

On-Campus Roaming

Integrate Your Corporate Wireless LANs Into Your iPass® Service

- Give mobile users secure, effortless Wi-Fi connectivity across public and private corporate wireless networks
- Enable zero-configuration Wi-Fi for a simplified user experience on-campus and remote
- Centrally enforce your security policies across your local wireless LANs — before allowing access



Wi-Fi connectivity helps keep employees in touch—across the corporate campus and around the world. The problem has been that, until now, workers have had to use one connection interface on campus and a different one (or two or three) when accessing public Wi-Fi hotspots. This has led to user confusion, misconfigurations, more calls to the help desk, lower productivity and ultimately higher costs.

LEVERAGE SECURE CONNECTIVITY ACROSS MULTIPLE NETWORKS

iPass solves these problems with On-Campus Roaming, a valuable component of the iPass Mobile Office service, which integrates your corporate wireless LAN with your iPass connectivity solution. Now you can easily offer a single user experience for all local and remote 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.

SINGLE CONNECTION EXPERIENCE

With On-Campus Roaming, users enjoy a single, consistent connection experience across all access types—whether they're connecting from an office in the next building or a sidewalk café across town. They also enjoy zero-configuration Wi-Fi, meaning they don't have to reconfigure their system for different SSIDs or security settings as they move across different Wi-Fi networks. This single user experience is based on the award-winning iPassConnect™ universal client, which lets users connect

to Wi-Fi access points within your corporation in the same way they access public hotspots and other connection types while on the road or at home.

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.

You gain in-depth session statistics on office Wi-Fi networks through intelligent Online Quality (iOQ®). This component of Mobile Office provides detailed reports to facilitate troubleshooting, improve customer service and proactively address many user connectivity issues. 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 iPassConnect 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 iPassConnect uses NDIS 5.1-compliant drivers, On-Campus 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

The On-Campus Roaming service 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 and anti-virus definition files can be pushed to end-user computers, further securing the corporate network.

HAVE IT YOUR WAY!

The On-Campus Wi-Fi service is flexible and can handle the various ways you may want to configure your wireless LAN infrastructure, including:

- WPA1 and WPA2 with TKIP and AES pre-shared keys
- SSID and WEP
- Broadcast or Non-broadcast SSIDs
- Generic Interface Specification (GIS)
- 802.1x (EAP-TLS, PEAP-TLS, TTLS)

ACHIEVE SECURE AUTHENTICATION OVER WI-FI

On-Campus 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 data. Support for EAP-TLS and PEAP-TLS provide new 802.1x options for enterprise-grade certificate-based authentication with a simple user interface.

SIMPLIFY DEPLOYMENT

On-Campus 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 On-Campus Roaming is integrated with iPassConnect, it can be delivered to existing iPass customers with a simple configuration or customization change 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 built-in component of the iPass Mobile Office service, On-Campus Roaming can help your organization leverage a unified solution of secure connectivity across public, corporate and home networks. For more information, visit www.ipass.com or talk to your iPass account manager today. ■

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

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

www.ipass.com

