

Endpoint Policy Management™

Protect Remote Computers Whenever they Touch the Internet

- Automate assessment, remediation and patch management
- Simplify software distribution to mobile employees
- Update client security software whenever users connect to the Internet
- Control and customize your endpoint policies via an intuitive console
- Implement flexibly – iPass and enterprise-hosted options available



Being on the road is exhausting — not only for high-value salespeople and executives, but also for your IT staff who must deal with the productivity-killing viruses and worms that notebooks and PDAs can pick up “in the wild.” Systems management for these far-flung devices is a challenge. Not only is it difficult to update remote users quickly and cost effectively, but their machines also pose the greatest risk to your network.

Fortunately, there’s Endpoint Policy Management™ from iPass — the smart way to protect mobile users anytime they connect to the Internet. This valuable service streamlines and automates patch management for Microsoft Windows OS, version control for anti-virus updates and distribution of software to mobile endpoint devices.

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. For more information on Shavlik go to www.shavlik.com.

AUTOMATING PROACTIVE SECURITY MANAGEMENT

The Endpoint Policy Management service helps you minimize vulnerabilities by keeping mobile workers’ security software

and operating systems up-to-date and properly configured. As part of iPass’ Policy Orchestration initiative, Endpoint Policy Management gives you customized control over assessment, remediation and compliance verification for mobile endpoints as soon as they connect to the Internet. Mobile endpoints get updated even if the user merely intends to surf the Web.

Automated Patch Management: Simplify the ongoing task of administering Microsoft OS patches by leveraging patch management expertise from Shavlik Technologies. Each time an OS patch is released from Microsoft, it directly becomes available through Endpoint Policy Management.

Automated Anti-virus Updates: Define how recent a user’s definition or signature levels must be before granting network access, to strengthen your anti-virus protection. Endpoint Policy Management automates the rest of the update process.

COMPLETE INVENTORY ASSESSMENT AND SOFTWARE DISTRIBUTION

Often it is difficult to even know the full extent and configuration of your remote and mobile assets. With Endpoint Policy Management, you immediately receive a complete inventory of all hardware and software installed on your endpoint devices, including Windows OS configurations and anti-virus software. The service then runs a security assessment, without requiring user interaction, and distributes the required software to bring rouge machines into compliance.

Endpoint Policy Management can also be used to distribute any software as part of mobile systems management. With the ability to send program executable and Microsoft Installer files, you can schedule, customize and automate updates

Trusted connections. No compromises.





to resources on remote computers. Whether installing and configuring new software for groups of mobile devices or removing unwanted malicious application from one user's laptop, Endpoint Policy Management is a versatile instrument for enforcing corporate policy.

USER-FRIENDLY, AUTOMATED REMEDIATION

Endpoint Policy Management enables you to enforce remediation based on your security policies and priority levels. High-priority updates occur immediately, before users are granted access to enterprise resources. For normal priority updates, users are allowed to launch a VPN and updates take place in the background.

Dynamic Bandwidth Throttling: Measure the speed and utilization of a user's connection to allocate bandwidth accordingly, keeping users productive while non-critical remediation occurs.

Progress Notification: Keep users informed when high priority updates are being performed, so they are not surprised by remediation activity, and push non-critical updates without disruptions.

Resumable Downloads: Let users continue a previous download at the point were they left off, enabling files to be downloaded over a series of network connections.

Smart Reboot: Minimize how much updates intrude on the user experience by suppressing reboots until all patch installations have been completed, making the update process faster for users.

CUSTOMIZED CONTROL FOR PEACE OF MIND AND PRODUCTIVITY

Gain the flexibility to manage patches, track inventory and review what is installed on each end-user device through the intuitive Endpoint Policy Management console. You can even establish the priority of each update and target update packages to groups of users and devices. What's more, Endpoint Policy Management can be hosted at your network operations center or within iPass Secure Transaction Centers — so you get flexibility and customized control.

Priority Controls: Gain flexibility in balancing security and productivity by defining an update as high priority or normal priority, and whether a high-speed connection is required.

Dynamic Group Targeting: Target patches or software updates to those who actually require them, based on appropriate OS, software, anti-virus update history and machine type.

Active Directory Integration: Leverage your existing user groups to set policies, so you can streamline processes and avoid maintaining separate user databases.

Automatic Dependency Verification: Compare dependencies for each OS and anti-virus update with the status of each endpoint device automatically and assemble customized update packages.

Real-Time Reporting: Receive up-to-date inventory reports on hardware, software, OS and anti virus.

Rollback: Remove a patch update at any time, if necessary.

Remote Control: Gain access to individual users' machines to assist in troubleshooting efforts.

UNIVERSAL POLICY ENFORCEMENT WITH INTEGRATED CONNECTIVITY AND SYSTEMS MANAGEMENT

Customers of iPass connectivity services can combine Endpoint Policy Management with the iPassConnect™ universal client and DeviceID service, to lock down the VPN for true policy enforcement. With all three in place, you can make VPN launch conditional, based on remediation and device authentication. In this way, you can restrict access to devices that are protected and ensure that remote and mobile workers get the security updates they need to obtain full network access and remain productive.

SECURE CONNECTIONS WITHOUT COMPROMISE

By combining policy-based security tools with leading networks around the world, iPass helps secure mobile connectivity without compromising on access availability, user productivity or IT resources. Learn more about how Endpoint Policy Management provides trusted connections without compromise. ■

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

+1 650-232-4100
+1 650-232-4111 fx

www.ipass.com

