aid.com](mailto:enews@aid.com).  
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by



Soft-Aid, Inc. | 271 Salem Street | Unit G | Woburn | MA | 01801