iPassConnect™ Universal Client

Trusted Connections for Remote and Mobile Workers

- **Simplify mobile connectivity with a consistent user experience across virtually all network types and devices**
- **Provide zero-configuration wireless connectivity**
- **Integrate Internet access, AAA and VPN login processes for a single sign-on experience**
- **Combine with device assessment and software patching to enforce policies over all networks**

Welcome to the age of business mobility. Armed with notebook PCs and PDAs, today people work when and where they can—across corporate campuses, in client offices, on planes and trains, in their homes and sometimes at the nearest coffeehouse. To stay productive, they need a consistent way to stay in touch with information resources and people while in motion. The simpler, the better. Because people just want to get connected and get down to business.

iPass offers these nomadic workers the new, improved iPassConnect™. It's a single universal client that excels in every connectivity scenario, helping users get access—and stay connected—quicker, easier and safer than ever before. In fact, iPassConnect meets mobile users' needs so effectively that this one connection manager is all they need to get access where and when they need it most.

USE OUR NETWORK OR YOURS

iPassConnect gives users simple, on-demand connectivity to the Internet and their corporate networks across a variety of access technologies. It serves as a single interface to the iPass Mobile Office service (formerly Corporate Access), which delivers unified access across the largest global broadband roaming network and the most prevalent dial-up coverage around the world. With access to mobile data networks, Connexion by Boeing℠ in-flight wireless, and over 60,000 Ethernet and Wi-Fi hotspots—including T-Mobile® HotSpot in the U.S. and Europe—your mobile users will have plenty of convenient access options.

iPassConnect also helps users stay productive by enabling the same consistent user experience when connecting to non-iPass networks, such as your corporate wireless LAN, public hotspots and personal wireless LANs. For IT, the best part is that through iPass, these connections come complete with enforcement of security policies and detailed usage reporting.

With the new iPassConnect universal client, your company enjoys a single interface that gives mobile professionals and IT staff just what they want:

- Users get safe, easy access to the Internet and corporate networks using virtually any network technology and a variety of devices.
- IT managers gain peace of mind, knowing that centrally managed policies for access, security and usage let them control how, where and under what circumstances users connect.
- iPassConnect lets IT staff minimize operational costs through quick and simple deployment and update capabilities.

ONE CLIENT, ALL LOCATIONS AND CONNECTIONS

iPassConnect is a full-featured connection manager and single resource for all the connections your users make, whether public or private, on or off iPass networks. By outfitting your roaming employees with iPassConnect, you help them more easily identify and make use of different access technologies—public Wi-Fi, corporate wireless LANs, home wireless networks, mobile data, Ethernet and others—ensuring a more seamless connection experience, tighter security, and lower access and support costs.

Take advantage of the following iPassConnect* connectivity features:

Network Detection** automatically detects all Wi-Fi and mobile data networks that are in range, including public hotspots. Available Ethernet service is also displayed when a network cable is plugged into a live outlet.

iPass®

Support for Non-iPass Networks makes it even easier to find a local Wi-Fi hotspot or mobile data connection. iPassConnect detects and displays all available wireless networks, including those that are not iPass enabled. If a non-iPass network requires further authentication, iPassConnect will launch a web browser and VPN for the user.

Mobile Data increases the connectivity options available to users. iPassConnect can be used to easily and securely access corporate resources using a range of high-speed wireless WAN data connections through iPass and mobile network operators.

iPASSCONNECT BENEFITS: UNIVERSAL CLIENT

- One client is all mobile employees need for any connection type wherever work takes them
- Auto-detects all Wi-Fi, mobile data and Ethernet connections and displays a balloon tip to notify users of available networks
- Auto-connects to preferred campus and personal wireless networks
- Helps users access non-iPass Wi-Fi by launching a web browser and VPN

STREAMLINED NETWORK LOGIN

- Location-based interface displays all available connection options
- Available broadband networks and bookmarked locations can be accessed quickly from the system tray
- Integration with leading VPN, personal firewall and anti-virus software simplifies the connection process
- Windows Live Logon gives users the same NT domain connection experience whether in the office or remote

POLICY-BASED END-TO-END SECURITY

- Enforces connection security via VPNs, personal firewalls and anti-virus software
- VPN enforcement ensures that only in-compliance devices access the corporate network
- Integration with the optional Endpoint Policy Management™ service enables automated assessment and remediation of remote and mobile devices

LOWER TOTAL COST OF OWNERSHIP

- Lower user support and training costs
- Quick and flexible deployment
- Cost-control mechanisms for different access types
- Single bill for all access options, with support for cost-center billing
- Windows, Mac and PDA support

On Campus Roaming integrates your corporate wireless LAN to give users the same experience in the office as when working remotely. Support for EAP-TLS and PEAP-TLS provide new 802.1x options for enterprise-grade certificate-based authentication with a simple user interface.

Personal Wireless Support makes user access easier for the increasing number of residential Wi-Fi access points. Users can add home networks to their iPassConnect directory and get automated detection with network card configuration.

Wireless Network Filtering helps users select the best network by prioritizing enterprise-ready Wi-Fi and mobile data networks, displaying them with an iPass icon and listing them first. Other available wireless networks are also shown and signal strength is displayed for all detected locations.

AUTOMATED AND CONVENIENT LOGIN

iPassConnect has been designed for a streamlined and intuitive user experience. Numerous features of the new universal client make it easier for users to get connected, stay productive and get on with doing business wherever they are.

Windows Live Logon gives remote users the same functionality they're accustomed to using at the office. Windows 2000 and XP users can benefit from domain logon scripting, user-defined drive-mapping capabilities and domain password-expiration notices.

System Tray Launch lets users connect to available broadband access points and bookmarked locations from an iPass icon in the system tray, when iPassConnect runs at system startup.

Auto-Connect to Preferred Networks simplifies the connection process on trusted networks by automatically linking to personal Wi-Fi access points, corporate wireless LANs and 802.1x Ethernet connections that have been designated as preferred.

Location-based Interface** makes it fast and easy to select the best possible connection for any given location. Available wireless and Ethernet networks are automatically displayed and once a location is entered, all local connection options are presented.

VPN Auto-Connect and Flexible Launch automatically passes user name and password to the VPN client when a user connects. When both SSL and IPSec VPNs are available, iPassConnect can automatically select the best VPN option based on the connection type selected.

POLICY-BASED END-TO-END SECURITY

iPass ensures that endpoints are secured as users initiate network access through iPassConnect and before they connect to the corporate network. This is an essential security requirement for connectivity in the age of increased mobility and broadband options.

Central Management Policies allow IT staff to easily configure and automatically distribute client security to iPass users, ensuring

the most up-to-date policies are enforced during each user login. Policies can be enforced that govern the use of network access and different access methods, endpoint security software and OS patch existence, version and configuration.

Third-party Security Compatibility is achieved through the iPass Alliance™ of technology partners, which allows iPassConnect integration with offerings from a range of enterprise security vendors including leading VPN, personal firewall, intrusion detection and anti-virus products. This has the two-fold benefit of giving users secure access, while simplifying the connection process.

Pre-Connect Security blocks the user from establishing an Internet connection unless the appropriate anti-virus software, personal firewall or intrusion detection systems are engaged. If they're not running before a session, iPassConnect can auto-launch the appropriate security services before connecting to the Internet.

Internet and VPN Auto-Disconnect can be configured to automatically close the Internet connection when a VPN tunnel, personal firewall or anti-virus security solution is disabled or not running.

VPN Enforcement***** enables IT to ensure that only devices that meet established security standards are allowed to launch a VPN connection to the corporate network. In conjunction with the DeviceID™ service, iPassConnect can be used to control VPN access. Additionally, when combined with the Endpoint Policy Management service, security software and operating systems can be updated prior to VPN launch, enabling policy enforcement without locking devices out of the network.

Secure Wi-Fi Networking provides end-to-end protection over public and private networks. For corporate and private wireless LANs, WPA and WPA2 provide secure enterprise networking, especially over 802.1x connections. TKIP and AES pre-shared keys are also supported.

Encrypted Login protects passwords from the client all the way back to the corporate server over wired and Wi-Fi links. iPassConnect uses advanced public-key cryptography to protect passwords against eavesdropping and assigns each session a unique ID to help prevent replay attacks.

LOWER TOTAL COST OF OWNERSHIP

iPassConnect provides control without complexity. In addition to making it easier for users to connect, the iPass service is simple for administrators to manage and delivers several cost-saving features.

Background Updates keep the iPassConnect directory current and help users get access to the latest connection options, even if the client has not been used recently. These automatic updates occur periodically over any available access method, including the corporate LAN. No direct connection is required as long as iPassConnect is running in the background.

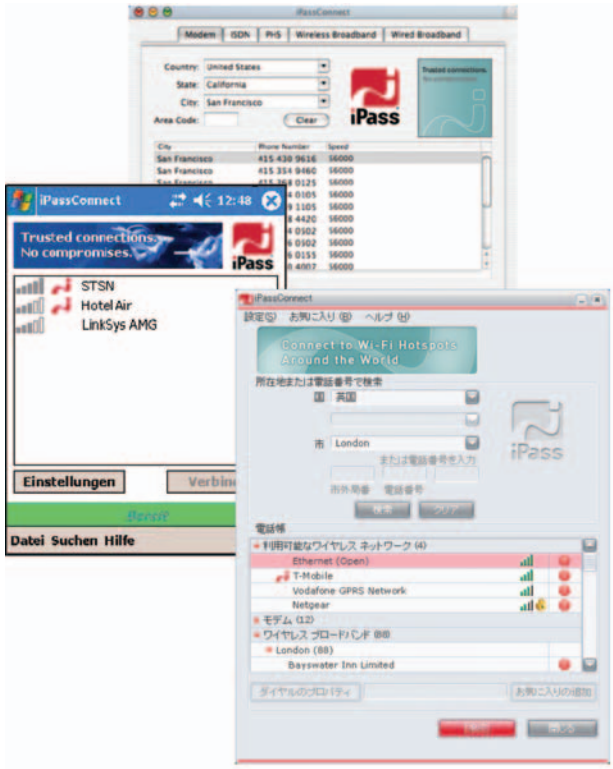
Access Point Quality and service availability are ensured by requiring all access providers to be certified Enterprise Ready. iPass frequently adds new access points and removes problematic ones. Background updates allow users to have the most current locations available, so that each connection is a success.

Dialing Intelligence greatly reduces help desk assistance calls. Users can search for local dial-up access points by number throughout the United States. All local access points are automatically dialed until a successful connection is made. Area codes are automatically added and international dialing rules are applied. Together these features save time and improve the user experience.

Universal All-Cities Numbers available in select regions, are affordable, nationwide access numbers. Toll-free access numbers, which cut down on separate billings from local phone companies, are also available.

Timeout Policies for idle and maximum session times prevent connections from being left open indefinitely, ensuring that access gets billed only for the time people actually use the iPass service.

Cost Center Billing lets IT departments easily track usage by associating users with departments, projects or domain names. User connection fees can also be charged to a corporate credit card to facilitate expense and cost center management.



iPassConnect 3.5 for Windows, iPassConnect 3.0 for PocketPC and iPassConnect 2.4 for Mac OS X.

Simple Customization is available through a variety of options that provide exceptional flexibility. For instance, administrators can add or delete RAS numbers and define connection behaviors for individual access points. iPassConnect can also be configured to display the company logo and help desk number.

TAMING CONNECTIVITY

Delivering safe, simple and effective connections lets remote and mobile professionals stay productive and gives IT staff peace of mind. iPassConnect makes it possible, whether users prefer to connect while on the road, from home or in the office. Learn why more Global 1,000 companies choose iPass to help remote and mobile professionals stay connected and stay productive. Visit www.ipass.com today.

COMPATIBILITY AND SYSTEM REQUIREMENTS

iPassConnect is compatible with security clients from these leading vendors — a listing of specific products can be found at www.ipass.com.

iPassConnect is available in the following languages with support for the platforms listed.

VIRTUAL PRIVATE NETWORKS

- Aventail
- Check Point
- Cisco Systems
- Juniper Networks
- Microsoft
- NCP
- Nortel

PERSONAL FIREWALLS AND INTRUSION DETECTION SYSTEMS

- Check Point/Zone Labs
- Internet Security Systems
- Sygate

ANTI-VIRUS SOFTWARE

- McAfee
- Symantec
- Trend Micro

SUPPORTED PLATFORMS

- Windows XP
- Windows 2000
- Windows Mobile 2003
- Mac OS X (10.1.5 and up)

SUPPORTED LANGUAGES

- English
- French
- German (Worldwide)
- Japanese
- Portuguese (Brazilian)
- Korean
- Chinese (Simplified & Traditional)
- Spanish (Mid-Atlantic)

Mac interface available in English only. PDA interface available in English, German and Japanese.

* Unless otherwise noted, features available on iPassConnect for Windows only.

** Available on iPassConnect for Windows and iPassConnect for Windows Mobile 2003.

*** Requires iPassConnect for Windows and DeviceID integration. Endpoint Policy Management integration optional.

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

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

www.ipass.com

© Copyright 2006 iPass Inc. All rights reserved. iPass and the iPass logo are registered trademarks of iPass Inc. iPassConnect, Endpoint Policy Management and DeviceID 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 which may arise. Specifications and other information in this document may be subject to change without notice..

PRDBF-IPC
7.28.06