

iPass® Mobile Office

Increasing Mobile Productivity While Delivering Control

- Provide mobile employees with global connectivity over world's largest virtual network
- Simplify the user experience through one interface for all connections
- Maintain control over how users connect while leveraging your existing security investments
- Streamline administration and maintenance with web-based management tools through the iPass Portal

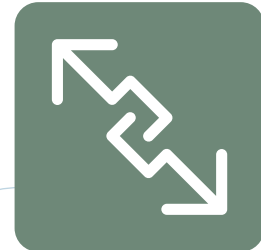
Business takes place everywhere. Take a look around these days. It's not just the traditional business travelers you see working while on the move. New classes of users are taking advantage of Wi-Fi hotspots between sales calls, the corporate wireless LAN between office meetings, and home broadband links after-hours. Clearly, companies that make the most of these exciting new mobile access options can increase their workforce productivity and gain a competitive advantage.

HELPING TO ACCOMPLISH YOUR MOBILITY STRATEGY

The iPass Mobile Office service (formerly Corporate Access) lets your company do just that. It features a single universal client for a consistent user experience across multiple access types. Your users gain on-demand connectivity to the Internet and corporate resources wherever they need access—whether they're roaming in far-away places, working from home or using your corporate wireless LAN.

Over the world's largest virtual network, iPass provides universal policy enforcement that tightly links access control to a user's compliance with your company's connectivity and security policies. Mobile Office also helps reduce your staffing requirements and total cost of ownership, through professional support for accelerated service rollout, customized training services, and extensive Web-based reporting and management tools.

It's everything you need to unify connectivity, security and management in a single solution for remote and mobile workers—helping you to make the most of mobility.



iPASS MOBILE OFFICE SERVICE OFFERS:

- The world's largest connectivity footprint made up of over 60,000 Ethernet and Wi-Fi access points, including T-Mobile® HotSpot locations in the U.S. and Europe; mobile data services; ubiquitous dial coverage; and even in-flight access through Connexion by Boeing®;
- Integration of your company's wireless LANs and home broadband access connections with the iPass global virtual network;
- An award-winning user interface for Windows, Macintosh and Pocket PC devices that simplifies the overall user experience—including auto-detection and configuration for Wi-Fi, mobile data and Ethernet;
- Central management and local enforcement of connectivity and security policies—including delivery of patches before allowing corporate network access;
- An architecture with unparalleled security features that shield enterprise information from third-party network providers, protect authentication requests across the Internet and leverage an IT department's existing authentication infrastructure;
- Solutions designed for simple service rollout and streamlined management to lower your total cost of ownership.



GET CONNECTIONS WHEN AND WHERE

YOU NEED THEM

Putting mobility to work for you is about where users can get access and, how reliable those connections are. Used by hundreds of Global 2,000 companies, the iPass Mobile Office service delivers unparalleled availability across more than 60,000 Ethernet and Wi-Fi access points, including T-Mobile® HotSpot locations in the U.S. and Europe. Users can connect through mobile data services, ubiquitous dial-up coverage and other access types that are part of the iPass network as well as non-iPass networks, including corporate wireless LANs, public hotspots and personal WLANs.

Not only does iPass provide the most extensive global network, iPass has put capabilities in place to ensure that your users get quality connections. All iPass access-provider partners are certified Enterprise Ready to ensure service availability and interoperability with leading enterprise security systems. iPass' patented Service Quality Management system directs user connections to the best-performing access points, providing an incentive for our providers to continually improve their reliability when serving iPass customers. Finally, iPass protects against outages by using multiple access providers in thousands of cities around the world.

SIMPLIFY YOUR MOBILE WORKERS' EXPERIENCE

Across multiple connection technologies and locations, the award-winning iPassConnect™ universal client offers mobile users a unified and consistent login experience. Available broadband networks including Wi-Fi, mobile data and Ethernet, are automatically presented to the user for quick, easy access. A drop-down location listing shows users all local connections such as dial-up, ISDN, PHS, Wi-Fi, Ethernet and GSM. With one click, they're connected.

In addition, the client can be configured to integrate numerous functions into the connection process. Examples include connection directory update, VPN auto-connect, token-based authentication, Windows pre-logon functions, endpoint policy compliance and more. Automatic detection of broadband networks and zero-configuration for wireless network cards make wireless as easy to use as dial. These features create a more seamless user connection experience, reducing your end-user support costs.

ENJOY END-TO-END PROTECTION

As remote and mobile connectivity evolves from simple dial-up access to include a multitude of access technologies, the iPass

Mobile Office service helps protect your corporate network from new security threats. iPass does this not only by applying unique protection to the authentication process, but also by ensuring that end users comply with your security policies before and throughout each network session.

Key security elements of iPass Mobile Office include:

- An authentication process that creates a single trust relationship between the customer and iPass; all sensitive "enterprise secrets" are kept from third party access-provider partners
- Use of digital certificates and SSL tunnels for all communications across the iPass network, from the provider to the enterprise
- Additional password encryption from the client device, through the access provider and into the iPass network core
- Support for emerging Wi-Fi security standards such as 802.1x, EAP-TLS, PEAP-TLS and WPA2
- Enforcement of connectivity and security policies before allowing corporate connectivity

POLICY-BASED CONTROL

The iPass network architecture is uniquely designed to help you implement and manage policies that define the conditions under which users get access to the corporate network. The Mobile Office service allows you to configure and manage policies based on your unique requirements through the secure iPass Portal. Your policies are then distributed to endpoint devices during the iPass authentication process and enforced both before and during each user session.

With this service you can implement a wide range of access control policies based on access method (e.g. dial, Wi-Fi hotspots), access provider, access point location and time of day. You can also limit the session length and set idle timeouts to avoid costly sessions.

Finally, you can require that users follow specific policies regarding endpoint security software, including use, proper configuration, and specific version of VPN, personal firewall and anti-virus software, as well as operating system security patches. You can even configure the service to force a user into compliance—all before they are allowed access to the corporate network.

SAY GOODBYE TO BILLING COMPLEXITY

Dealing with multiple access providers and technologies can make billing complex and confusing. In addition, mobile con-

nectivity costs can become buried in traveling users' hotel bills, resulting in "black budget" expenses that may not impact IT directly, but do inflate your company's overall spending on broadband access. iPass simplifies the process by providing a single bill and connection detail records for all enterprise wired and wireless broadband, dial-up, ISDN and PHS services no matter where or how often users connect. Our industry-leading clearinghouse and billing system can provide daily or monthly records, usage summary reports, and even be set up to directly charge end users' corporate credit cards.

Add the Mobile Data Service option to iPass Mobile Office and further simplify your billing by getting one consolidated invoice for use of EV-DO and 1xRTT CDMA networks in the U.S. along with all other access types. With iPass as the sole provider for all remote connectivity, including mobile data services, IT departments gain the advantage of being able to track expenses and control costs more easily through one bill.

ROLLOUT SERVICE QUICKLY

iPass Mobile Office service is designed to help you get up and running without excessive drain on your staff. Equally important, no new infrastructure is required, as iPass interoperates with leading AAA and enterprise security systems, allowing you to leverage your significant investment in best-in-class solutions.

Service deployment is composed of three major steps:

1. Install iPass' RoamServer™ software behind your corporate firewall to get SSL-protected communications between iPass Transaction Centers and your network. The RoamServer software enforces policies and translates between the iPass protocol and your existing AAA database, whether it's based on RADIUS, TACACS+, LDAP, NT Domains or Unix password files.
2. Use the iPass Portal to create your custom user policy profiles, which will be enforced for each connection.
3. Use our software distribution tools to automatically deploy the iPassConnect universal client across your user base.

Now you're ready to activate Mobile Office.

For larger deployments involving complex technical operating environments, iPass offers a broad array of implementation services to assist with planning, customization, integration, installation and service activation. This ensures a smoother rollout, shorter deployment cycle and faster investment pay back.

THE iPASS MOBILE OFFICE SERVICE INCLUDES THESE FEATURES:

- **Universal Connections** provide access to any Internet connection, including those that are not part of the iPass global virtual network, such as home DSL, public hotspots, personal wireless LANs, your corporate wireless LAN and mobile data networks.
- **intelligent Online Quality (iOQ)** delivers detailed reports on actual end-user experiences in order to facilitate troubleshooting and proactively address user connectivity issues.
- **Encrypted Login** uses public-key cryptography to protect passwords from the client all the way to the corporate server over wired and Wi-Fi links.
- **Training for Users and Helps Desks** enables your company to get up and running quickly through online tutorials and live training sessions.

OPTIONAL SERVICES CAN BE ADDED TO MOBILE OFFICE AT ADDITIONAL COST:

- **Hosted Authentication** provides a managed option for enterprises that would rather have iPass host their authentication database.
- **Fixed Broadband Services** extend always-on broadband IP VPN to employees in home offices, branch offices and retail locations.
- **Endpoint Policy Management™ Service** enables enterprises to proactively manage remote and mobile devices wherever they are, through automated inventory, assessment, remediation and patching.
- **DeviceID™ Service** establishes which endpoints are trustworthy through a unique device identification process and ensures that only corporate-authorized machines access the network.
- **Universal Policy Enforcement** combines iPassConnect with the DeviceID and Endpoint Policy Management services from iPass to force endpoint policy checks and corrective action over any Internet connection before allowing a VPN session.
- **Customized iPass Training** helps get your help desk staff up to speed quickly to support iPass services, and provides custom training tools for end users to accelerate deployment.



STREAMLINE MAINTENANCE AND MANAGEMENT

Once the service is running, standard management functions are a breeze. Here's why:

- Since the service uses your existing AAA database, any changes made there are immediately enacted on the iPass service as well.
- You can take advantage of the simple and secure iPass Portal as your single Web-based source for a wealth of information and management functions—including billing, policy management, usage and service quality reporting, customer care, and training.
- Updates to the iPassConnect universal client, configuration files, and connection directory are designed to automatically "push" to your clients, based on your centrally managed corporate policies.

- iPass Customer Care help desks around the globe monitor the iPass network 24x7, proactively testing connections, troubleshooting issues and providing support to your IT staff.

LEARN MORE

Discover why well over 1,000 corporations around the world—including General Motors, HSBC and Sony—have standardized on iPass Mobile Office service. 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.

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

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

www.ipass.com

