

iPassConnect™ Universal Client

Trusted Connections for Remote and Mobile Workers

- Simplify connectivity with a consistent user experience across devices and access technologies
- 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

Business travelers, mobile professionals and teleworkers need easy-to-use, reliable access to corporate resources and the Internet. Meanwhile, IT departments struggle to provide convenient user connectivity that is secure, centrally manageable and compatible with existing infrastructure. Wi-Fi hotspots, mobile data and in-flight Internet access promise greater productivity, but also threaten to make getting connected more difficult for users and to complicate managing connectivity for the IT department.

iPass addresses the needs of both users and IT by making safe, simple and effective network access from afar a reality. Through the iPass® Corporate Access™ service, users can get on-demand mobile connectivity to their corporate networks through a variety of access methods in over 150 countries. iPass delivers this through pervasive dial-up coverage around the world and the largest global broadband roaming network. With access to mobile data networks, Connexion by BoeingSM in-flight wireless, and over 20,000 Ethernet and Wi-Fi hotspots - anchored by T-Mobile® HotSpot in the U.S. - chances are you'll find a connection where and when you need one.

iPass even helps users stay productive by enabling connections over non-iPass networks, such as public hotspots, personal wireless LANs and your corporate wireless LAN. For IT, the best part is that through iPass these connections come complete with enforcement of security policies and detailed usage reporting.

What makes all this possible is the iPassConnect™ universal client, a single interface which gives mobile professionals and IT staff just what they want.



- Users get access to corporate networks using a variety of computing devices and virtually any network technology, safely and easily.
- 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.

AUTOMATED AND CONVENIENT LOGIN

Based on usability focus groups around the world where iPass users were observed, iPassConnect has been designed for a streamlined and intuitive user experience. The results helped define the following features.

Windows Domain Pre-logout 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 Wi-Fi access points, mobile data networks and bookmarked locations from an iPass icon in the system tray, when iPassConnect runs at system startup.

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

One-Click VPN Integration automatically passes user name and password to the VPN client when iPassConnect is launched.

Trusted connections. No compromises.





WIRELESS THAT'S AS SAFE AND SIMPLE AS DIAL-UP

Wi-Fi and mobile data networks are gaining acceptance, but using them can still be complicated. iPassConnect features are designed with the goal of making wireless access as easy as dial-up. New features including signal strength display and support for non-iPass networks make wireless easier to use than ever before.

iPASSCONNECT BENEFITS:

WIRELESS AS SIMPLE TO USE AS DIAL-UP

- Auto-detects all Wi-Fi and mobile data networks
- Auto-configures users' network cards
- Displays balloon tip to notify users when Wi-Fi and mobile data networks are available
- Helps users connect to non-iPass Wi-Fi by launching a web browser and VPN
- Displays Wi-Fi and mobile data signal strength

STREAMLINED NETWORK LOGIN

- Location-based interface displays all available connection options
- Wireless networks and bookmarked locations can be accessed quickly from the system tray
- One-click integration with leading VPN, personal firewall and anti-virus software
- Windows GINA Prelogon support

POLICY-BASED END-TO-END SECURITY

- Integrated endpoint policy management performs assessment and remediation
- Enforces connection security via VPNs, personal firewalls and anti-virus software
- VPN Enforcement ensures that only in-compliance devices access the corporate network

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

Wireless Network Detection and Configuration[®] automatically detects all Wi-Fi and mobile data networks that are in range, including public hotspots. Once a wireless network is selected, the user's network card is automatically configured with the proper connection settings.

Support for Non-iPass Networks[®] makes it even easier to find a local Wi-Fi hotspot or mobile data connection. Now 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.

Wireless Network Filtering[®] helps users select the best network by prioritizing enterprise-ready Wi-Fi and mobile data networks by 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.

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.

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.

Secure Wi-Fi Authentication provides end-to-end protection. iPass access providers have implemented a security standard for Wi-Fi access gateways which authenticates hotspots by digital-certificate exchange before a connection is made. User credentials are then sent through an SSL tunnel, ensuring secure authentication from the client to the corporate network.

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 governing the use of network access and different access methods, endpoint security software and OS patch existence, version and configuration.

Endpoint Policy Management[™] protects mobile users anytime they connect to the Internet by automating security policy management, enforcement and remediation. This valuable service streamlines and automates patch management for Microsoft Windows operating systems and anti-virus updates.

Third-party Security Compatibility is achieved through the iPass Alliance™ of technology partners, which allows iPassConnect integration with 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.

SecureConnect Integration 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.

Auto-Teardown Integration 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 which 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 Endpoint Policy Management, security software and operating systems can be updated prior to VPN launch, enabling policy enforcement without locking devices out of the network.

iPass Secure End-to-end Encrypted Login (iSEEL) 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.

Quality-Based Phonebook Sorting automatically checks for an updated access-point directory upon each successful connection. iPass frequently adds new access points and removes problematic ones. This allows users to have the most current numbers available, displayed in order of measured reliability, so that each connection is a success.

Dialing Intelligence greatly reduces help desk assistance calls and user aggravation. For dial-up calls, iPassConnect automatically knows whether to add an area code within the United States and correctly applies international dialing rules.

Local Number Lookup searches for local dial-up access throughout the United States, speeding connections and reducing long-distance costs.

Smart Redial saves time and reduces user frustration by using the built-in redundancy of the iPass network. iPassConnect automatically dials all local access points until it makes a successful connection.

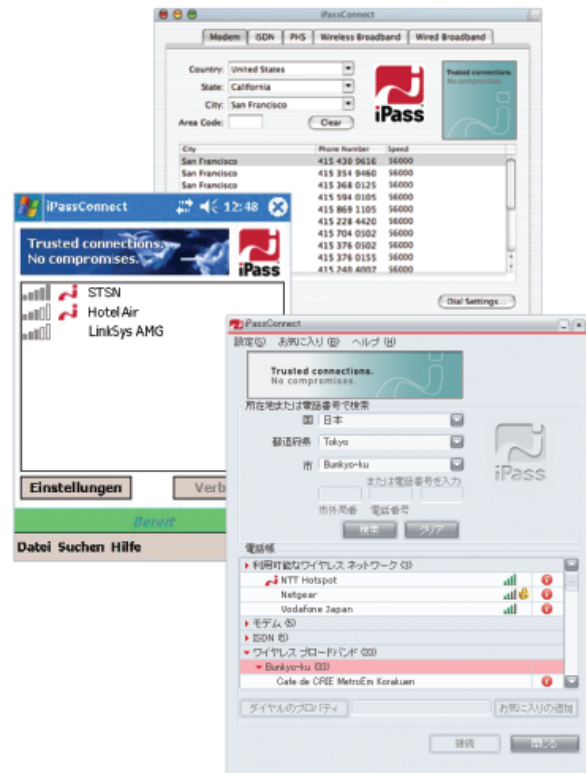
Universal All-Cities Numbers available in select regions, are affordable, nationwide access numbers. Toll-free access numbers, which cut down on separate billings from local phone companies, are also available.

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.

Credit Card Billing enables user-connection fees to be charged to a corporate credit card to facilitate expense and cost center management.

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.



iPassConnect 3.35 for Windows, iPassConnect 3.0 for PocketPC and iPassConnect 2.4 for Mac OS X.



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 a desktop, notebook or handheld device to access the corporate network. Learn why more Global 1,000 companies choose iPass to help remote and mobile professionals stay connected to the office and their customers.

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
- Microsoft
- NCP
- Nortel

PERSONAL FIREWALLS AND INTRUSION DETECTION SYSTEMS

- Internet Security Systems
- Sygate
- Zone Labs

ANTI-VIRUS SOFTWARE

- Network Associates/McAfee
- Symantec/Norton
- 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.

ⁱ Available on iPassConnect 3.x for Windows only. Version 3.3 or above required for Mobile Data and Endpoint Policy Management. Access to non-iPass networks and Connexion by Boeing in-flight hotspots is subject to additional service charges.

ⁱⁱ Available on iPassConnect 3.x for Windows and iPassConnect 3.x for Windows Mobile 2003.

ⁱⁱⁱ Requires iPassConnect 3.35 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

