I m p r o v e d  M a n a g e a b i l i t y :  A S F  2 . 0

Today’s IT manager faces increasing pressure to reduce network maintenance costs and computing infrastructure. The typical enterprise uses a manageability software suite to fill this need. However, software alone cannot solve all manageability challenges. In some cases, a hardware-based technology is the answer. PCs installed with the Alert Standard Format (ASF) 2.0 tool can deliver these solutions to the IT manager.

Leading PC manufacturers, such as Dell and HP, have shipped over 75 million ASF-enabled PCs, and will continue to include ASF 2.0 in future PC lines. These systems can be controlled using any manageability console that supports ASF 2.0.

I T  B e n e f i t s  O v e r v i e w

• Reduces PC provisioning time by over 90%
• Enhances software patching security & reliability
• Cuts desk-side visits by remotely fixing problems
• Protects PCs from physical threats such as theft

A d v a n t a g e s  i n  U s i n g  S t a n d a r d s - B a s e d  T e c h n o l o g y

The industry has long recognized the need for some type of OS-absent functionality. In the early 1990’s, proprietary client manageability technologies were developed. Ultimately, the PC industry demanded a standards-based approach, thus giving rise to ASF. ASF provides comprehensiveness, interoperability, security, and choice for IT managers.

L a r g e  I n s t a l l e d  B a s e  i n  P l a c e

The vast majority of PCs sold by Tier 1 PC OEMs over the past three years contain ASF-enabled hardware. By the end of 2005, nearly 75 million PCs with ASF-enabled hardware will have been deployed. This run rate is expected to continue through, at a minimum, 2007 (see graphic). The typical PC refresh cycle within the enterprise is four years, so ASF is expected to be the dominant technology through at least 2010. Thus, any similar technology introduced now would take until 2010 before it has the presence and critical mass to make it useful to IT.

ASF 2.0 is the clear technology choice.
Client Manageability Use Cases
The following sections summarize typical use cases and demonstrate how IT managers can leverage their ASF-capable systems today.

Use Case 1: Shortening PC Provisioning
When provisioning new PCs, IT technicians typically download a standard corporate image to the hard drive. This is done on an often space-constrained provisioning bench. With the current method of checklisting hardware I/O components, monitoring boot processes/messages, and image downloading, the routine is both cumbersome and time consuming: up to 25 minutes per PC.

ASF eliminates many of these manual steps. ASF allows a streamlined process without technician intervention, enabling systems to be provisioned in parallel: It only takes up to 25 minutes for all PCs.

Use Case 2: Improving Software Patching

Securely and reliably patching the software image on enterprise PCs is critical to network integrity. Often, these patches are sent to client PCs overnight using Wake on LAN technology (WoL), which is used to remotely turn on PCs. WoL has limitations, including no security and no feedback, making it non-ideal for such a critical task.

ASF provides a robust solution for this critical task With ASF, management consoles support HMAC/SHA-1-based authentication, secure two-way communication, deployment of patches across multiple subnets, and resetting of hung PCs.

Use Case 3: Repairing a Hung PC
A desk-side technician visit to diagnose and repair a PC that is hung and will not boot is expensive. Because the PC cannot reach an OS-present state, most of the over-the-wire IT tools are not available. Typical causes are those associated with hardware and the system BIOS, or corrupted files.

“ASF-compliant hardware allows IT managers to further extend the power of Altiris management solutions through additional hardware control.”

--Tyler Smith, Altiris Vice President of Business Development

Use Case 4: Controlling Physical Threats
As a company expands, physical asset management becomes increasingly more difficult. Protection of valuable assets is essential to controlling costs. This can be a very difficult task. According to Safeware, an insurance company: in 2003, 600,000 computers were stolen in the United States. This equates to a loss of approximately $0.5 billion (based on a unit cost of $800).

ASF reduces the need for deskside visits
From a central location, IT can diagnose/repair problems without dispatching highly skilled Level 2 or 3 technicians to address common issues, thus reducing IT costs. ASF also allows IT to address more tasks with Level 1 technicians, rather than more costly Level 2 or 3 specialists.

ASF alerts status/changes with physical assets
Using pre-defined alerts, ASF monitors physical threats such as component theft, PC misplacement, unauthorized PC re-configuration, and malfunctioning hardware. The IT administrator is notified via the management console when a physical threat occurs, even if the PC is off or hung.