

Wireless LAN Roaming

Integrate Your Corporate Wi-Fi LANs into iPass® Corporate Access™

- Create and manage a custom network integrating on-site Wi-Fi networks with the iPass Corporate Access service
- Provide a simplified user experience for all remote and local Wi-Fi connections
- Extend centralized management, coverage, security policies and ease-of-use to private wireless LANs operated by the enterprise
- Protect corporate resources through secure connectivity across public, corporate and home networks

Leverage Secure Connectivity Across Multiple Networks

Wireless LAN Roaming is a valuable add-on option to the iPass Corporate Access service. Now your enterprise IT department can easily offer a single user experience for all remote and local wireless connections while extending centralized management of security policies to the most vulnerable piece of the office-networking environment. Your mobile users and IT department gain tremendous productivity benefits by leveraging a unified solution of secure connectivity across public, corporate and home networks.

This single user experience is based on the award-winning iPassConnect™ service interface, which lets users access the corporate network from public dial, ISDN, PHS, wired and Wi-Fi hotspots, home broadband connections, and now from Wi-Fi access points within the corporation. Your users run the same iPassConnect service interface they are accustomed to using while on the road or at home, and enjoy the same zero-configuration benefits (on XP Professional & Home Editions, 2000, ME and Windows 98 Second Edition).

Protect Your Corporate Resources

If you're responsible for network security, the benefits of iPass policy-based connectivity extend to the wireless LAN as well. These benefits include access point authentication, end-to-end protection of user credentials and the ability to create, modify and enforce fine-grained security policies before users are allowed access to corporate resources.

Your IT department benefits from in-depth session statistics on office Wi-Fi networks via iPass intelligent Online Quality (iOQ™). Plus, you can deploy this service with confidence knowing that it is designed to support both today's and tomorrow's WLAN authentication standards.

Ensure a Consistent User Experience

Extending the simple user experience to corporate wireless LANs lowers end-user support costs and boosts satisfaction. Only Wi-Fi corporate access points that you approve are detected and presented to users. Rogue access points are suppressed and remain invisible to the user. Users simply select the access point, enter credentials and the iPassConnect service interface does the rest, such as configuring the Wi-Fi adapter, enforcing IT policies, auto-launching security clients and launching the VPN.

Mobile workers utilize the same credentials as for all other iPass access. And since the iPassConnect interface uses NDIS 5.1-compliant drivers, Wireless LAN Roaming works with most popular Wi-Fi cards. As

users roam from home to office to hotspots, there's no need to configure the software or Wi-Fi card settings such as SSIDs, security settings, or WEP keys.

Gain Policy Management Over Your Corporate WLAN

Wireless LAN Roaming lets IT administrators centrally manage and enforce all remote-access policies and all personal firewall, anti-virus and VPN capabilities, ensuring that all campus Wi-Fi network users are secured. The service also interoperates with the Endpoint Policy Management™ service to inspect and patch non-complaint security software before allowing a connection. Operating system patches, anti-virus definition files and other important security updates can be pushed to end-user computers, further securing the corporate network.

Achieve Secure Authentication Over Wi-Fi

Wireless LAN Roaming supports a variety of authentication types to make the connection attempt secure, even though users enter a simple username and password. Wi-Fi authentication support includes GIS and IEEE 802.1x. and integrates with your existing AAA. GIS is a de facto standard used by many leading wireless access gateways for digital certificate exchange and SSL tunneling of credentials. IEEE 802.1x standard is a device authentication standard which secures both authentication and traffic that is part of the Wi-Fi Alliance's Wireless Protected Access (WPA) specification and will soon be incorporated into the IEEE 802.11i WLAN security standard.

Have it your way! The Wireless LAN Roaming service is flexible and can handle the various ways you may want to configure your wireless LAN infrastructure, including:

- SSID and WEP
- Broadcast or Non-broadcast SSIDs
- Generic Interface Specification (GIS)
- 802.1x

Simplify Deployment

Wireless LAN Roaming simplifies deployment because it supports the leading wireless network adapters and access points, as well as best-of-breed enterprise security solutions already in place. And since Wireless LAN Roaming is integrated with the iPassConnect service interface, it can be delivered to existing iPass customers with a simple configuration or customization change, a software push, to the supporting connection directory to add approved corporate Wi-Fi access points. IT administrators can also mask network changes or changes in authentication methods from end users.

Reap the Productivity Benefits

As a valuable add-on to iPass Corporate Access, the Wireless LAN Roaming service can help your organization leverage a unified solution of secure connectivity across public, corporate and home networks and reap the benefits of increased productivity from corporate and mobile workers. For more information, visit www.ipass.com or talk to your iPass account manager today.

Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065 United States
Tel: +1 650.232.4100 Fax: +1 650.232.4111
www.ipass.com

