

iPass Device Management

Maintain Cost-Effective Control Over Systems Wherever They Go

- **Manage and protect end-user devices over the LAN and across the Internet**
- **Easily implement and maintain a flexible platform that automates a wide range of systems management tasks**
- **Gain high-performance features that keep users productive while desktops, laptops and handheld devices are managed**
- **Deploy patches, security updates and applications as soon as remote devices touch the Internet—without requiring a VPN connection**



Today's challenge in systems management is to efficiently maintain visibility into and control over the growing number and variety of devices used by your workforce. Laptops and handheld systems are particularly tricky as they only connect sporadically from varying remote locations. Their access methods may also be slower and less reliable. These conditions can make it difficult to quickly deliver updates to these devices and ensure they meet your corporate requirements before connecting to your network.

Fortunately, there's the iPass Device Management solution—the simple, cost-effective way to get control over all your systems and, in particular, those difficult-to-administer remote and mobile endpoints. Available as enterprise software or as an iPass-hosted service, Device Management provides a flexible platform for managing both local and distributed computers. It allows IT to efficiently implement a comprehensive suite of automated functions that includes hardware and software inventory, software distribution and management reporting. In addition, automated patching and anti-virus update management enable IT to quickly address critical security vulnerabilities.

INCREASE IT PRODUCTIVITY THROUGH A WIDE RANGE OF MANAGEMENT FUNCTIONS

iPass Device Management significantly automates local, remote and mobile systems management. With accurate inventory information and software distribution capabilities, there's no need to mail update CDs to distributed users or

SIMPLIFY SYSTEMS ADMINISTRATION

The power of iPass Device Management is in its easy-to-use Package Editor, which lets you define a wide array of systems administration tasks through a drag-and-drop interface. No scripting knowledge is required. Using Package Editor, IT administrators gain the flexibility to be as creative as they need to in addressing the management of their systems.

The following use cases illustrate some of the ways iPass customers are making the most of this flexibility:

- **Deploy Microsoft Office 2007.** Automate system inventory to ease the planning process for the move, simplify software distribution across local and remote devices and limit the impact on user productivity with mobile-optimized bandwidth throttling.
- **Send a "Kill Pill" to lost or stolen devices.** Track remote devices, encrypt hard drives of missing devices, upload or save files to FTP before taking more drastic action and remotely destroy files or folders, if needed.
- **Tame "Patch Tuesday."** Assess which devices are impacted by newly released patches, determine system dependencies, streamline deployment and automate remediation.
- **Simplify laptop-battery recalls.** Determine which of your corporate notebooks are affected by a recall, inform individual end users that their machines are affected, verify if and when batteries have been replaced and track the entire process.



spend time physically touching every PC. Some of Device Management's top features include:

Device inventory. Rapidly gather detailed hardware and software information from desktops, laptops and handheld devices. Seamlessly view your entire network of devices by silently collecting system data without user intervention. Use this valuable data to determine the full extent and configuration of your local, remote and mobile endpoints.

Software distribution. Deploy new applications, distribute software updates or simply automate many daily routine administrative IT tasks on local and distributed devices. Use the solution's smart, flexible Package Editor to define and automatically distribute updates as needed, based on your specific needs.

Broad-based patching. Extend patch management beyond Windows security patches to include non-security patches and additional applications, such as Microsoft Office, Adobe Acrobat, Macromedia Flash, WinZip and Firefox.

Easy Deployment for Mobility Software and Increased IT Productivity. New mobility software templates for deploying or upgrading iPassConnect, Mobile Broadband device drivers, VPN software from Cisco, Nortel and CheckPoint, and anti-virus software from McAfee, Symantec and Trend Micro.

Comprehensive package and patch advertisements.

Deploy packages and patches to devices as soon as they meet the conditions you define. Your updates are automatically re-advertised on a regular basis to ensure that they are applied again, should a user inadvertently uninstall any software after initial deployment.

Flexible scheduling options. Control the timing of distribution and execution for both packages and patches. For example, you can specify that a package be distributed immediately or at a scheduled date and time. You can also specify whether an update runs immediately, after a specified date and time, or within a certain time range.

Group targeting through Active Directory*. Target update packages to those PCs that actually require them.

Group devices based on appropriate OS, software, anti-virus update history and machine type to simplify the process.

Real-time reporting. Receive up-to-date inventory reports on any aspect of hardware, software, OS patches and anti-virus levels, eliminating much of the guesswork associated with systems administration.

IMPLEMENT A SINGLE SOLUTION FOR LOCAL, REMOTE AND MOBILE ENDPOINT SYSTEMS

Very soon, your workforce will likely have more laptop and handheld devices than desktops. This means you need to look for systems management solutions that take into account devices that are not "always on" and connect over unknown networks from outside your firewall. Not only does Device Management serve LAN-based systems, but it is also optimized for the more difficult remote and mobile environments.

Agent-driven enforcement mechanism. Ensure timely, accurate updates of all your end-user systems. The Device Management agent runs as a background service on end-user devices. At configurable intervals, the agent performs an endpoint assessment, fetches policies, and downloads and installs the appropriate update packages.

Unparalleled support for mobile and remote devices. Device Management requires no VPN connection or additional proxy server. It also provides dynamic bandwidth throttling and checkpoint restart for resiliency in the face of unreliable connections.

Handheld support. Extend full Device Management functionality to handheld systems based on Windows Mobile 5—one of today's fastest-growing categories of mobile devices. See the "Supported Endpoint Platforms" box for a complete list of supported handheld systems.

Windows Vista. Device Management fully supports Windows Vista in native mode, providing complete systems management functionality for this platform and a seamless user experience. Earlier versions of Windows are also supported.

REDUCE ADMINISTRATION OVERHEAD

Typically, the bulk of money spent on device management follows the initial purchase. Many systems for device

management are not very scalable and require a number of specialized staff to manage and maintain. Others require intensive and expensive training in order to be used effectively. Thanks to features of the iPass Device Management solution, you won't suffer such drawbacks.

Quick deployment. Deploy the Device Management server within a day. Likewise, you can quickly, automatically push out the agent to end-user devices.

Minimal training. Reduce initial and ongoing training costs. The solution requires only minimal administrator training before full implementation.

Highly scalable. Each Device Management server can manage up to 15,000 devices.

Fully redundant architecture with no single point of failure. Ensure fault-tolerant operation without service interruption through a fully redundant architecture. If Device Management's primary server fails, the solution automatically switches over to a secondary one.

iPass-hosted service option. iPass can host the service for you in its data centers, allowing you to avoid capital expense.

PROTECT YOUR DEVICES, SAFEGUARD YOUR BUSINESS

As you probably know, the most secure endpoint is a well-managed one. Device Management helps you protect information and infrastructure by unifying and simplifying the management of endpoint devices. It gives you the tools you need to quickly assess vulnerabilities, target patch deployments and send anti-virus updates to groups of users or individual systems:

Automated patch assessment and remediation. Simplify the ongoing task of administering Microsoft OS patches by leveraging patching expertise from Shavlik Technologies. Each time an OS patch is released from Microsoft, it directly becomes available through Device Management.

Pre-VPN updates. Distribute OS patches, anti-virus definitions and software prior to granting access to the Internet or establishing a VPN tunnel to your network.

POWERED BY SHAVLIK TECHNOLOGIES

Shavlik Technologies helps IT professionals manage assessment, scanning and remediation of security vulnerabilities due to missing patches. The industry standard HFNetChkPro™ has dramatically changed the way security patches are managed by providing a robust, detailed scanning technology that ties directly to Microsoft's security patch updates.

Device Protection. Optional, on-demand service that mitigates the risks related to use of the Internet, USB ports and rogue applications, without requiring up-front and ongoing investment in new enterprise infrastructure. This iPass-hosted service integrates Symantec Sygate Enterprise Protection with the assessment, remediation and systems administration capabilities of Device Management.

Device Lockdown.** Optional integration with personal firewalls enables IT to apply rules for locking and unlocking the firewall at different points in the connection process, based on the remediation status of the device. This helps prevent out-of-date devices from accessing the Internet or the corporate network.

Cisco Network Admission Control (NAC) Integration. Not only can you protect remote and mobile devices from threats on the Internet, you can also protect your network from vulnerable devices. Through integration with NAC, Device Management enables administrators to restrict devices that have not undergone remediation from accessing the network. It also ensures that remote and mobile workers get the security updates they need to obtain full network access and remain productive.

IMPROVE THE END-USER EXPERIENCE TO KEEP EMPLOYEES PRODUCTIVE

Device Management is specifically designed to optimize systems management while minimizing the impact on workers.

Intelligent reboot. Reduce the number of productivity-hampering reboots that affect your end users. Administrators can configure Device Management to



postpone the reboot processes a number of times during a series of patches or updates.

Priority controls. Balance management and productivity by defining an update as high priority or normal priority and if a high-speed connection is required.

Dynamic bandwidth throttling. Keep users productive while non-critical remediation occurs in the background. Device Management automatically measures the speed and utilization of a user's connection and adjusts its consumption of bandwidth accordingly.

Checkpoint restart: Automatically resume a previous download at the point where it left off, enabling files to be downloaded over a series of connections.

LEARN MORE

Interested in centrally managing your local, remote and mobile devices—even those that only sporadically attach to the corporate network? Learn more about the iPass Device Management solution today. Visit www.ipass.com.

FLEXIBLE DEPLOYMENT OPTIONS

Enterprise Software

- Resides at your network operations center
- Integrates with your existing infrastructure
- Includes remote control functionality

iPass-Hosted Service

- Resides in secure data centers monitored and managed 24x7 by iPass operations
- Includes an intuitive Web application for administration
- Frees IT from purchasing, installing and maintaining new infrastructure

SUPPORTED ENDPOINT PLATFORMS

PCs

- Microsoft Windows Vista (Business & Ultimate editions)
- Microsoft Windows 2003 Server (Standard, Enterprise, Web & Data Center editions)
- Microsoft Windows XP (Professional and Tablet editions)
- Microsoft Windows 2000 (Professional, Server, Advanced Server & Enterprise Server editions)
- Windows NT 4.0, SP6a (Server & Workstation editions)

Handheld Devices

- Microsoft Windows Mobile 5 (Smartphone and Pocket PC editions)
- Microsoft Pocket PC 2003, 2002 and 2000
- Microsoft Windows CE 5.0, .NET 4.2

* Active Directory integration is not available when Device Management is hosted by iPass.

** The device lockdown feature is available with the iPass port-blocker agent or Symantec Sygate Enterprise Protection 5.1.

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065

+1 650-232-4100
+1 650-232-4111 fx
www.ipass.com

