

Wireless LAN Roaming

Integrieren Sie Ihre unternehmensinternen Wi-Fi-Netze in iPass® Corporate Access™

- Integrieren sie Ihre unternehmensinternen Wi-Fi-Netze in Ihren kundenspezifischen iPass Corporate Access Service
- Ermöglichen sie Ihren Nutzern einfachsten Verbindungsaufbau über verschiedenste unternehmensinterne und externe Netzzugänge hinweg
- Integrieren sie Ihre unternehmensinternen WiFi Zugänge in das zentrale Management unter Beibehaltung der Sicherheitsrichtlinien- und das bei einfachster Handhabung
- Schützen sie Ihre Unternehmensdaten durch sicheren Verbindungsaufbau, sei es vom öffentlichen, privaten oder Firmennetz aus.

Nutzen Sie sichere Verbindungen über alle verfügbaren Netze hinweg

WLAN Roaming ist eine optionale, jedoch sehr effiziente Ergänzung Ihres iPass Corporate Access Services. Es ermöglicht Ihrer IT Abteilung, das zentralisierte Management der unternehmensinternen Sicherheitsrichtlinien auf die anfälligste „Komponente“ des Netzes auszudehnen – den mobilen Mitarbeiter. Sowohl die IT Abteilung als auch Ihre reisenden Mitarbeiter profitieren von der vereinheitlichten Lösung des Zugangs zum Firmennetz, egal ob diese Verbindung aus dem öffentlichen, einem privaten oder dem Firmennetz aufgebaut wird.

Die Lösung basiert auf dem Einsatz des mit verschiedensten Auszeichnungen bedachten iPassConnect™ Client, der es den Nutzern ermöglicht, eine sichere Verbindung zum Firmennetz aufzubauen, ob er sich von einem öffentlichen Einwahlknoten aus, über PHS, über Breitbandverbindungen oder öffentliche oder private WiFi Hotspots einwählt. Ohne weitere Parameter konfigurieren zu müssen, können Ihre Nutzer mit dem gleichen Client arbeiten, den sie von Zuhause aus oder von unterwegs bereits gewohnt sind. (Die iPass Software unterstützt die Betriebssysteme XP Professional, Home Edition, 2000, ME sowie Windows 98 Second Edition)

Schützen Sie Ihre Unternehmensdaten

Die Vorteile einer auf iPass basierenden Lösung gelten in punkto Netzsicherheit auch für die Wi-Fi-Netze. Zu diesen Vorteilen gehören die Authentifizierung von Zugangspunkten, ein „End-to-End-Schutz“ der Nutzerzugangsdaten und die Möglichkeit, firmenspezifische Sicherheitsregeln zu erstellen, diese zu ändern und durchzusetzen, bevor die Nutzer auf die Unternehmensdaten zugreifen dürfen.

Ihre IT-Abteilung profitiert durch „iPass Intelligent Online Quality“ (iOQ™) von umfassenden Statistiken über Sitzungen zu den unternehmenseigenen Wi-Fi-Netzen. Außerdem können Sie diesen Service mit dem Wissen implementieren, dass er sowohl die WLAN-Authentifizierungsstandards von heute als auch die von morgen unterstützt.

Sorgen Sie für ein einheitliches Nutzerszenario

Die einfachere Nutzung des Wi-Fi-Netzes im Unternehmen senkt die Kosten für die Endnutzer-Betreuung und sorgt für eine höhere Zufriedenheit. Den Nutzern werden ausschließlich Wi-Fi-Zugangspunkte bereitgestellt, die von der IT Abteilung genehmigt wurden. Nicht vertrauensvolle Zugangspunkte werden unterdrückt und bleiben für den Nutzer unsichtbar. Der Nutzer wählt einfach den Zugangspunkt aus und gibt seine Zugangsdaten ein – den Rest, z. B. das Konfigurieren des Wi-Fi-Adapters, das Durchsetzen von IT-Regeln, das automatische Starten von Sicherheits-Clients und das Starten des VPN, erledigt die iPassConnect-Service Interface.



Mobile Mitarbeiter nutzen stets die gleichen iPass Zugangsdaten. Und weil die iPassConnect-Nutzeroberfläche NDIS 5.1-konforme Treiber verwendet, funktioniert Wireless LAN Roaming mit den meisten gängigen Wi-Fi-Karten. Beim Roaming zwischen Zuhause, Büro und Hotspots ist es nicht erforderlich, die Software- oder Wi-Fi-Karteneinstellungen, z. B. SSIDs, Sicherheitseinstellungen oder WEP-Schlüssel, zu konfigurieren.

Regelverwaltung über das WLAN Ihres Unternehmens

Mit Wireless LAN Roaming können IT-Administratoren alle Regeln für den Remote-Zugriff sowie alle Funktionen für Personal Firewall, Virenschutz und VPN zentral verwalten, durchsetzen und somit sicherstellen, dass alle Nutzer des firmeneigenen Wi-Fi-Netztes gesichert sind. Der Service arbeitet auch mit dem Endpoint Policy Management™-Service zusammen, um nicht-konforme Sicherheits-Software zu prüfen und zu korrigieren, bevor eine Verbindung hergestellt wird. Patches für das Betriebssystem, Anti-Viren-Definitionsdateien und andere wichtige Sicherheits-Updates können zum zusätzlichen Schutz des Unternehmensnetzes auf die Computer der Endnutzer aufgespielt werden.

Konfigurieren Sie frei gemäß Ihren Anforderungen. Wireless LAN Roaming ist flexibel und unterstützt die verschiedensten Konfigurationen Ihrer Wireless-LAN-Infrastruktur. Dazu gehören:

- SSID und WEP
- Broadcast- oder Non-Broadcast-SSIDs
- GIS (Generic Interface Specification)
- 802.1x

Ermöglichen Sie eine sichere Authentifizierung über Wi-Fi

Wireless LAN Roaming unterstützt zahlreiche Authentifizierungstypen, um einen Verbindungsversuch selbst dann sicher zu gestalten, wenn sich der Nutzer mit einem einfachen Username und Passwort einloggt. Die Wi-Fi-Authentifizierung unterstützt unter anderem GIS und IEEE 802.1x und kann in Ihr bestehendes AAA integriert werden. GIS ist ein De-facto-Standard, der von vielen führenden Access Gateways für den Austausch digitaler Zertifikate und das SSL-Tunneling von Zugangsdaten verwendet wird. IEEE 802.1x ist ein Standard zur Geräteauthentifizierung, der sowohl die Authentifizierung als auch den Datenverkehr sichert. Dieser Standard ist Teil der WPA-Spezifikation (Wireless Protected Access) der Wi-Fi Alliance (WPA) und wird in Kürze in den WLAN-Sicherheitsstandard IEEE 802.11i integriert.

Vereinfachen Sie die Implementierung

Wireless LAN Roaming sorgt für eine einfachere Implementierung, weil es neben den gängigen drahtlosen Netzadaptern und Zugangspunkten auch die bereits eingesetzten, führenden Sicherheitslösungen für Unternehmen unterstützt. Und weil Wireless LAN Roaming in die iPassConnect-Service Interface integriert ist, können freigegebene firmeneigene Wi-Fi-Zugangspunkte bestehenden iPass-Kunden mit einer einfachen Konfiguration oder über eine Anpassungsänderung (sog. Software-Push) im jeweiligen Verbindungsverzeichnis zur Verfügung gestellt werden. IT-Administratoren haben außerdem die Möglichkeit, Änderungen am Netz oder an den Authentifizierungsmethoden vor dem Endnutzer zu verbergen.

Profitieren Sie von den Produktivitätsvorteilen

Als wertvolle „Add-On-Option“ zu iPass Corporate Access unterstützt Wireless LAN Roaming Ihr Unternehmen bei der Nutzung einer einheitlichen und sicheren Verbindungslösung über verschiedenste unternehmensinterne und externe Netzzugänge hinweg. Somit profitieren Sie von der höheren Produktivität Ihrer mobilen und direkt am Firmensitz tätigen Mitarbeiter. Weitere Informationen erhalten Sie unter www.ipass.com – oder sprechen Sie noch heute mit Ihrem iPass Betreuer!

*iPass EMEA
Region D/A/CH
Wiener Platz 7
D-81667 München
Germany
www.ipass.de*

