

Endpoint Policy Management

Technical Brief

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



www.ipass.com
+1 650-232-4100
+1 650-232-0227 fx

TABLE OF CONTENTS

Executive Summary	3
Introduction	4
Endpoint Policy Management – The Basics	4
Flexible Implementation	4
Integrated Connectivity and Systems Management.....	5
How It Works	5
System Components	5
<i>Client</i>	5
<i>Servers</i>	5
<i>Management Console</i>	6
<i>Service Architecture – iPass-Hosted Endpoint Policy Management (“Online”)</i>	6
<i>Service Architecture – Enterprise Hosted Endpoint Policy Management (“Enterprise”)</i>	7
Functional Modules.....	7
<i>System Manager</i>	7
<i>Patch Manager</i>	8
<i>Package Editor</i>	8
Features and Benefits	9
Core Functionality	9
<i>Hardware and Software Inventory</i>	9
<i>Software Distribution</i>	9
<i>Automated Assessment and Remediation</i>	9
<i>Endpoint Lockdown</i>	9
<i>Remote Control</i>	10
Optimized User Experience	10
<i>Dynamic Bandwidth Throttling</i>	10
<i>Resumable Downloads</i>	10
Management and Control Features	10
<i>Real-Time Reporting</i>	10
<i>Dynamic Group Targeting</i>	11
<i>Active Directory Integration</i>	11
<i>Automatic Dependency Verification</i>	11
<i>Priority Controls</i>	11
Case Study: Keeping Emergency Services Responsive	12
Security, Far and Wide	12
Supported Platforms	13
Appendix 1: Feature Matrix	14
General Features.....	14
Patch Management Features	15
Software Distribution/Configuration Management Features.....	17
Agent Technology Features	18
Anti-Virus Remediation Features.....	18
Administration	19



Endpoint Policy Management

TECHNICAL BRIEF

Executive Summary

Today's traditional system management products are great tools for managing enterprise computers that are within the confines of the corporate firewall a majority of the time. However, the same cannot be said for using such products to manage and secure remote and mobile devices that only come into contact with the corporate LAN sporadically.

The difficulty with managing these devices "in the wild" is that they connect from different locations, at varying rates and intermittent intervals. In fact, it may be a long time, if ever, before sales people or employees at remote sites connect to the company network directly. Traditional systems management products are no match for the challenges posed by these remote and mobile devices.

As a result, many companies resort to mailing out updates on CD and walking users through installation over the phone. Or even worse, users may have to send in their notebooks for updates and repairs by overnight mail. The costs in terms of lost productivity due to lag times can be phenomenal, as personnel in the field are often a company's biggest revenue generators. The increasing numbers of remote and mobile workers is only making the problem much more prevalent in corporate settings.

iPass developed Endpoint Policy Management as a centralized way for organizations to efficiently, reliably track, manage and protect corporate assets regardless of a user's location or connection type. Endpoint Policy Management hides the complexities of managing distributed computers, while giving IT full control. IT staff gain the ability to securely manage mobile devices over the Internet, without requiring the user to establish a VPN connection. As long as remote systems have Internet access, they are in a managed state, helping minimize the risk of lost productivity for high-performing and revenue-generating remote workers. Endpoint Policy Management also gives IT the tools to be proactive rather than reactive through automated security patches and anti-virus updates.



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. Mobile computing is a great boon for productivity. However, it can be a real challenge for IT staff, who must somehow manage and secure the devices that these remote and mobile workers use “in the wild”—that is, not directly connected to the corporate LAN.

The challenge then is to quickly and cost-effectively update these far-flung devices with the latest OS patches, security updates and any other corporate-defined software packages—and keep them that way every time they access the Internet.

Endpoint Policy Management – The Basics

Endpoint Policy Management from iPass is the simple, cost-effective way to manage and protect mobile systems any time they connect to the Internet. iPass’ unique understanding of mobility with enterprise scalability hides the complexities of managing mobile devices while giving IT administrators full control over their mobile workforce regardless of the end-user’s location or connection type. Endpoint Policy Management helps overcome the challenge of supporting remote and mobile endpoints by providing IT administrators with the tools to manage devices and distribute software to them. All of this is done through one central management interface using advanced scripting capabilities.

Endpoint Policy Management provides accurate software and hardware inventories together with a flexible reporting engine that allows IT administrators to stay on top of the health of their end-user devices. It also offers security features including automated patch and anti-virus update management, allowing IT personnel to quickly react to security vulnerabilities. In addition, Endpoint Policy Management’s systems management capabilities enable IT administrators to address their end users’ day-to-day issues in a timely manner, while keeping them productive and in compliance with operational rules and corporate policies.

Flexible Implementation

Designed for scalability and flexible implementation, Endpoint Policy Management is available in two service options. Both give you the customizable tools you need to manage your remote and mobile devices. You choose the best implementation option for your organization.

- iPass Hosted – resides within redundant servers at iPass Secure Data Centers and provides a Web management console.
- Enterprise Hosted – integrates with your existing infrastructure and resides at your network operations center.

Carrier-Grade Reliability

When hosted by iPass, Endpoint Policy Management is monitored and managed 24/7/365 by iPass operations. The iPass Data Centers where the service is hosted provide full infrastructure redundancy and failover mechanisms for carrier-grade reliability.



Integrated Connectivity and Systems Management

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

How It Works

System Components

Several components work behind the scenes to power Endpoint Policy Management. These components include the client, servers and administration console.

The Endpoint Policy Management client is installed on endpoint devices and performs machine assessment. The client registers each machine and reports the inventory of hardware and software to the servers. Through the administration console, IT administrators can easily track each machine's inventory and manage those devices.

The following sections provide additional detail about each component of Endpoint Policy Management.

Client

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

The client runs silently as a service at system startup and immediately looks for Internet connectivity. Whenever it senses connectivity, it searches for updates at intervals determined by the IT manager. By running all the time over any Internet connection, the client quickly and easily determines if updates or patches are needed.

The Endpoint Policy Management client is expressly designed for the mobile environment and includes a number of features that make the user experience seamless. In most cases, assessments, downloads and installations of patches or software occur in the background without any user interaction.

Servers

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
- Remote Command Server (iPass-hosted only)
- Relay Server (Enterprise-hosted only)



The Primary Command Server receives communications from the clients installed on your endpoint devices and directs the agents to the Command Server. The Command Server receives requests from the distributed agents, looks up policies and then tells the clients which packages need to be deployed as well as from where to download the packages.

Management Console

The Endpoint Policy Management administration console lets IT control each module, client and server component. IT staff use this intuitive interface to track endpoint inventory, manage patches, deploy software, create and deploy packages and access reports. It is also used to automate routine administrative tasks, manage administrator access to the service and aid help desks in their troubleshooting efforts.

Service Architecture – iPass-Hosted Endpoint Policy Management (“Online”)

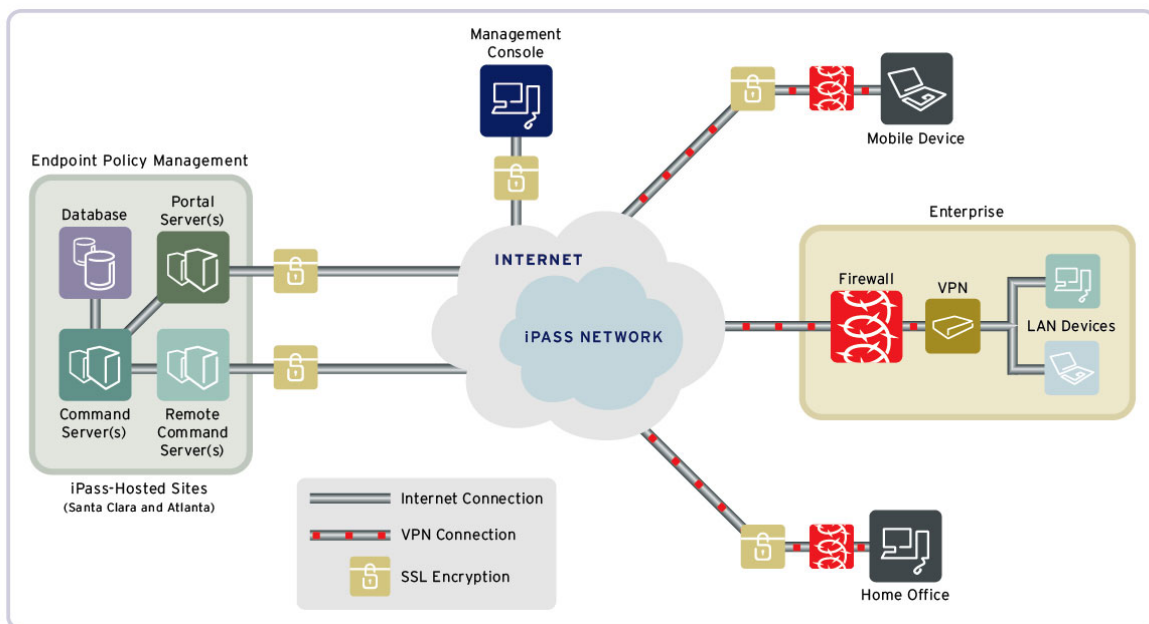


Figure 1: Endpoint Policy Management – Online Architecture. Fully available and highly redundant, the server infrastructure is deployed and maintained by iPass in our secure data centers. When hosted by iPass, the server infrastructure includes Remote Command Servers – locally resident databases that are synchronized regularly with the other back-end servers for high availability.

Service Architecture – Enterprise Hosted Endpoint Policy Management (“Enterprise”)

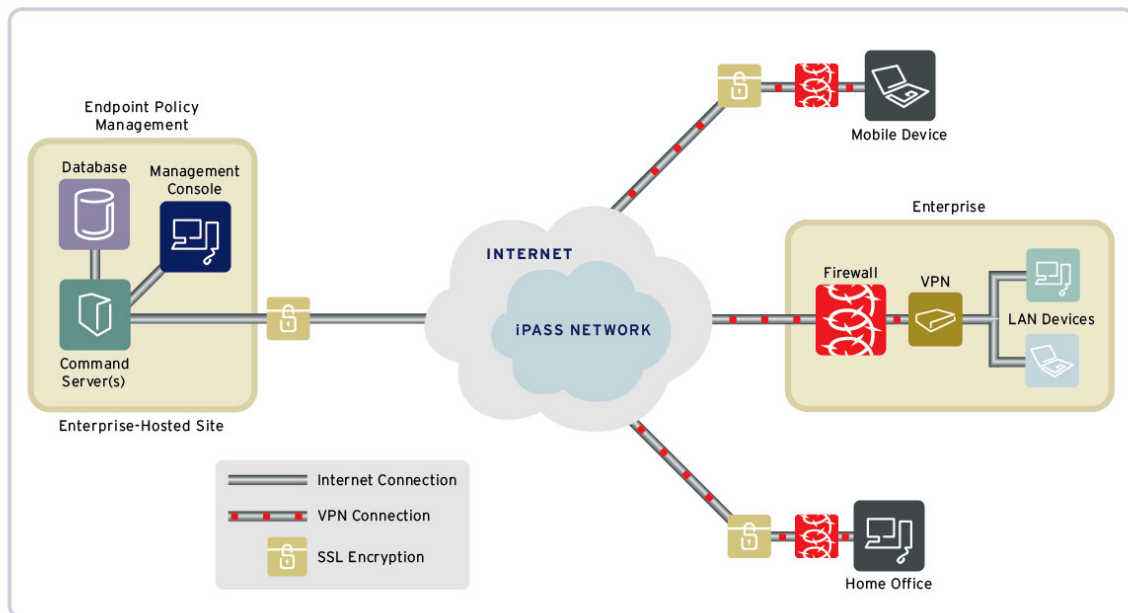


Figure 2: Endpoint Policy Management – Enterprise Architecture. Server components are housed within the customers network operations center or data center. A Win32 management console provides direct access to the Command Server and all systems management and patching tools. When hosted by the enterprise, a customer may also elect to install relay servers (not shown in this diagram). Relay servers can be geographically dispersed, allowing users to download packages from nearby machines.

Functional Modules

The system components of Endpoint Policy Management deliver two core functional modules: System Manager and Patch Manager. At the highest level, System Manager is the assessment portion of the service and Patch Manager gives administrators the ability to update out-of-compliance systems.

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 software assessment. For example, the smart, flexible package editor allows administrators to create custom packages for distribution. Package editor can employ intelligent processes such as inventory analysis to greatly automate software distribution and help secure systems by detecting and removing rogue applications.

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. When patches are released by Microsoft, the Shavik patching engine delivers them directly to Endpoint Policy Management from which they can be quickly and easily deployed to end users.

Package Editor

The Smart Package Editor is the Endpoint Policy Management tool for package creation and management. A package consists of one or more source files that you can distribute to client machines, compressed into a single file with the registered file extension .pkg. These files can be applications, data files or a set of instructions that perform actions on specific endpoint devices. Alternately, a package can consist of an image of a computer's applications and files, which you can then apply to any managed device. Many of the software distribution, patch management and anti-virus update functions of Endpoint Policy Management are controlled through the package editor.

Endpoint Policy Management includes several task packages to help you get started. You can use them as-is or modify them as needed through the package editor's easy-to-use wizard. Some examples of standard packages are listed in the table below.

Package Name	Description
Daily File Backup	Backs up files on the client machine every day at midnight. Files are backed up to Package Editor's working folder, or you can specify an alternate folder.
Execute Network Settings	Executes the network settings Snapshot daily at 6:00 a.m. to keep network settings in compliance.
Network Settings Maintenance	Creates the Network Settings Snapshot. Use it with the Execute Network Settings Package to keep network settings in compliance, by enforcing them daily.
Low Disk Space Cleanup	Checks a client machine's hard disk and determines if it has less than two megabytes of available disk space. If more than two megabytes of disk space are available, no further action is taken. If less than two megabytes of disk space are available, files are deleted from several temporary and temp folders, and the Recycle bin is emptied.
McAfee Virus Scan	Determines whether the McAfee Virus Scan application is installed on the client machine. If found, it is run every day at 8 a.m. after prompting the user. If it is not found, you are notified.
MS Backup	Schedules a weekly backup that runs every Wednesday at 5 p.m. using the Microsoft Backup program installed with Windows NT. It confirms that Microsoft Backup is installed on the client machine.

Features and Benefits

Core Functionality

Endpoint Policy Management provides the following core capabilities that are designed for the mobile environment. All Endpoint Policy Management features are integrated within a single client that is designed to make them reliable, regardless of the end user's location or connection type—even when the administrator knows nothing about the device's next connectivity session.

Hardware and Software Inventory

A key feature of Endpoint Policy Management is the ability to swiftly and easily customize inventory information—not only what information is collected, but how it is displayed. With competing products this can be a difficult and time-consuming task, if even possible—or it may require consulting services. Endpoint Policy Management also has an open database and encourages you to “mine” your own data for reporting purposes. In fact, iPass can provide you with its database schema for integrating and leveraging specialized reporting tools like Crystal Reports.

Software Distribution

The Endpoint Policy Management Smart Package Editor is a very capable application deployment tool—and much more. In fact, it can be used to automate many daily routine IT tasks—or even distribute resource libraries or other file types. Further, organizations can leverage existing packages that they have written with other scripting languages or even packages from traditional LAN-based systems-management products. Those packages can be placed in an Endpoint Policy Management package that's used as the delivery mechanism.

Automated Assessment and Remediation

Endpoint Policy Management gives you the tools you need to quickly assess vulnerabilities and target security patch deployments and anti-virus updates to groups of users or individual systems. Leveraging the award-winning scanning engine from Shavlik Technologies, Endpoint Policy Management can determine what machines are missing any given Microsoft patch and then automatically download that patch to the server. Packages are deployed via the Endpoint Policy Management client architecture—complete with checkpoint restart and bandwidth throttling. Within the console, patches are organized by severity level, release date, products affected, and who has or does not have the selected patch.

Endpoint Lockdown

This optional service enhancement helps prevent non-compliant devices from accessing the Internet or corporate network by “locking” the endpoint until high priority patches or packages are installed by Endpoint Policy Management. Integration between Endpoint Policy Management and personal firewalls enables rules for locking and unlocking the firewall to be applied at different points in the connection process. Based on the compliance status detected by Endpoint Policy Management, the lockdown feature orchestrates firewall open/close rules so that the endpoint is only able to access the resources necessary for remediation. Once Endpoint Policy Management completes remediation and the device reaches compliance, lockdown is lifted, the firewall is opened and the user is able to access the Internet and network again.



Remote Control

When hosted by the enterprise, Endpoint Policy Management includes a remote control feature that allows IT administrators and help-desk operators to act on configuration and inventory information for individual devices. Remote control allows IT administrators to assume control of a system either without end-user approval (unattended mode) or when an end user initiates a help session (attended mode). Both provide additional tools for ensuring that endpoint devices remain up to date and in compliance.

Optimized User Experience

The Endpoint Policy Management client is uniquely designed with features that minimize the impact of systems management on mobile workers. Intelligent inventory capabilities help ensure only appropriate updates occur. Dynamic bandwidth throttling keeps users productive by performing updates when spare bandwidth becomes available. Resumable downloads allow updates to continue at the point where they left off, if interrupted over an unstable connection or cancelled by the user.

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

Dynamic Bandwidth Throttling

This feature allows users to remain productive while non-critical remediation occurs. Updates execute in the background using bandwidth only when it is available, allowing other, more important network traffic to have higher priority. Dynamic bandwidth throttling 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.

Resumable Downloads

Also called checkpoint restart, this feature enables users to continue a download at the point where it left off during a previous session. This allows files to be downloaded over a series of network connections which is advantageous in mobile- and remote-working environments where the connection speed and duration are unpredictable.

Management and Control Features

Through the Endpoint Policy Management administration console, you get complete control over defining policies, implementing patches, distributing software and determining which endpoint devices require specific updates. You can even choose to rescind an update at any time through the intelligent rollback feature. Endpoint Policy Management offers the following control features.

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. Administrators can produce a diverse range of reports, from a pie chart that shows the number of machines by operating system, to a tabular report of the number of users within the various domains



on your network. All reports can be viewed through the management console, printed or exported to Microsoft Excel. Report categories include:

- **Audit:** track the activity of all EPM administrators and users. Audit reports can be run by user or by computer.
- **Computers:** display lists of systems sorted by job status, patch download activity and most recent connection.
- **Hardware:** Display information on the hardware configuration on your client machines based on BIOS vendor, CPU speed, manufacturer, memory and more.
- **Networks:** View network information by machines in a domain and users in a domain.
- **Operating system:** View operating system information on endpoint devices by operating systems and services packs.
- **Patch:** Display information on the installation status of operating system, security and application patches.
- **Software:** Display information on the software installed on endpoint devices based on anti-virus updates, Internet information servers, MS Office versions, OS, software usage and more. Administrators can also search for services and software and generate reports based on the search results.

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.

Active Directory Integration

Leveraging existing user groups to set policies, companies can streamline processes and avoid maintaining separate user databases (available when the service is enterprise-hosted).

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.

Priority Controls

Gain flexibility in balancing management 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.

Critical updates occur immediately, before users are given any access to enterprise resources.

For non-critical updates, users are allowed to launch a VPN, and updates take place in the background.



Case Study: Keeping Emergency Services Responsive

Warren County Ohio's 200,000 residents depend on more than 200 police cars, fire trucks and emergency vehicles equipped with mobile PCs. These mobile systems connect emergency personnel to one another and to critical information through a CDMA cellular backbone and various Wi-Fi networks.

Keeping all of these systems mobile and up to date had become an ordeal according to Gary Estes, data system manager for Warren County's telecommunications department. "To schedule in our PC-equipped vehicles for servicing often required two or three weeks," recalls Estes. "By the time we'd get a third of the way through our fleet, it was time to start over. As a result, a lot of our mobile PCs were out of date."

In October 2005, Warren County began using Endpoint Policy Management for patch management, software installation and hardware and software inventory on its entire emergency response fleet, 13 emergency dispatch centers and 20 data center servers. The solution paid off immediately. "We were facing a daunting update that could potential require touching every mobile system up to eight times," reports Estes. Within the first 72 hours, Endpoint Policy Management automatically updated 78 percent of the mobile systems. "Manually, it would have taken 65 days to schedule and pull that much of the fleet through our shop," informs Estes.

Warren county also uses Endpoint Policy Management to automatically place an updated version of the county's most wanted list onto every mobile desktop. With every agency in the county receiving the list, a lot of people are on the lookout for area criminals.

"Today we use Endpoint Policy Management for patch management, software installation and hardware and software inventory. We're even using it in the critical segments of our 911 emergency response center. Anything we install there has to work—and Endpoint Policy Management does."

**Gary Estes
Data System Manager
Warren County**

Security, Far and Wide

As you've now seen, Endpoint Policy Management is perfect for the organization interested in reliably tracking, managing and protecting its growing mobile workforce regardless of user location or connection type. It provides the tools to understand the true health of your company's remote and mobile devices through simple yet granular reporting, and take action by distributing customized software packages to those endpoint devices using advanced scripting capabilities.

Endpoint Policy Management. It's another way iPass is providing trusted connections without compromise.



Supported Platforms

EPM agent:

Microsoft Windows XP (including SP1 or SP2)
Microsoft Windows 2000
Microsoft Windows 2003

Anti-virus support:

McAfee VirusScan Enterprise Version 7.x, 8.0i
Symantec Norton AntiVirus Corporate Edition 9.0
Trend Micro OfficeScan Edition – 5.58, 6.5, 7.0

Web-based administrative console requires:

Microsoft Internet Explorer 5.0 or later

Optional:

iPassConnect 3.3 or greater



Appendix 1: Feature Matrix

The following charts provide comprehensive lists of features, indicating which are available in the Enterprise-hosted and iPass-hosted service options. Unless otherwise indicated, iPass connectivity services and integration with iPassConnect are not required.

General Features

Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
System Scan	Automatic scanning of endpoints for installed hardware, software and operating system configuration settings. Results are stored on a central server for future use.	Automatically retrieves information about computers and creates an inventory that can be accessed as needed, even if remote computers are not currently online.	Yes	Yes
Custom Scan	Lets administrators specify additional elements to be included in the system scan inventory, such as registry key entries, .INI file entries and additional WMI system calls.	Enables the administrator to add custom fields to inventory and keeps centrally stored information on computing assets up to date.	No	Yes
Detailed View	Detailed report displays all information collected about endpoint devices.	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.	Yes	Yes
Software Usage and Licensing Tracking	Manage assets and detailed hardware configurations.	Provides administrators with tracking and reporting functionality for asset management. Help-desk operators gain a detailed view of each computer to speed in troubleshooting.	Yes	Yes
Preconfigured Groups	Endpoint computers are automatically grouped based on common attributes, such as operating system version.	Provides administrators the ability to track all their assets from a single location, even when the devices are offline.	Yes	Yes



Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Custom Static Groups	Create static groups that show endpoint devices using customer-defined selection criteria.	Provides administrator with an easy way to define and navigate custom groups of computers. Groups are updated manually by the administrator for increased control.	Yes	Yes
Custom Dynamic Groups	Create dynamic groups that show client computers based on common attributes.	Allows administrator to create groupings of computers that are updated automatically based on system attributes.	No	Yes
Active Directory Groups	Create groups of endpoint devices based on the customer's Active Directory Services tree contents.	Allows administrator to leverage investment made in Active Directory Services, as automatic grouping rules for viewing scanned computers.	No	Yes
Pre-VPN Updates	Security and configuration updates can be executed without requiring a VPN connection. When hosted by the enterprise, flexible implementation options allow customers to set up the server infrastructure either in the DMZ in front of the corporate firewall or behind it.	Ensure that OS patches, anti-virus definitions and software are up-to-date prior to granting access to the Internet or establishing a VPN tunnel to your network.	Yes	Yes

Patch Management Features

Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Content Download	Automatic download of the latest Microsoft patch knowledge base from Shavlik Technologies servers.	Allows rapid patch deployment using pre-tested, pre-packaged patches. Patches are made available by the IT department without any user interaction.	Yes	Yes



Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Patch Scan	Automatic scan of client computers for missing and installed Microsoft OS patches, application updates and service packs. Results are stored on the central server for future use.	Automatically retrieves endpoint system information for targeted patch deployment, allowing administrators to access data, even if remote systems are not currently online.	Yes	Yes
Multilanguage OS Patching	Automatic scan of non-English versions of Microsoft Operating System patches.	Provides a single patch management system for English and non-English OS patching.	Yes	Yes
Automatic Scan	Automatic scan of endpoint devices at regular intervals.	Keeps centrally stored information about computing assets up to date.	Yes	Yes
Automated Install	Automates the installation of one or more patches, allowing the process to occur without user intervention or knowledge of patch interdependencies.	Allows a reliable and easy way to deploy complex patches without end user involvement. Lets IT administrators focus on productive activities.	Yes	Yes
Preconfigured Group Deployment	Utilizes preconfigured groups of computers to simplify patch deployment to more than one computer.	Provides a faster method for deploying patches to more than one computer at the same time.	Yes	Yes
Custom Static Group Deployment	Utilize static groups created by IT to display endpoint devices sorted by using customer-defined selection criteria.	Allows administrators to leverage groupings of computers that best reflect their organizational needs to simplify patching to more than one computer at a time.	Yes	Yes
Custom Dynamic Group Deployment	Utilize auto-populated dynamic groups that display endpoint devices based on common attributes.	Helps administrators automate machine targeting based on defined grouping profiles (software/hardware inventory). Doesn't require manual machine group assignment or removal for patch deployment.	No	Yes
Active Directory Groups	Utilize Active Directory Services tree contents for selecting more than one computer to receive one or more patches.	Allows customers to leverage their Active Directory Services while automating patch distribution using grouping rules for multiple devices.	No	Yes



Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Windows Update Control	Ability to track and configure Windows Automatic Update settings on remote computers.	Allows administrators to centrally view and control settings on remote computers and automatically install Microsoft Critical Updates via Windows Update.	Yes	No
Custom Patches	Ability to deploy custom patches.	Allows administrators to deploy custom patches.	Yes	Yes
Support for International Operating System Patches	Patch Manager supports distribution of patches that are specific to local language versions of Windows for Brazilian Portuguese, Dutch, German, Italian and Spanish.	IT administrators can manage multiple language operating systems from a single console.	Yes	Yes

Software Distribution/Configuration Management Features

Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Scheduled Software Distribution for any Application or .MSI File	Ability to schedule and send any executable or .msi file to a remote computer for installation. Track the progress and retrieve results for future use and analysis.	Administrators can automate the process of installing applications on many remote computers without having to physically touch remote systems.	Yes	Yes
Smart Package Editor	Ability to create scripted software installations and perform end user interaction operations such as prompting and logical comparisons.	Allows customers to automate complex configuration management and deployment processes.	Yes	Yes
Rogue Software Detection	Ability to detect and remove rogue applications.	Allows administrators to remove unwanted or malicious applications that users may have acquired when visiting Websites.	Yes	Yes
Data Removal	Ability to send a "poison pill" package to any lost or stolen machine.	Allows administrators to remove any confidential information or unauthorized software or content from stolen or lost machines.	Yes	Yes



Agent Technology Features

Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Control of VPN Launch	Ability to push high-priority patches and updates prior to VPN launch. Requires iPassConnect integration.	Allows administrators to enforce the security policies required by their organization on remote computers prior to granting VPN access. This helps protect the device and the corporate network.	Yes	Yes
Dynamic Bandwidth Throttling	Automatic detection of network and client download performance. Updates execute in the background using bandwidth only when it is available, allowing other, more important network traffic to have higher priority.	Designed to optimize the user experience for remote and mobile workers, patch downloads and software distribution have minimal impact on the end user's computing and network experience.	Yes	Yes
Checkpoint Restart	Automatic restart of software and patch downloads from the point where the process was interrupted.	Allows download of large files over a series of network connections without requiring the user to stay connected for the entire download process.	Yes	Yes
Proxy Agnostic	The client is proxy-aware, enabling it to auto-detect proxy settings and connect directly to the Internet if no settings are present.	Proxy-agnostic agents allow flexible deployment architecture for enterprises with or without proxies.	Yes	No

Anti-Virus Remediation Features

Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Auto Detection of .DAT File Status	Automatic scan of remote computers for missing or out-of-date AV .DAT files. Scan results are reported back to a central server for later reporting.	Allows customers that use McAfee, Symantec or Trend Micro anti-virus products to centrally track the current state of their AV definition (.DAT) files.	Yes	Yes
Deployment of AV .DAT File Updates	Ability to force updates of AV .DAT files on remote devices.	Allows customers that use McAfee, Symantec or Trend Micro anti-virus products to force an update	Yes	Yes



Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
		of their specific AV definition (.DAT) file content based on specified time periods.		

Administration

Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
iPass-Hosted Server	iPass hosts the command server and database repository in a secure data center.	Customer does not have to install, configure and manage the server-side infrastructure. The solution is hosted inside iPass Data Centers around the world which are secure and highly available.	Yes	No
Customer-Hosted Server	Customers host the command server and database repository in their own "DMZ" or data center.	Customers can manage the infrastructure themselves as well as view the data in the repository along side existing IT management systems and repositories.	No	Yes
Administration Portal	Hosted Web-based application for patch, package, AV updates, machine inventory, reporting and management. Only available when the service is hosted by iPass.	Allows easy access to all collected data and the ability to perform management operations from any location via a secure Web browser.	Yes	N/A
Administration Consoles	Server console for viewing inventory and managing remote devices. A Web-based remote administration console is also available when the service is hosted by the customer.	The server console provides a direct window into the heart of the inventory data and enables all of the management functions. The Web-based remote administration console allows IT to view system data when direct access to server machines is not available.	N/A	Yes



Feature	Description	Benefit	iPass Hosted	Enterprise Hosted
Rich Role-Based Security	Granular control of various product functions and access rights based on administrator credentials.	Allows administrator to assign different roles to groups of people within the organization. Access to full product functionality can be limited to specific roles.	Yes	Yes
Remote Control	Ability to provide help-desk operators with a Web-based view of user configuration and inventory information.	Allows help-desk staff to troubleshoot user machines more quickly and easily.	No	Yes
User Management Enhancements	READ-ONLY access that can be configured as a global setting for both administrative and non-administrative users.	Allows users with READ-ONLY access to view, but not modify information, and prevents non-administrative users (help desk) from doing harm by deploying unauthorized patches, AV updates and packages.	Yes	No
Storage Requirements	A pre-determined amount (5G) of disk space is allocated for hosted storage of content such as custom patches, packages and software for deployment.	Centralized storage environment enhances and simplifies the administrator experience.	Yes	No
Redundancy and High Availability	Complete redundancy of key infrastructure components hosted in geographically dispersed sites with fail-over from one site to another.	Removes service instability and vulnerabilities associated with a single point of failure. IT managers gain a reliable, highly available service. Agents and clients can connect without downtime during software or patch upgrades.	Yes	No

Copyright © 2006 iPass Inc. All rights reserved. iPass and the iPass logo are registered trademarks of iPass Inc. Endpoint Policy Management, iPassConnect and iPass Corporate Access are trademarks of iPass Inc. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, iPass does not accept liability for any errors or mistakes that may arise. Specifications and other information in this document may be subject to change without notice.

