

Reducing Costs and Increasing Productivity with Powerful Remote Problem Resolution



Table of Contents

Executive Summary	3
Introduction: The Quest to Cut Costs, Downtime and Risk.....	3
Improving IT Platform Management Efficiency with Intel® AMT.....	4
Raising the Bar on System Manageability with LANDesk® Management Suite 8.6 and Intel AMT.....	4
Extended Capabilities with LANDesk® Software Agents Installed.....	6
Conclusion.....	7
References.....	7

This document contains confidential and proprietary information of LANDesk Software ("LANDesk") and its affiliates and is provided in connection with the identified LANDesk® product(s). No part of this document may be disclosed or copied without the prior written consent of LANDesk. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LANDesk's terms and conditions of sale for such products, LANDesk assumes no liability whatsoever, and LANDesk disclaims any patent, copyright or other intellectual property right. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. LANDesk does not warrant that this material is error-free, and LANDesk reserves the right to update, correct, or modify this material, including any specifications and product descriptions, at any time, without notice.

Copyright © 2006, LANDesk Software Ltd. All rights reserved.

LANDesk is a trademark or registered trademark of LANDesk Software, Ltd. and its affiliated companies in the United States and other countries. Other brands and names may be claimed as the property of others.

LSI-0436 03/06 JBB/KL

Executive Summary

Managing computers throughout the enterprise can be complex, time consuming and expensive. IT professionals must know what hardware and software is running on their computers so they can: 1) successfully respond to financial and regulatory audits; 2) keep computers running and solve user problems to fulfill the business value of IT services; and 3) protect computers against threats such as viruses, worms and denial of service attacks.

Agent-based management services enable exceptional levels of information gathering, remote troubleshooting, and configuration security management. But an agent-based solution by itself can be limited when client software or operating systems have crashed, when new client hardware is deployed and agents have not yet been installed, or when users have disabled or tampered with agents. This can limit management effectiveness, and force IT staff to physically visit troublesome computers—a slow and expensive proposition that keeps IT staff from performing other critical tasks.

To address these problems, LANDesk and Intel Corporation (“Intel”) have partnered to extend agent-based management to enable greater levels of IT access and control. This white paper examines how LANDesk® Management Suite 8.6 supports Intel® Active Management Technology (AMT) to extend management control and enable “always-available management” for remote computers via out-of-band device discovery, healing, and security control.

Introduction: The Quest to Cut Costs, Downtime and Risk

It’s no secret that diagnosing and fixing computer problems is a costly productivity drain for both end users and IT personnel alike. Many problems, such as boot failures and hardware failures, traditionally require at least one desk-side visit by a technician just to diagnose the problem, and a second or third visit to fix the problem once it’s been diagnosed. The resultant downtime means lost productivity and money.

For example, in one study by Intel, the company reported that while desk-side visits accounted for only 5% of IT support incidents, these visits resulted in 52% of support costs, far outpacing other ongoing operations costs such as helpdesk, patch management, engineering, etc.¹ And according to Carey Schwaber of Forrester Research, corporate IT departments “spend an average of 76% of their budgets on ongoing operations, leaving just 24% for new IT investments. Such an overhead rate would be unacceptable in any other industry.”²

Another significant IT hurdle is the need for better asset management. Complete, current and accurate asset data is the foundation for IT infrastructure planning, maintenance, upgrade and retirement tasks. The problem is that timely and accurate information is a moving target—sometimes literally, with more mobile and handheld computing devices making their way into the enterprise. Standards like the IT Infrastructure Library (ITIL) and regulations like HIPAA and Sarbanes-Oxley make effective asset management critical to business success.

To ensure the complete health and productivity of their overall IT infrastructure, organizations must be able to actively manage every single PC distributed throughout their network. Unfortunately, IT departments are often unaware of the percentage of systems on the network, and some systems remain difficult to locate after they’ve been upgraded or re-imaged. Most mid-to-large sized organizations struggle to reach more than 80% to 90% of their installed machines without having to make a desk-side visit. This last 10% to 20% of their computers are not visible online either because they have been powered down, have crashed, or because management agents have accidentally or deliberately been removed.

In an August 2005 Intel Information Technology white paper, authors Bob Bogowitz and Tracie Zenti reported:

“Asset management remains a critical problem for IT organizations. Most of the U.S. corporations we surveyed reported that they were unable to find 15 to 20 percent of their assets; for some firms, the number exceeded 30 percent. Some non-U.S. corporations reported that far fewer of their platforms could be found. Inaccurate asset information also poses a security threat because IT organizations need to know which assets require securing. Unknown or unmanaged assets present critical vulnerabilities.

The financial value of ‘lost’ assets in large corporations is enormous; smaller companies face proportionate losses as well. Incomplete asset inventories lead corporations to over-purchase ‘missing’ assets and precludes the sharing or redistribution of unused or under utilized assets.”³

The inability to remotely discover and manage 100% of an organization’s computers creates a number of different problems for IT managers, CIOs and their organizations as a whole. In order to show compliance with government and industry regulations, many organizations need to be able to document their computer and software assets. This information not only needs to be complete and accurate, but it often needs to be made available shortly upon request. When automated discovery processes fail to pinpoint every machine, technicians have to drop whatever they’re doing to conduct manual audits, consuming considerable time and expense. The same holds true when organizations need inventory reports to verify the correct number of software licenses being used, as well as to facilitate the budgeting of future software purchases.

Improving IT Platform Management Efficiency with Intel AMT

Within its own organization, Intel has deployed more the 150,000 computing devices and manages an annual IT budget that supports more than 120,000 employees and contingent workers. In an effort to make PCs, laptops, servers and other devices less expensive to deploy, operate and maintain, Intel design teams worked to develop enterprise asset management and repair solutions that became Intel Active Management Technology (Intel AMT). In a nutshell, Intel AMT is a platform manageability technology designed to improve asset management and reduce repair costs and platform downtime.

This machine-resident hardware and firmware solution uses out-of-band (OOB) communication for remote device information, diagnostics, debugging, updating and control capabilities regardless of the state of the operating system (OS) and power state. It does this through remote boot capabilities, console redirection, and integrated device electronics redirect (IDE-R) drives. Intel AMT allows remote problem diagnosis even if platforms are turned off or the OS is non-operational. To achieve this, the platform must be attached to the network and plugged in to a power outlet, enabling 3.3-volt auxiliary power.

Even when a device is powered down or has a non-operational OS, Intel AMT maintains access to and management of the device. This “any platform state” access gives corporate IT departments unprecedented power to remotely discover, heal and protect computing assets. The results are more efficient computing asset management and significantly reduced IT operating costs.

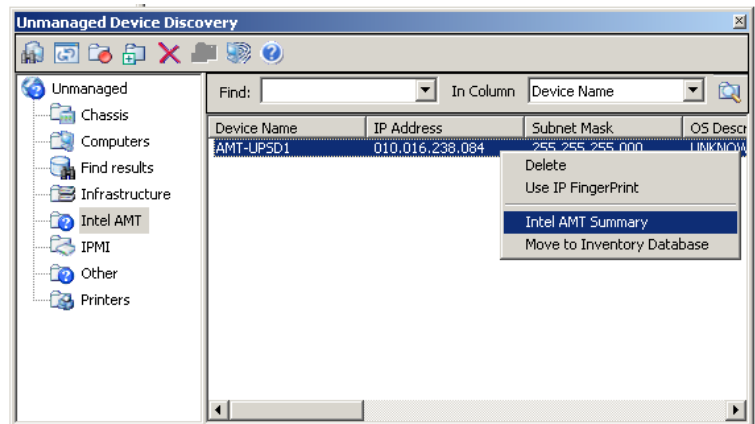
Raising the Bar on System Manageability with LANDesk Management Suite 8.6 and Intel AMT

LANDesk® Management Suite provides centralized management and protection of IT assets from a single integrated console, improving security and visibility throughout the organization. It enables IT professionals to automate systems management tasks and proactively control and protect desktops, servers and mobile devices.

The combination of LANDesk Management Suite 8.6 and Intel AMT enables organizations to remotely discover and manage all of their computers, even those that traditionally would not be visible or reachable over the network due to system failure, lack of power, or the absence of a management agent.

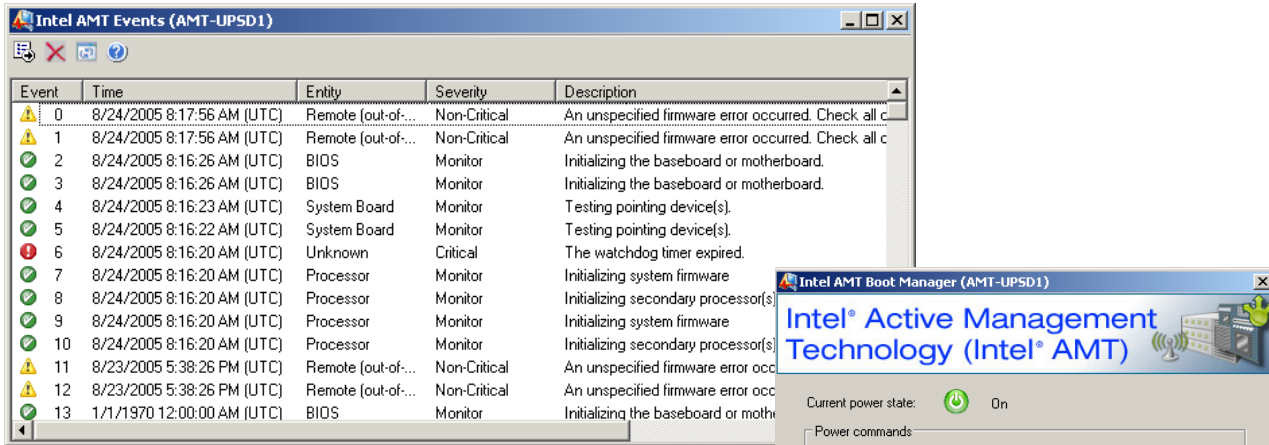
For example, Unmanaged Device Discovery (UDD) within LANDesk Management Suite 8.6 now supports hardware-based discovery through Intel AMT for more accurate hardware accounting, compliance and audit support. Discovered computers are automatically grouped in the UDD interface to make them easy to work with. Intel AMT provides basic information on the hardware environment, including manufacturer, processor, BIOS, memory and disk.

Right-click a newly discovered computer to access Intel AMT features. You can move newly discovered computers into the management database with a single click. Once the computer is added to the database, Intel AMT makes it possible to perform a variety of remote information gathering and control activities—before you’ve even installed a management agent.



As illustrated below, you can quickly open the Intel AMT event log to view hardware and boot events. You can use this information to validate the boot process, or troubleshoot hardware failures or OS crashes. Because these event logs are stored in hardware by Intel AMT, you can view them at any time regardless of the current operating state of the computer.

The AMT settings determine what events are captured in this log. You can view the date/time of the event, the source of the event (Entity column), a description, and the severity as determined by the AMT settings (Critical or Non-Critical). You can also export the log data in comma-separated value (CSV) format.



The Remote Boot Manager (right) gives you the ability to cycle power, control the remote computer's boot options, and redirect the computer's screen output or boot from an alternate source, such as a network drive, PXE server, or a bootable CD in the console computer's drive.

Extended Capabilities with LANDesk® Software Agents Installed

When LANDesk® software agents are installed, Intel AMT technology extends agent-based management to provide additional capability. For example, if you detect suspicious behavior on a managed computer and you’ve subscribed to the LANDesk® security database, you can use the “Force Vulscan on Reboot” feature to immediately reboot the remote computer and run a full LANDesk vulnerability scan to identify and remediate security threats.

The Disable OS Network feature lets you turn off a remote computer’s network card and disconnect the computer from the network. Use this capability to help reduce the potential damage caused by a virus-infected computer or to disconnect a computer being used as part of a denial of service attack. Once the computer is off the network, you can use other Intel AMT features to troubleshoot and repair the security breach. The remote computer cannot connect to the network until you explicitly restore services using the Enable OS Network feature, helping you protect against malicious attack from inside your network.

The following table lists the management options available when a device has Intel AMT only compared with Intel AMT and a LANDesk® Management Suite agent.

Available Management Options			
	Intel® AMT Only	Intel AMT in Conjunction with LANDesk® Agent	LANDesk Agent Only
Inventory	Summary	•	•
Event Log	•	•	•
Remote Boot Manager	•	•	
Disable OS Network		•	
Enable OS Network		•	
Force Vulscan on Reboot		•	
Inventory History		•	•
Remote Control	Limited	•	•
Chat		•	•
File Transfer		•	•
Remote Execute		•	•
Wake Up	•	•	•
Shut Down	•	•	•
Reboot	•	•	•
Inventory Scan	Limited	•	•
Scheduled Tasks and Policies		•	•
Group Options		•	•
Run Inventory Report		•	•
AMT Alerting		•	•

Without question, Intel AMT technology used in conjunction with LANDesk Management Suite 8.6 gives you the power to gain control over your computing environment. Easily discover Intel AMT-equipped computers and view core hardware configuration information whether the computer is powered on or not. Remotely heal and troubleshoot problems to quickly restore services and keep users working through remote power control, IDE redirect and remote console redirection. Protect the network from malicious attack with extended network disconnect and reconnect features.

Given that organizations would typically add Intel AMT enabled devices into their IT infrastructure incrementally over time, it’s reassuring from a cost standpoint to know that LANDesk® management solutions enable you to manage your current infrastructure while providing the support for Intel AMT devices as they come online in the future. Intel AMT support is built into both LANDesk Management Suite 8.6 and LANDesk® Server Manager 8.6 to extend your management control and enable both in-band and out-of-band access and control from a single, unified console.

Possible Use Case Scenarios

Isolating Denial of Service Attacks and Other Security Threats

LANDesk® Management Suite 8.6 has been extended with tools to protect the network from security threats. Suppose a system is determined to be the source of a network incident, like a Denial-of-Service attack. Traditionally, the administrator could take steps such as disabling the port on the switch or tracking down the system and shutting it down. However, disabling the port on the switch disables *all* communication to that system. Tracking down the machine can be time consuming.

Now consider the same scenario with an Intel AMT enabled system and the LANDesk® management console. With this technology combination, you could immediately disconnect the offending system by disabling its network card, whereupon the user would receive a message that this was done. Steps could then be taken to terminate the offending process, including rebooting the system to perform a vulnerability scan. Then when the machine was ready to be added back onto the network, you could re-enable the network card using the right-click menu in the console.

A Computer Virus that Can't be Removed while the System is Running

As mentioned earlier, the Intel AMT machine-resident hardware and firmware solution uses out-of-band (OOB) communication for remote device information, diagnostics, debugging, updating, and control capabilities regardless of OS state and power state. Let's assume you have a computer containing a virus that cannot be removed while the system is running. With Intel AMT technology, you could first create a diagnostic image and use the Intel AMT IDE-R to boot to that image. You could then clean up the machine's disk and subsequently reboot back to the regular OS when you were ready.

A Computer that Won't Boot

There are many reasons why a computer won't boot, and it typically requires some troubleshooting at the machine to determine the problem. Intel AMT technology and LANDesk® Management Suite can reduce or eliminate desk-side visits for diagnosing these problems. With the Intel AMT Event Log you could remotely view any hardware failure logs, OS crashes, or other events. If a hardware component were dead, you could take the replacement part with you on a one-time visit to the machine. If it happened to be a problem with the OS, the system could be re-imaged using console redirection and PXE boot, eliminating the need to visit the machine.

Keeping Track of Re-imaged Machines

Accurate platform, software and hardware inventories are necessary for regulatory compliance and for accurately managing maintenance contracts and software licenses. IT departments are often unaware of the percentage of systems on the network, and some systems remain difficult to locate after they've been upgraded or re-imaged. An Intel AMT enabled machine stores the device ID information in the hardware, and LANDesk® Management Suite uses this persistent information to index the machine, helping you avoid the issues that go into resolving duplicate entries even if you replace a hard drive or re-image an OS.

Conclusion

LANDesk® Management Suite 8.6 helps organizations save time and increase productivity by extending remote, centralized management capabilities to Intel AMT enabled computers that do not have a management agent installed, are turned off, have crashed, or do not respond. By leveraging Intel AMT and this version of LANDesk Management Suite, IT administrators can perform out-of-band management tasks on these devices, including discovery, inventory gathering, remote boot, console redirection, IDE redirection, vulnerability scans, and network disconnect, thereby reducing costly desk-side visits.

References

- 1 Intel IT Trouble Tickets & Spending, Intel Corp., 2003
- 2 Carey Schwaber, "The Expanding Purview Of Software Configuration Management," July 22, 2005
- 3 Bob Bogowitz and Tracie Zenti, Intel Corporation, "Reducing Costs with Intel Active Management Technology," August 2005