

A background image of a globe with a wireframe grid, showing the Americas. The globe is rendered in a light blue and grey color scheme, with a red vertical bar on the left side.

# **Endpoint Policy Management**

## **Technical Brief**

Protecting Remote Workers  
Whenever They Touch the Internet

### **Corporate Headquarters**

---

iPass Inc.

3800 Bridge Parkway

Redwood Shores, CA 94065 USA

<http://www.ipass.com>

T: +1 650.232.4100

F: +1 650.232.0227

## TABLE OF CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>4</b>
<b>Endpoint Policy Management – The Basics</b>	<b>4</b>
<b>Flexible Implementation</b>	<b>5</b>
Endpoint Policy Management–Enterprise .....	5
Endpoint Policy Management–Online.....	5
Integrated Connectivity and Systems Management .....	6
<b>How It Works</b>	<b>6</b>
Modules .....	6
Agent .....	6
Server .....	6
Administration Console.....	6
Using Endpoint Policy Management .....	7
<b>Features and Benefits</b>	<b>7</b>
Core Functionality.....	7
Performance Enhancement Features.....	8
Management and Control Features .....	8
Feature Comparison .....	9
General Features.....	9
Patch Management Features.....	10
Software Distribution/Configuration Management Features .....	10
Agent Technology Features.....	11
Anti-Virus Remediation Features .....	11
<b>Endpoint Policy Management in Action</b>	<b>11</b>
<b>Security, Far and Wide</b>	<b>12</b>
<b>Supported Platforms</b>	<b>12</b>

# Endpoint Policy Management

## PROTECTING REMOTE WORKERS WHENEVER THEY TOUCH THE INTERNET

### Executive Summary

Since the summer of 2003 when the Blaster and SoBig viruses wreaked devastating effects on business, the threat posed by malware has only increased. According to the 2004 Enterprise Security Survey<sup>1</sup> published by research house IDC, “Viruses, Trojans, worms, and malicious software reign supreme on the list of what threatens the security of an enterprise.” The average time from vulnerability to exploit is now only five to six days, meaning that you often must get updates fully distributed in less than a week to be sure your mobile and corporate assets are safe. And attacks are becoming more frequent, growing from 10 times a day to 13 times a day in just the last year according to Symantec<sup>2</sup>.

Add mobile and remote devices to the mix and the picture becomes even more complex. “Laptops, remote PCs, and other devices cause problems because they act as transfer agents that vector malicious code into the LAN via ‘trusted’ VPN connections,” writes Brian E. Burke of IDC in a paper analyzing policy-enforced client security<sup>3</sup>. Companies afflicted with viruses and worms struggle to clean up their networks—only to have them re-infected by users attaching compromised devices after the fact.

Because of such threats, enterprises are increasingly viewing security as an inherent part of remote access to the corporate network. “Traditional perimeter security technologies allow remote users to authenticate and securely connect to corporate networks, but they do not look at the security of the device connecting,” states IDC’s Burke. For this reason, it is no longer sufficient to establish a perimeter and protect the network core from external threats. Mobile devices also need to be protected from the dangers of the Internet. Without addressing the security of endpoints, companies will continue to be vulnerable to compromised end-user devices that are connect remotely.

Using Endpoint Policy Management™ from iPass has a dual effect on enterprise network security. Endpoint Policy Management enables enterprises to enforce device-level policies when users are outside of the network perimeter by streamlining the management and protection of remote and mobile computers. By providing greater security against worms and virus attacks for endpoint devices, companies can keep mobile users safe and productive, while also protecting their entire networks.

---

<sup>1</sup> IDC's Enterprise Security Survey, 2004 (IDC # 32593, December 2004),

<sup>2</sup> Symantec Internet Security Threat Report (Volume VII, March, 2005).

<sup>3</sup> Policy-Enforced Security – Myth or Reality? (IDC # 32252, November, 2004).

## Introduction

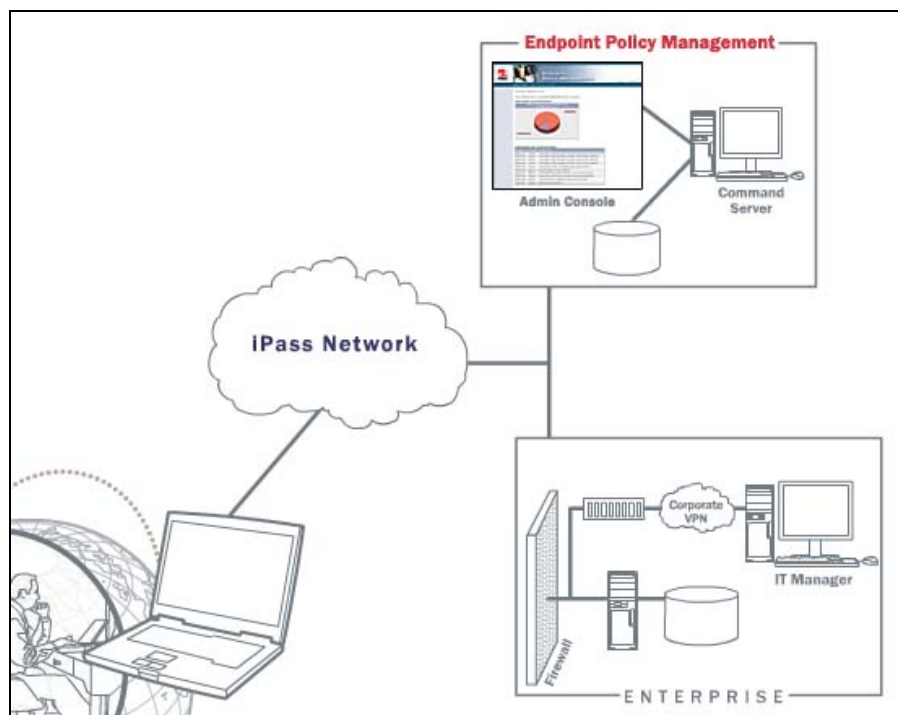
Business is becoming more mobile every day. Just look at the numbers of telecommuters, day extenders, business travelers and hallway warriors comprising the average company today.

Moving to a more virtual business model is a great boon for productivity, as it allows people to work almost anywhere at anytime. However, it can be a nightmare for IT staff, who must deal with the viruses, worms and other productivity-killing malware that endpoint devices pick up when they're outside of the network perimeter. These remote machines can bring business operations to a grinding halt if they access enterprise network resources and are infected.

Restricting out-of-compliance users from the network isn't a viable option, because they need to remain productive and responsive to customer needs. Therefore, the challenge becomes to quickly and cost-effectively update these far-flung devices with the latest security updates and OS patches—and keep them that way every time they access the Internet.

## Endpoint Policy Management – The Basics

Fortunately, there's Endpoint Policy Management from iPass—the smart way to protect mobile users any time 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.



**Figure 1:** Endpoint Policy Management automatically assesses your mobile PCs connecting to the Internet and provides remediation of any out-of-date Microsoft Windows OS patches and anti-virus definition files—before allowing remote users access to enterprise resources.

Endpoint Policy Management works by automating the assessment, remediation and management of operating system (OS) patches and anti-virus definition file updates for end-user PCs. When an end user's remote device is updated with the latest patches and updates, it is best protected against known worms, viruses and other malware. And when a new bug crops up, Endpoint Policy Management makes sure that all of your user's machines are immediately updated—even before they connect, as you deem necessary.

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 enables proactive management of endpoint security and enforcement of your company's specific security policies. You get 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.

Endpoint Policy Management permits companies to quickly bring remote and mobile devices into effective compliance with enterprise software policies as soon as they touch the Internet. Organizations can automatically distribute and upgrade software packages, as well as remove unauthorized or "rogue" applications, as soon as the device establishes an Internet or network connection. This enables network administrators to enforce required security policies more quickly by delivering software and OS patches that address critical vulnerabilities before a threat compromises the endpoint and risks infecting corporate network assets.

## **Flexible Implementation**

Architected for scalability and flexible implementation, Endpoint Policy Management is available in two service options. Endpoint Policy Management–Enterprise resides at your network operations center, while Endpoint Policy Management–Online is hosted on redundant servers within iPass Secure Transaction Centers. Both options give you the tools you need to manage endpoint policy—you choose the best implementation option for your organization.

### **Endpoint Policy Management–Enterprise**

Integrated with your existing infrastructure, Endpoint Policy Management can run “out of the box” or be easily customized to meet your company's unique needs. Active Directory integration lets you leverage your existing user groups to set policies, so you gain all the benefits of the service without managing an additional user database. In addition, the Enterprise option includes advanced scripting language that allows you to add automated software removal and installation to the powerful patch management features of the service.

### **Endpoint Policy Management–Online**

Let iPass simplify assessment, remediation and patch management for your mobile devices with this iPass-hosted service. You get all the benefits of the service with the ability to control and customize your policies via a Web console. Plus, you avoid the overhead of deploying and maintaining new infrastructure.

## **Integrated Connectivity and Systems Management**

Customers of iPass connectivity services can combine the capabilities of Endpoint Policy Management with the iPassConnect™ universal client, allowing enforced remediation of critical endpoint OS and software updates **before** launching the VPN client. Endpoint Policy Management reports back to the iPassConnect universal client on the endpoint's remediation status. The iPassConnect client will only launch a VPN after remediation is successfully completed. This protects the enterprise by granting VPN access to only those systems that meet your established policies.

## **How It Works**

While both the Enterprise and Online service options of Endpoint Policy Management look and feel like a simple client/server application with an administration console, there are actually several components working behind the scenes.

### **Modules**

Endpoint Policy Management comprises two core modules: System Manager and Patch Manager. At the highest level, System Manager is the assessment portion of the service and Patch Manager gives you the ability to remediate out-of-compliance systems. Both System Manager and Patch Manager are accessed through the Endpoint Policy administration console.

### **Agent**

An important component of the Endpoint Policy Management service is the agent installed on every user's machine. This agent performs the endpoint assessment, uploads data to the Endpoint Policy Management servers, fetches policies and installs the appropriate update packages.

### **Server**

Whether installed on your network or hosted by iPass, the server side of Endpoint Policy Management includes the following components:

- Primary Command Server
- Command Server
- Relay Server

The Primary Command Server receives communications from the agents installed on your endpoint devices and directs the agents to the Command Server. The Command Server receives requests from the distributed agents, looks up the policies and then tells the agents which packages need to be received as well as where to download the packages. Optionally, a customer may also elect to install relay servers. Relay servers can be geographically dispersed, allowing users to download packages from nearby machines.

### **Administration Console**

The Endpoint Policy Management administration console lets IT administrators control each module and server component. IT staff use this intuitive interface to manage patches, track inventory and review what is installed on each client. They can then target update packages to users and groups.

## Using Endpoint Policy Management

When the agent is first installed, it immediately performs a machine assessment and uploads the hardware and software data to the Endpoint Policy Management servers. Once a machine registers with the server, an IT administrator can track the machine's inventory and begin to administer policies. Optionally, machines can be organized into groups, so policies can be administered for groups of machines instead of on a machine-by-machine basis.

### **System Manager**

System Manager is used to manage machine inventories. From a hardware perspective, it can be used for asset management, OS configuration inventory, DMI/WMI compliance checking and serial number tracking. Endpoint Policy Management can also report on all aspects of installed software. This capability is essential to understand which aspects of software might be missing from a machine. System Manager also provides tools to create policies based on the software assessment.

### **Patch Manager**

Patch Manager is a best-in-class Microsoft patch management system based on Shavlik Technologies' expertise in Microsoft patches. Patch Manager takes the information reported by System Manager and performs a complete Microsoft patch vulnerability assessment. This assessment allows an IT administrator to create policies for patch distribution. Patch Manager eliminates the need to acquire patches and reduces the decision-making, analysis and testing needed before deployment.

### **Agent**

The Endpoint Policy Management agent makes the user experience seamless. In most cases, assessments, downloads and installations of patches or software occur in the background without any user interaction.

The agent runs silently as a service at system startup and immediately looks for Internet connectivity. Whenever it senses connectivity, it periodically searches for updates. The default setting is every 15 minutes, but IT Managers can adjust this setting. By running all the time over any Internet connection, the agent quickly and easily determines if patches are needed.

## Features and Benefits

### **Core Functionality**

The Endpoint Policy Management service offers these intelligent features to protect mobile PCs whenever they're connecting to the Internet:

- **Continuous, automated assessment.** Endpoint Policy Management provides an immediate inventory of software installed on your endpoint devices, including Windows OS configurations and anti-virus software. It then promptly runs a security assessment without requiring user interaction.
- **Automated remediation.** After assessing the endpoint device, Endpoint Policy Management offers automatic remediation of Microsoft OS patches and anti-virus definition files based on your security policies and priority levels. All update processes, including installation and reboot, occur without requiring end-user intervention, and users are informed as updates take place.

- Critical updates occur immediately, before users are given any access to enterprise resources.
- For non-critical updates, users are allowed to launch the VPN, and updates take place in the background.
- **Automated patch management.** Endpoint Policy Management simplifies 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 immediately becomes available through the Endpoint Policy Management administration console.
- **Automated anti-virus updates.** Endpoint Policy Management automates the management of anti-virus updates. Unlike Windows OS patch management, where IT staff select a specific compliance level, here they simply define how often a user's definition or signature levels must be updated before granting network access—every day, 7 days, 14 days or 30 days.

### Performance Enhancement Features

The Endpoint Policy Management service includes these intelligent performance-enhancing features to maximize productivity and minimize mobile worker disruptions:

- **Dynamic bandwidth throttling.** Allow users to remain productive while non-critical remediation occurs. These updates execute in the background using bandwidth only when it is available, allowing other, more important network traffic to have higher priority. This feature takes into account the speed of the user's connection while continually measuring the actual utilization of that connection by the user. As a result, it balances the need for user productivity and the need to get updates delivered quickly.
- **Progress notification:** Notify users about the progress of critical remediation and push non-critical updates without interrupting user productivity.
- **Resumable downloads.** Users can continue a download at the point where they left off during a previous session.
- **Smart reboot:** Suppress reboots until all patches are installed, making the update process faster for users.
- **Rollback:** IT managers can rest assured that patches and anti-virus updates are removable at any time, if necessary.

### Management and Control Features

Through the Endpoint Policy Management administration console, you get complete control over defining policies. Endpoint Policy Management, offers the following control features:

- **Dynamic group targeting.** IT staff can target update packages to only those users and groups of users who actually require them—based on appropriate OS, software, anti-virus update history and machine type.
- **Automatic dependency verification.** This feature automatically compares dependencies for each OS and anti-virus update with the status of each endpoint device and assembles a customized update package—greatly simplifying the patch management process.
- **Real-time reporting.** IT staff 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 mobile administration.

- **Priority controls.** Gain flexibility in balancing security and productivity by defining an update as critical or non-critical, and determining whether or not it should only execute over a high-speed connection.

## Feature Comparison

The following chart provides a comprehensive list of features, indicating which are available in the Enterprise and Online service options. Unless otherwise indicated, iPass connectivity services and integration with iPassConnect is not required.

### General Features

Feature	Description	Benefit	Online	Enterprise
<b>System Scan</b>	Automatic scanning of each computer for installed hardware, software and operating system configuration settings.	Retrieves information about many computers automatically so that the data can be accessed as needed, even if remote client computers are not currently online.	Yes	Yes
<b>Automatic Scan</b>	Automatically scans remote computers for information at regular intervals.	Keeps centrally stored information on computing assets up to date.	Yes	Yes
<b>Custom Scan</b>	Customization of the system scan process to include details such as Registry Key entries, .INI file entries and/or additional WMI system calls.	Allows customer to produce reports that are more specific to their environment plus allows for additional automatic groupings of machines based on customer specific data in the management console display.	No	Yes
<b>Detailed View</b>	Detailed report of individual computers that displays all information collected about each.	Provides administrator with tracking and reporting functionality for asset management and help-desk operators with a detailed view of each computer to speed in trouble shooting system problems.	Yes	Yes
<b>Tracking of Software Usage and Licensing</b>	Catalogues assets and detailed hardware configurations.	Provides administrators the ability to track all their assets from a single location even when the devices are offline.	Yes	Yes
<b>Pre-Configured Groups</b>	Scanned computers are automatically grouped based on common attributes such as operating system version.	Provides administrator with an easy way to navigate groups of computers.	Yes	Yes
<b>Custom Groups</b>	Creation of static and dynamic groups that show computers based on custom selection criteria	Allows administrator to create groupings of computers that best reflect organizational needs.	No	Yes
<b>Active Directory Groups</b>	Grouping of computers based on Active Directory Services.	Allows administrator to leverage investment made in Active Directory Services as automatic grouping rules for viewing scanned computers.	No	Yes

## Patch Management Features

Feature	Description	Benefit	Online	Enterprise
<b>Content Download</b>	Automatic download of latest Microsoft patch knowledge base from Shavlik Technologies.	Administrator does not have to remember to periodically check for new content published by Microsoft.	Yes	Yes
<b>Patch Scan</b>	Automatic scanning of client computer for missing and installed OS and application patches as well as service packs.	Retrieves information about many computers automatically so that the data can be accessed as needed by administrators, even if remote computers are not currently online. Also allows for targeted deployment of patches so patches are not sent indiscriminately.	Yes	Yes
<b>Automated Install</b>	Automatically installs one or more patches without user intervention or knowledge of patch interdependencies.	Allows reliable and easy deployment of complex and large patches to endpoint devices without having to involve the user or analyze each patch dependency prior to deployment.	Yes	Yes
<b>Deployment to Pre Configured Groups</b>	Pre-Configured groups can be used for selecting more than one computer to receive patches.	Allows faster method for deploying patches to more than one computer at the same time.	Yes	Yes
<b>Windows Update Control</b>	Ability to track and configure Windows Automatic Update settings on remote computers.	Enables administrator to centrally view and control the settings of remote computers to allow or prevent automatic download and installation of Microsoft Critical Updates via Windows Update.	Yes	No
<b>Custom Patches</b>	Ability to deploy custom patches.	Gives administrator additional control over policy and patch deployment.	No	Yes

## Software Distribution/Configuration Management Features

Feature	Description	Benefit	Online	Enterprise
Scheduled Software Distribution of Any Application or .MSI File	Send any executable or .msi file to a remote computer for installation, track the progress and retrieve the results of the installation back to a centralized server for later display usage; also includes options to schedule the distribution.	Allows administrator to automate the process of installing applications on many remote computers without having to physically be at the remote computer or perform manual one-on-one installations.	No	Yes
Package Editor	Create scripted installations of applications and perform end-user interaction operations such as prompting and logical comparisons.	Allows administrator to automate a complex configuration management process and deploy that solution to many remote computers simultaneously without having to perform the task manually. This includes rogue application removal.	No	Yes
Rogue Software Detection	Detect and remove rogue applications	Allows customers to remove unwanted malicious applications.	No	Yes

## Agent Technology Features

Feature	Description	Benefit	Online	Enterprise
<b>Control of VPN Launch</b>	Push high-priority patches and updates to endpoint devices prior to launching the VPN. <b>iPassConnect integration required.</b>	Allows administrator to enforce the security policies required by their organization on remote computers prior to granting network access via VPN.	Yes	No
<b>Dynamic Bandwidth Throttling</b>	Automatic detection of network and client download performance and adjustment of downloading process.	Downloading of patch and software distribution content has minimal impact on end user's computing and network experience.	Yes	Yes
<b>Checkpoint Restart</b>	Automatically restarts downloading operating system patch or software distribution files from the point that process was interrupted.	Allows for downloading of large files over a series of network connections made by the user without requiring the user to stay connected for the entire download process.	Yes	Yes

## Anti-Virus Remediation Features

Feature	Description	Benefit	Online	Enterprise
<b>Auto Detection of .DAT File Status</b>	Automatically scans remote computers for missing or out-of-date AV .DAT files and reports results to a centralized server for later reporting usage.	Allows administrators that use McAfee, Symantec or Trend Micro Antivirus products to centrally track the current state of their AV definition (.DAT) files centrally.	Yes	Yes
<b>Deployment of AV .DAT File Updates</b>	Ability to force updates of AV .DAT files on remote devices.	Allows customers that use McAfee, Symantec or Trend Micro Antivirus products to force an update of their specific AV definition (.DAT) file content based on time periods such as – devices whose definition files were updated a week ago, 2 weeks ago, more than a month ago etc.	Yes	Yes

## Endpoint Policy Management in Action

One morning as your IT manager commutes into work, she hears about a new virus that's exploiting a Window's vulnerability and making its way around the Web. Sounds like it could be trouble. Sure enough. When she gets into the office, her inbox is filled with 200 emails from corporate users all having similar problems with their PCs.

With Endpoint Policy Management, the IT manager brings up the administration console and selects the Microsoft patch to combat this outbreak. Because of the seriousness of the threat, the IT manager sets the update's priority as high priority. This ensures that users download the update before gaining access to the enterprise. Your IT manager clicks Apply, and the update immediately begins making its way out to the user base.

In our scenario, the Microsoft patch is only 300kB in size. So as users attempt to connect to the network, they are notified that a high-priority OS update is necessary, and the download starts immediately. Thanks to automatic remediation the user experience is painless, and users are kept informed as the update takes place.

If the IT manager had set the update as normal priority, users would have continued receiving network access through their normal secure VPN tunnel while updates took place in the background using “spare” bandwidth.

A few moments later, the download is complete and installed, and the user is connected to the enterprise network in a normal fashion.

## **Security, Far and Wide**

As you’ve now seen, as part of the iPass Policy Orchestration initiative, Endpoint Policy Management gives IT staff the tools to understand the true health of your organization’s security through simple yet granular reporting, and take action to bring the organization into compliance with corporate security policies—protecting the overall enterprise network.

iPass Endpoint Policy Management—another way iPass is providing trusted connections without compromise.

## **Supported Platforms**

### **Operating Systems:**

Microsoft Windows 2000

Microsoft Windows XP Professional/Home

### **Anti-virus:**

McAfee VirusScan Enterprise

Symantec AntiVirus Corporate Edition

Trend Micro Version

### **Optional:**

iPassConnect 3.3 or greater