

A grayscale image of a globe with a white grid overlay, showing the continents of North and South America. A solid red vertical bar is on the left side of the image.

iPass® Wireless LAN Roaming - Technisches Referenzhandbuch

Version: 1.0, 05.07.2004

Hauptsitz des Unternehmens

iPass Inc.

3800 Bridge Parkway


Redwood Shores, CA 94065 USA

<http://www.ipass.com>

Tel: +1 650.232.4100

Fax: +1 650.232.0227

iPass® Wireless LAN Roaming – Technisches Referenzhandbuch	4
Übersicht	4
<hr/>	
Vorteile.....	4
iPass Wireless LAN Roaming-Service-Optionen.....	5
Universelle Servicekomponenten:	5
Erweiterte Servicekomponenten:.....	5
Überlegungen zum Netz	6
Positionierung der Zugangsknoten:	6
SSID: aktiv oder passiv (gesendet/nicht gesendet)	6
Verbindung zum Zugangsknoten: Methoden.....	6
Optionen zur Nutzerauthentifizierung (Advanced Service)	7
Richtlinien für den Support.....	7
Beschreibungen der Service-Optionen	7
<hr/>	
Option 1: Wireless LAN Roaming Basic	8
So funktioniert's	8
Einzigartige Funktionen	9
Empfohlene Architektur gemäß Best Practices:.....	9
Konfigurationseinstellungen:	9
Kundeneigener Telefonbucheintrag	9
Option 2: iPass Wireless LAN Roaming Advanced mit GIS-Authentifizierung.....	10
So funktioniert's	10
Zusätzliche Servicekomponenten:.....	11
Einzigartige Funktionen	11
Empfohlene Architektur gemäß Best Practices:.....	11
Konfigurationseinstellungen:	11
Kundeneigener Telefonbucheintrag	11
Routing der Nutzererkennung	12
Option 3: iPass Wireless LAN Roaming Advanced mit 802.1x-Authentifizierung	13



INHALTSVERZEICHNIS

So funktioniert's	13
Zusätzliche Servicekomponenten:.....	14
Einzigartige Funktionen	14
Empfohlene Architektur gemäß Best Practices:.....	14
Konfigurationseinstellungen:	14
Festlegen der 802.1x-Authentifizierungsmethode	14
Zertifikatsvalidierung für 802.1x mit TTLS:	15
Routing der Nutzerkennung	15
Standardmethoden für die 802.1x-Authentifizierung:	15
Methoden für die getunnelte 802.1x-Authentifizierung:	15
Weitere Informationen	16
iOQ/SQM-Daten	16
Schlussfolgerung	16
Informationen zu iPass	17

iPass® Wireless LAN Roaming – Technisches Referenzhandbuch

Übersicht

WLAN Roaming ist eine optionale, jedoch sehr effiziente Ergänzung der iPass® Corporate Access™ - Services. Es ermöglicht Ihrer IT-Abteilung, die zentralisierte Verwaltung der Sicherheitsrichtlinien auf das schwächste Glied des Netzes auszudehnen – den mobilen Mitarbeiter. Sowohl die IT-Abteilung als auch die mobilen Nutzer profitieren von der einheitlichen Lösung für den sicheren Zugang zum Firmennetz, egal ob Sie die Verbindung aus dem öffentlichen, einem privaten oder dem firmeninternen Netz aufgebaut wird.

Die Lösung basiert auf dem mehrfach preisgekrönten iPassConnect™ Client, der es den Nutzern ermöglicht, eine sichere Verbindung zum Firmennetz aufzubauen, ob er sich von einem öffentlichen Zugangsknoten aus, über ISDN, PHS, Festnetz, über Breitbandverbindungen oder über öffentliche oder private WiFi-Hotspots einwählt. Ohne weitere Parameter konfigurieren zu müssen, können Ihre Nutzer mit dem gleichen Client arbeiten (von Windows 98 bis XP), den sie von unterwegs oder von zu Hause aus bereits gewohnt sind.

Vorteile

Die Vorteile von Wireless LAN Roaming ergänzen viele der anderen Vorteile der iPass-Services. Mit diesem Service können Sie:

- ein nutzerdefiniertes Netz erstellen und verwalten, das WiFi-Netze vor Ort in den iPass® - Service integriert.
- firmeneigene Daten durch sichere Verbindungen über alle Netze hinweg (öffentliche, firmeninterne und private) schützen.
- den Nutzern die Bedienung erleichtern, indem Sie eine einheitliche Oberfläche für sämtliche WiFi-Verbindungen (private wie öffentliche) bereitstellen:
 - Automatische Erkennung von Wireless-Netzen (beim Senden der SSID)
 - Gleicher Nutzernamen und gleiches Passwort
 - Ähnlichkeit zu allen anderen WiFi-Verbindungen
 - Keine manuelle Änderung der Client-Konfiguration nötig
- die zentralisierte Verwaltung, Netzabdeckung, Sicherheitsrichtlinien und Nutzerfreundlichkeit auf private, vom Unternehmen betriebene LANs ausdehnen:
 - Es gibt nur eine Authentifizierungsdatenbank für alle iPass-Nutzer (in der Advanced-Option).
 - Richtlinien wie VPN-Start & Auto-Teardown, PFW-Integration, AV-Integration können erzwungen werden.
 - Die Schulung von Nutzern und die Notwendigkeit eines HelpDesk für eine andere Lösung entfällt.
 - Es muss kein weiterer Client für den internen Zugriff bereitgestellt werden.
 - Die Auslastung lokaler WiFi-Netze kann über iPass Intelligent Online Quality (iOQ®) überwacht werden.

iPass Wireless LAN Roaming-Service-Optionen

Da die Netzwerkumgebungen und die Sicherheitsanforderungen je nach Kundenanforderungen variieren, bieten wir den iPass Wireless LAN Roaming-Service in verschiedenen Varianten an. Dazu gehören die Folgenden:

- Wireless LAN Roaming Basic (keine Authentifizierung):
 - Offenes Netz
 - WEP (Pre-Shared Key)
- Wireless LAN Roaming Advanced (mit Authentifizierung):
 - GIS-Authentifizierung
 - 802.1x-Authentifizierung

HINWEIS: Diese Optionen schließen sich nicht gegenseitig aus. Kunden können sich dafür entscheiden, verschiedene Konfigurationen für verschiedene Teile ihres Wireless-Netzes zu verwenden. So können Kunden, die an einem Standort bereits 801.1x implementiert haben, an anderen Standorten jedoch noch nicht, für diese anderen Standorte beispielsweise WEP-Schlüssel oder GIS-Lösungen einsetzen.

Universelle Servicekomponenten:

Folgende Serviceoptionen sind in allen Wireless LAN Roaming-Servicekomponenten enthalten:

- Netzwerk:
 - Kundeneigene IEEE 802.11b-Zugangsknoten (WiFi) mit gesendeter oder verborgener SSID (Service Set Identifier)
 - 40-Bit- oder 128-Bit-WEP (Wired Equivalent Privacy) – (optional)
 - Integration vorhandene VPN-Lösung des Kunden zur Sicherstellung der Kommunikation mit dem Firmennetz – (optional)
 - iPassConnect cbook-Einträge mit folgenden Details konfiguriert:
 - Name des Standorts, Land, Bundesstaat und Stadt
 - richtiges Zugriffsverfahren (zur Verbindung mit dem Zugangsknoten)
 - richtige SSID – aktiv oder passiv
 - iOQ-Daten (Bei Bestellung des iOQ-Dienstes)
- Nutzer:
 - Betriebssystem: Windows 98SE, Windows ME, Windows 2000 oder Windows XP Home und Professional
 - IEEE 802.11b-Schnittstellenkarte (WiFi)
 - iPassConnect 3.2 oder höher

Erweiterte Servicekomponenten:

Der Wireless LAN Roaming Advanced Service ist dafür ausgelegt, mit den internen WiFi-Netzen von Kunden zusammenzuarbeiten, die folgende Merkmale aufweisen:

- GIS-Authentifizierung:
 - Kundeneigene installierte GIS-fähige IEEE 802.11b-Zugangs-Gateways
 - *HINWEIS: Eine Liste GIS-fähiger Zugangs-Gateways finden Sie im iPass Portal.*
 - Kundeneigene installierte RADIUS AAA-Server zur Nutzerauthentifizierung
- 802.1x-Authentifizierung:
 - Kundeneigene installierte 802.1x AAA-Server, die MD5, LEAP, TLS-MD5, TTLS-PAP, TTLS-CHAP, TTLS-MSCHAP oder TTLS-MSCHAPV2 zur Nutzerauthentifizierung verwenden.

Überlegungen zum Netz

Der iPass Wireless LAN Roaming-Service ermöglicht je nach den individuellen Kundenanforderungen mehrere Konfigurationen. Kunden müssen ihre Optionen in Bezug auf die Positionierung der Zugangsknoten, SSID-Sendeoptionen, Methoden zum Verbindungsaufbau mit den Zugangsknoten und zur Nutzerauthentifizierung überdenken.

Positionierung der Zugangsknoten:

Bei der Positionierung der Zugangsknoten sollten Sicherheitsrisiken und die Zugänglichkeit für Nutzer genau gegeneinander abgewogen werden.

- Einige Kunden möchten möglicherweise den Wireless-Zugangsknoten innerhalb und den Sender außerhalb des lokalen Netzes positionieren und so den Zugriff auf Unternehmensdaten für Gäste öffnen. Auf Grund der damit verbundenen Sicherheitsrisiken rät iPass von einem solchen Szenario ab, obwohl es unterstützt werden kann. In diesen Fällen muss der Kunde bestimmte Ports in der Firewall öffnen, so dass regelmäßige Telefonbuchaktualisierungen durchgeführt und SQM-Daten übertragen werden können.
- Andere Kunden erlauben möglicherweise den offenen Zugang zu einem bestimmten abgegrenzten Bereich, um auf das Internet zuzugreifen, verlangen jedoch die Verwendung eines VPN für die Verbindung mit dem firmeneigenen Intranet. In dieser Architektur würde sich der Wireless-Zugangsknoten innerhalb der DMZ befinden, der Sender jedoch außerhalb des Netzes, was mehr Sicherheit gegen bösartige Angriffe bietet.

SSID: aktiv oder passiv (gesendet/nicht gesendet)

Darüber hinaus muss der Kunde entscheiden, ob die SSID gesendet werden soll oder nicht.

- Wenn die SSID gesendet wird, können alle Nutzer in Reichweite des Zugangsknoten diesen automatisch erkennen und eine Verbindung herstellen. Der iPassConnect-Client zeigt dem Nutzer den Zugangsknoten automatisch im Feld **Verfügbare Wireless-Netze** an. Der Nutzer muss nur noch auf **Verbinden** klicken. Da jedoch kein bestimmter Verzeichniseintrag ausgewählt ist, liefert SQM keine standortspezifischen Daten.
- Wenn die SSID nicht gesendet wird (also verborgen bleibt), muss der Nutzer die SSID kennen, um das Netz erkennen und eine Verbindung herstellen zu können. Der iPassConnect-Client erkennt den Zugangsknoten nicht automatisch. Stattdessen muss der Nutzer Land, Bundesstaat (falls zutreffend) und Stadt eingeben und den entsprechenden Verzeichniseintrag auswählen. Optional kann der Nutzer den Zugangsknoten mit einem Lesezeichen versehen, um schneller darauf zugreifen zu können. In diesem Fall enthalten die SQM-Datensätze alle Daten zum verwendeten Zugangsknoten, weil der entsprechende Verzeichniseintrag ausgewählt ist.

Verbindung zum Zugangsknoten: Methoden

Der iPass Wireless LAN Roaming-Service bietet die folgenden Methoden zum Herstellen einer Verbindung zum Zugangsknoten:

- **Offener Zugang:** Bei dieser Methode greift der Client nur mit Hilfe der SSID auf das Netz zu, ein WEP-Schlüssel wird nicht verwendet. Nutzer werden zwar aufgefordert, ihre Anmeldeinformationen einzugeben, eine Authentifizierung findet jedoch nicht statt.
- **WEP/Pre-Shared Key-Modus:** Um ein offenes Netz zusätzlich zu schützen, empfiehlt iPass die Verwendung eines gemeinsamen WEP-Schlüssels. In diesem Modell wird zusätzlich zur SSID noch ein gemeinsamer WEP-Schlüssel verwendet, um dem Verbindungsaufbau eine weitere Sicherheitsebene hinzuzufügen. Wenn ein Nutzer diesen POP verwendet, stellt der Client die Verbindung zum Netz her, indem er die angegebene SSID zusammen mit dem

entsprechenden WEP-Schlüssel verwendet. Die Anmeldeinformationen des Nutzers werden nicht authentifiziert, der Client wird jedoch anhand der Kenntnis des WEP-Schlüssels validiert.

- WEP-Schlüssel und SSID werden zusammen mit den Details des kundeneigenen Hotspots übermittelt. Der WEP-Schlüssel kann 40 oder 128 Bit lang sein und im ASCII- oder Hexadezimalformat vorliegen. Aus Sicherheitsgründen wird eine 128-Bit-Verschlüsselung empfohlen.
- Sobald die Telefonbuchinformationen generiert und veröffentlicht wurden, wird der WEP-Schlüssel in der Datei `cust_pop_wep.txt` und die entsprechende SSID in der Datei `cust_pop_ssid.txt` angegeben. Um noch mehr Sicherheit zu gewährleisten, werden diese Werte mittels iPassConnect 3.2 verschlüsselt.

Optionen zur Nutzerauthentifizierung (Advanced Service)

Vielen Kunden behagt das Konzept eines offenen Netzes nicht und sie würden eine Lösung bevorzugen, bei der die Nutzer anhand der Unternehmensdatenbank authentifiziert werden, um nicht autorisierte Zugriffe zu verhindern. Diesen Kunden bietet iPass im Rahmen des Advanced Service zwei Methoden zur Nutzerauthentifizierung an.

- **GIS-Zugangs-Gateway:** Die Integration eines Zugangs-Gateways ermöglicht die Weiterleitung der Anmeldeinformationen von Nutzern an die Unternehmensdatenbank zur Authentifizierung. Auch hier kann die SSID aktiv oder passiv sein (gesendet werden oder nicht) und auf Wunsch ein WEP-Schlüssel verwendet werden. Kunden können ein beliebiges, von iPass als GIS-fähig zertifiziertes Zugangs-Gateway verwenden.
- **802.1x-Authentifizierung:** Kunden, die sich für Ihr Firmennetz bereits für eine 802.1x-Lösung entschieden haben, können dies in den iPassConnect-Client integrieren. Wie bei der Lösung mit dem Zugangs-Gateway werden die Anmeldeinformationen der Nutzer authentifiziert und auf Wunsch kann auch ein WEP-Schlüssel einbezogen werden.

Weitere Informationen zu Implementierung und Betrieb eines privaten Wireless-Netzes finden Sie im *iPass@Security Best Practices Guide*.

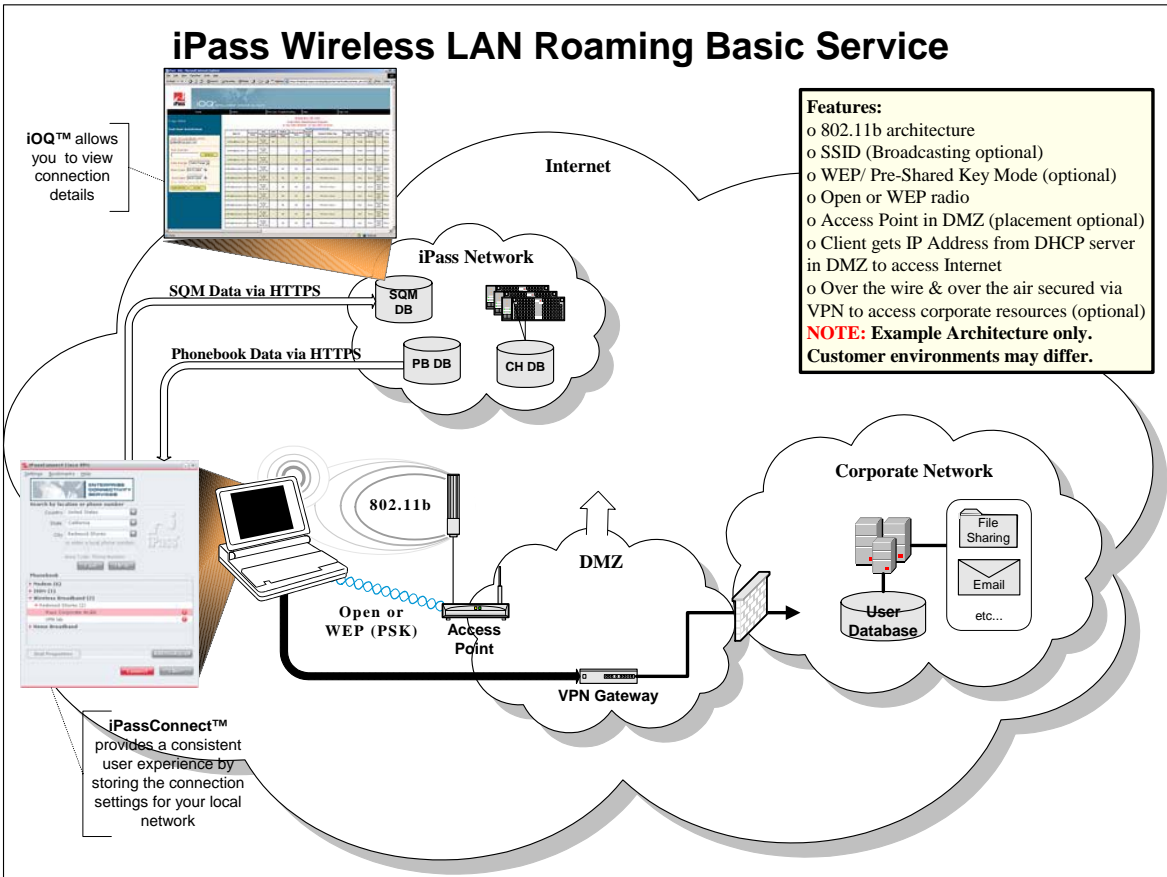
Richtlinien für den Support

Da die Netzumgebungen und Unternehmensanforderungen sehr unterschiedlich sind, sind die Kunden von Wireless LAN Roaming für die Installation und den Betrieb ihrer Netzkomponenten selbst verantwortlich. iPass unterstützt die iPass-spezifischen Komponenten des Wireless LAN Roaming-Service, einschließlich der Integration der Wireless-Zugangsknoten des Kunden mit dem iPassConnect Service Interface. Um eine problemlose Bereitstellung zu garantieren, geht iPass davon aus, dass der Kunde vor der Integration des iPass-Service sein Wireless-Netz sachgemäß eingerichtet und auf sein ordnungsgemäßes Funktionieren getestet hat.

Beschreibungen der Service-Optionen

Im Folgenden finden Sie eine detaillierte Beschreibung und Musterbeispiele für jede angebotene Option von Wireless LAN Roaming.

Option 1: Wireless LAN Roaming Basic



So funktioniert's

- Der Nutzer startet den iPassConnect-Client:
 - Wenn die SSID gesendet wird, erkennt iPassConnect anhand des Eintrags im kundeneigenen Telefonbuch (cbook) automatisch alle WiFi-Zugangsknoten, die zum Wireless LAN Roaming gehören, und stellt diese genau wie iPass WiFi-Hotspots dar.
 - Wenn die SSID nicht gesendet wird, gibt der Nutzer Land, Bundesstaat und Stadt des Unternehmensstandortes ein. Der Unternehmensstandort wird dem Nutzer zusammen mit anderen iPass WiFi-Hotspots als ein Wireless-Standort zur Auswahl angezeigt. Wie jeden anderen Telefonbucheintrag auch, kann der Nutzer den Unternehmensstandort im Client mit einem Lesezeichen versehen, um ihn künftig schneller auswählen zu können.
 - Der Nutzer klickt auf **Verbinden**. Wenn ein VPN konfiguriert ist, kann der Nutzer aufgefordert werden (optional), seine VPN-Anmeldeinformationen einzugeben.
- Der iPassConnect-Client verwendet SSID, WEP-Schlüssel (falls verwendet) und das NONE.1-Zugriffsverfahren aus dem cbook-Eintrag, um sich beim Zugangsknoten anzumelden. Dank dieses Verfahrens funktioniert der cbook-Eintrag in jeder Beziehung wie jeder andere Telefonbucheintrag, jedoch mit einem großen Unterschied: die Anmeldeinformationen des Nutzers werden nicht authentifiziert.
- Der Zugangsknoten erhält von einem DHCP-Server (entweder innerhalb der DMZ oder des Unternehmensnetzes) eine IP-Adresse und gibt diese an den iPassConnect-Client weiter, damit dieser auf das Internet zugreifen kann. (Über

diese Internetverbindung können das Telefonbuch und/oder Softwareupdates hochgeladen bzw. SQM-Daten übertragen werden.)

4. Wenn ein VPN konfiguriert ist, startet iPassConnect den VPN-Client. Die Zugriffsanforderung wird dann an den AAA-Server oder die Nutzerdatenbank im Unternehmensnetz weitergeleitet, damit die Anmeldeinformationen des Nutzers autorisiert werden. Nach erfolgreicher Autorisierung liefert das VPN eine IP-Adresse an das Unternehmensnetz, um die Funkkommunikation zu sichern.

HINWEIS: Bei Verwendung der Basic-Version des Service werden die Nutzerkennungen weder übertragen noch authentifiziert (außer VPN-Anmeldeinformationen, falls verwendet). iPassConnect dient hier nur dazu, den WiFi-Adapter zu konfigurieren und die Verbindung zwischen Nutzer und Zugangsknoten herzustellen.

Einzigartige Funktionen

- Der Verbindungsaufbau erfolgt ähnlich wie bei jeder anderen WiFi-Verbindung.
- Zum Verbindungsaufbau mit dem Wireless-Netz werden die Anmeldeinformationen von Nutzern nicht authentifiziert, genau wie bei Home Broadband. Der IT-Administrator kann jedoch festlegen, wer den Standort "sieht", und die iOQ-Daten sind umfangreicher.

Empfohlene Architektur gemäß Best Practices:

- Passive (nicht gesendete) SSID
- Aktivierter WEP/Pre-Shared Key-Modus mit 128-Bit-Verschlüsselung
- Zugangsknoten innerhalb der DMZ
- VPN-Verbindung für Zugriff auf Unternehmensdaten erforderlich

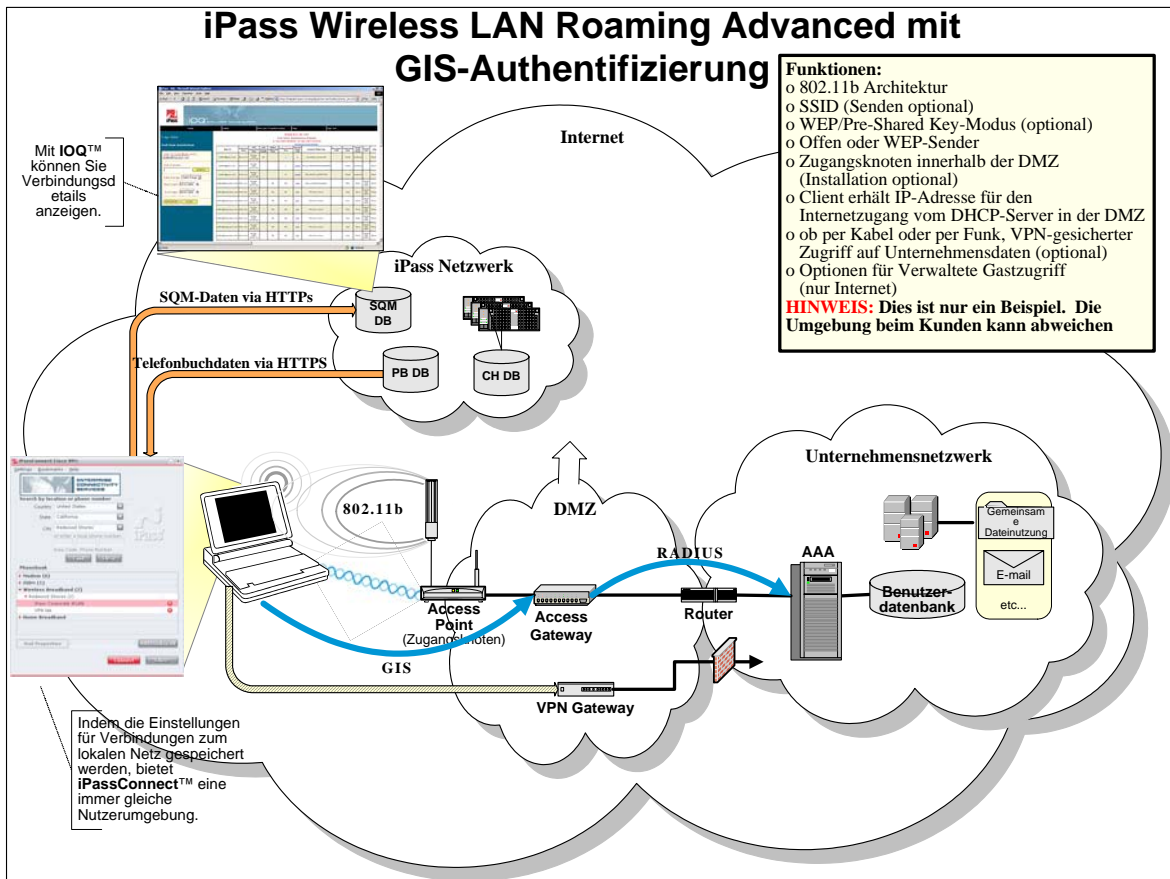
Konfigurationseinstellungen:

Kundeneigener Telefonbucheintrag

Die einzige, zur Implementierung dieser Lösung erforderliche Konfigurationseinstellung ist der kundeneigene Telefonbucheintrag (cbook) mit der richtigen SSID, dem WEP-Schlüssel (falls WEP verwendet wird) und dem NONE.1-Zugriffsverfahren. Dieses Zugriffsverfahren veranlasst den iPassConnect-Client, die Datei `ap_non_1.dll` für die Verbindung zu verwenden. Der Client versucht nicht, den Nutzer im Kundennetz zu authentifizieren, sondern startet die für das Clientprofil konfigurierten Aktionen nach Verbindung (wie VPN, persönliche Firewall und/oder Anti-Viren-Programm). Dadurch verhält sich der Client ähnlich wie eine Home Broadband-Verbindung.

Anweisungen zum Erstellen der vom kundeneigenen Telefonbuch (cbook) übermittelten Daten finden Sie im Dokument *iPass® Customer Tech Note: Creating a Customer Access Point List (Cbook)*. Das Dokument finden Sie im Portal unter **Tech Info > Documentation > Tech Notes**.

Option 2: iPass Wireless LAN Roaming Advanced mit GIS-Authentifizierung



So funktioniert's

1. Der Nutzer startet den iPassConnect-Client:
 - a. Wenn die SSID gesendet wird, erkennt iPassConnect anhand des Eintrags im kundeneigenen Telefonbuch (cbook) automatisch alle WiFi-Zugangsknoten, die zum Wireless LAN Roaming gehören, und stellt diese genau wie iPass WiFi-Hotspots dar.
 - b. Wenn die SSID nicht gesendet wird, gibt der Nutzer Land, Bundesstaat und Stadt des Unternehmensstandortes ein. Der Unternehmensstandort wird dem Nutzer zusammen mit anderen iPass WiFi-Hotspots als ein Wireless-Standort zur Auswahl angezeigt. Wie jeden anderen Telefonbucheintrag auch, kann der Nutzer den Unternehmensstandort im Client mit einem Lesezeichen versehen, um ihn künftig schneller auswählen zu können.
 - c. Der Nutzer klickt auf **Verbinden** und wird aufgefordert, die für das Netz erforderlichen Anmeldeinformationen einzugeben. Wenn ein VPN konfiguriert ist, muss der Nutzer die VPN-Anmeldeinformationen ebenfalls eingeben.
2. Der iPassConnect-Client verwendet SSID, WEP-Schlüssel und das GI.1-Zugriffsverfahren aus dem cbook-Eintrag, um sich beim Zugangsknoten anzumelden und die Anmeldeinformationen des Nutzers via GIS an das Zugangs-Gateway (innerhalb der DMZ oder des Unternehmensnetzes) zu übermitteln.
3. Das Zugangs-Gateway überträgt die Verbindungsdatensätze mittels RADIUS an den AAA-Server des Unternehmens, der die Nutzerberechtigungen in der firmeneigenen Nutzerdatenbank überprüft. Wenn diese Datenbank zur Verwaltung von Nutzerprofilen nicht RADIUS verwendet, kann der Kunde einen Proxy-Server (wie FreeRadius) verwenden, um die "Übersetzung" der Daten von RADIUS aus dem

Zugangs-Gateway in das Format der Nutzerdatenbank, wie LDAP, und umgekehrt zu übernehmen.

4. Sobald der Nutzer anhand der Datenbank authentifiziert ist, wird die Zugriffsantwort über den AAA-Server, das Zugangs-Gateway und den Zugangsknoten zurück an den iPassConnect-Client gesendet. Der Zugangsknoten erhält vom Zugangs-Gateway eine IP-Adresse und leitet diese an den iPassConnect-Client weiter, damit dieser auf das Internet zugreifen kann. (Über diese Internetverbindung können das Telefonbuch und/oder Softwareupdates hochgeladen bzw. SQM-Daten übertragen werden.)
5. Wenn ein VPN konfiguriert ist, startet iPassConnect den VPN-Client, der über WLAN mit dem VPN Concentrator kommuniziert. Dieser wiederum leitet die Zugriffsanforderung zur Autorisierung an den AAA-Server im Unternehmensnetz weiter. Nach erfolgreicher Autorisierung erhält das VPN von einem DHCP-Server im Unternehmensnetz eine IP-Adresse und leitet diese an den iPassConnect-Client weiter, um die Funkkommunikation zu sichern.

GASTZUGRIFF: Da GIS Standard-HTTPS-Messaging verwendet, kann der Zugriff entweder über eine Client-Software (z. B. iPassConnect) oder über eine einfache Browseranmeldung angefordert werden. Deshalb ist diese Konfiguration optimal für Kunden, die Gastzugriffe auf das Internet steuern und gleichzeitig den Zugriff auf Unternehmensdaten absichern möchten.

Zusätzliche Servicekomponenten:

Die Konfiguration für GIS-Authentifizierung umfasst folgende zusätzliche Servicekomponenten:

- ein kundeneigenes installiertes GIS-fähiges IEEE 802.11b-Zugangs-Gateway. Eine Liste GIS-fähiger Zugangs-Gateways finden Sie im iPass Portal unter **Tech Info > Interoperability**.
- einen kundeneigenen, von diesem betriebenen RADIUS AAA-Server sowie eine Authentifizierungsdatenbank

Einzigartige Funktionen

- Die GIS-Implementierung bietet erweiterte Sicherheit durch die Verwendung eines in der Branche häufig verwendeten De-facto-Standardprotokolls.
 - Der SSL-Tunnel sichert Anmeldeinformationen der Nutzer
 - Das Zugangs-Gateway kann für den Gastzugriff auf das Internet via Webbrowser konfiguriert werden.
- Für alle iPass-Nutzer kann dieselbe Authentifizierungsdatenbank verwendet werden.
- Für den Nutzer besteht kein Unterschied zu allen anderen iPass Wireless Broadband-Verbindungen.

Empfohlene Architektur gemäß Best Practices:

- Aktive (gesendete) SSID
- Offener Sender für Zugangsknoten (WEP/Pre-Shared Key-Modus optional)
- Zugangsknoten und Zugangs-Gateway in der DMZ
- VPN-Verbindung für Zugriff auf Unternehmensdaten erforderlich

Konfigurationseinstellungen:

Kundeneigener Telefonbucheintrag

Diese Lösung kann ganz einfach durch die Übermittlung eines kundeneigenen Telefonbuchs (cbook) implementiert werden. Wie in der Basic-Version enthält dieser Eintrag die für die Verbindung mit dem Zugangsknoten erforderliche SSID und den WEP-Schlüssel (falls verwendet).

Darüber hinaus muss der cbook-Eintrag die Verwendung des GI.1-Zugriffsverfahrens (ap_gi_1.dll) sowie das erforderliche Routing-Präfix, Projekt-/Abteilungscode und die Roaming-Domain definieren, damit die Authentifizierungsanfragen ordnungsgemäß an das lokale Netz übertragen werden.

Anweisungen zum Erstellen der vom kundeneigenen Telefonbuch (cbook) übermittelten Daten finden Sie im Dokument *iPass® Customer Tech Note: Creating a Customer Access Point List (Cbook)*. Das Dokument finden Sie im Portal unter **Tech Info > Documentation > Tech Notes**.

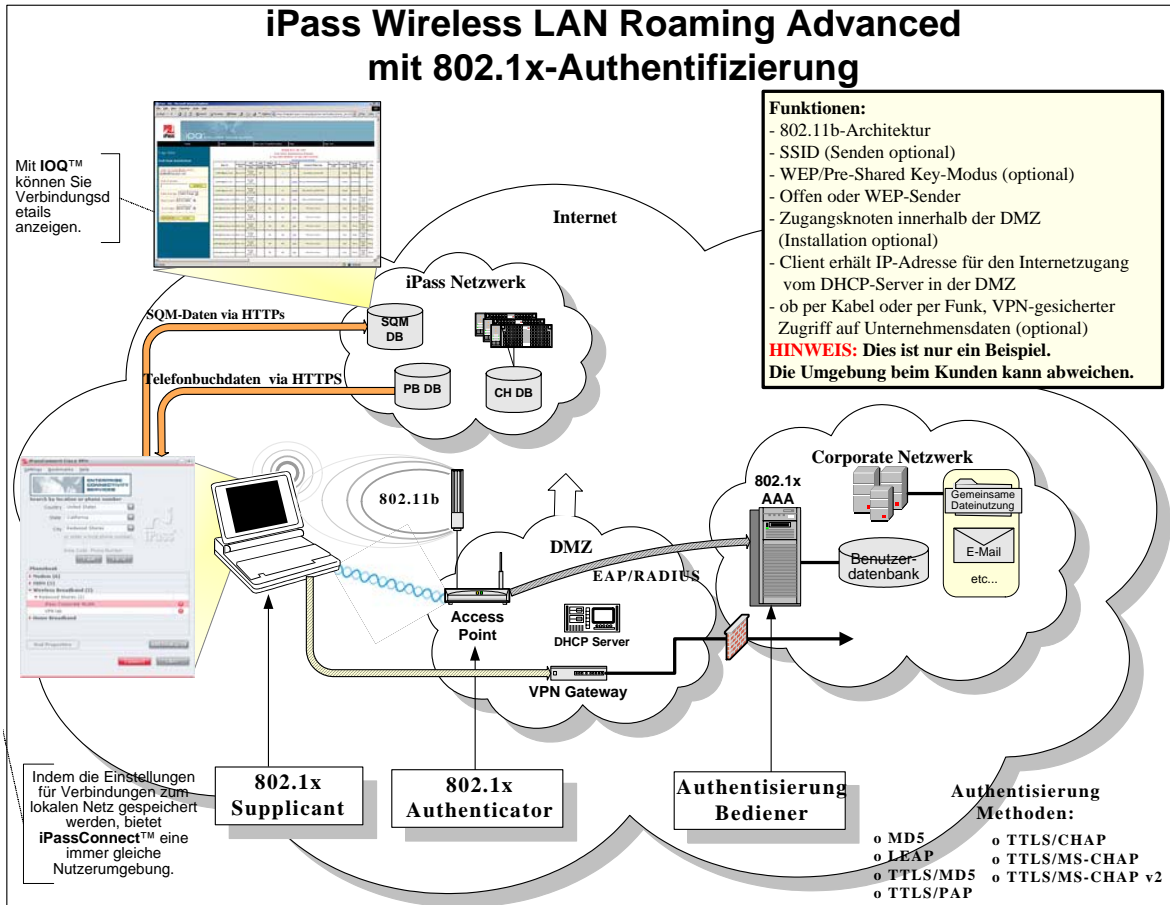
Routing der Nutzererkennung

Die iPassConnect-Software enthält, abhängig von dem Netz, zu dem eine Verbindung hergestellt werden soll, Standardeinstellungen für den Aufbau der Anmeldeinformationen von Nutzern. Nutzerkennungen für Verbindungen zum iPass-Netz (pbook POPs) werden anders aufgebaut als die Anmeldeinformationen für Verbindungen zu Kundennetzen (cbook POPs) oder VPN-Verbindungen.

Besonders wenn ein Nutzer eine Verbindung zu einem kundeneigenen Hotspot herstellt, erstellt iPassConnect Nutzerkennungen durch das Verknüpfen von möglichem Präfix (Eintrag in `cbook.txt`), Nutzernamen (wie in iPassConnect in der Maske **Nutzerinformationen** eingegeben) und möglichem Suffix, d. h. einer weiteren Routing-Domäne (Eintrag in `cbook.txt`).

Wenn dieses Client-spezifische Standardroutingformat für die Anforderungen des Kunden nicht ausreicht (z. B. wenn sich Nutzer mit vielen unterschiedlichen Domänen oder Abteilungs-/Kostenstellenangaben anmelden), kann es durch iPass Customer Care geändert werden.

Option 3: iPass Wireless LAN Roaming Advanced mit 802.1x-Authentifizierung



So funktioniert's

- Der Nutzer startet den iPassConnect-Client:
 - Wenn die SSID gesendet wird, erkennt iPassConnect anhand des Eintrags im kundeneigenen Telefonbuch (cbook) automatisch alle WiFi-Zugangsknoten, die zum Wireless LAN Roaming gehören, und stellt diese genau wie iPass WiFi-Hotspots dar.
 - Wenn die SSID nicht gesendet wird, gibt der Nutzer Land, Bundesstaat und Stadt des Unternehmensstandortes ein. Der Unternehmensstandort wird dem Nutzer zusammen mit anderen iPass WiFi-Hotspots als ein Wireless-Standort zur Auswahl angezeigt. Wie jeden anderen Telefonbucheintrag auch, kann der Nutzer den Unternehmensstandort im Client mit einem Lesezeichen versehen, um ihn künftig schneller auswählen zu können.
- Der iPassConnect-Client verwendet SSID, WEP-Schlüssel (falls verwendet) und das 802.1x-Zugriffsverfahren (auf der Grundlage des Authentifizierungstyps) aus dem cbook-Eintrag, um sich via 802.1x beim Zugangsknoten anzumelden.
- Der Zugangsknoten überträgt die Verbindungsdaten mittels EAP/RADIUS an den 802.1x-Authentifizierungsserver im Unternehmensnetz weiter. Wenn diese Datenbank zur Verwaltung von Nutzerprofilen nicht RADIUS verwendet, können verschiedenste 802.1x-Authentifizierungsserver (wie MS IAS-, Funk- oder MDC-Server) die Daten in das Format der lokalen Datenbank, beispielsweise LDAP oder Active Directory, "übersetzen".
- Sobald der Nutzer authentifiziert ist, wird die Zugriffsantwort über den AAA-Server und den Zugangsknoten zurück an den iPassConnect-Client gesendet. Der

Zugangsknoten erhält von einem DHCP-Server (entweder innerhalb der Firewall oder des Unternehmensnetzes) eine IP-Adresse und gibt diese an den iPassConnect-Client weiter, damit dieser auf das Internet zugreifen kann. (Über diese Internetverbindung können das Telefonbuch und/oder Softwareupdates hochgeladen bzw. SQM-Daten übertragen werden.)

5. Wenn ein VPN konfiguriert ist, startet iPassConnect den VPN-Client, der über Funk mit dem VPN Concentrator kommuniziert. Dieser wiederum leitet die Zugriffsanforderung zur Autorisierung an den AAA-Server im Unternehmensnetz weiter. Nach erfolgreicher Autorisierung erhält das VPN von einem DHCP-Server im Unternehmensnetz eine IP-Adresse und leitet diese an den iPassConnect-Client weiter, um die Funkkommunikation zu sichern.

Zusätzliche Servicekomponenten:

Die Konfiguration für 802.1x-Authentifizierung umfasst folgende zusätzliche Servicekomponenten:

- kundeneigene, installierte 802.11b-Zugangsknoten, die mindestens eine der folgenden 802.1x-Authentifizierungsmethoden unterstützen:
 - MD5
 - LEAP
 - TTLS – PAP
 - TTLS – CHAP
 - TTLS – MD5
 - TTLS – MSCHAP
 - TTLS – MSCHAPv2
- einen kundeneigenen, von diesem betriebenen 802.1x-Authentifizierungsserver
- eine kundeneigene Authentifizierungsdatenbank

Einzigartige Funktionen

- Die 802.1x-Implementierung bietet verbesserte Sicherheit.
- Für alle iPass-Nutzer kann dieselbe Authentifizierungsdatenbank verwendet werden.
- Für den Nutzer besteht kein Unterschied zu allen anderen iPass Wireless Broadband-Verbindungen.

Empfohlene Architektur gemäß Best Practices:

- SSID-Übertragung (optional)
- Offener/EAP-Sender für Zugangsknoten (WEP/Pre-Shared Key-Modus optional)
- Zugangsknoten und DHCP-Server in der DMZ
- VPN-Verbindung für Zugriff auf Unternehmensdaten für LEAP-Authentifizierung erforderlich

Konfigurationseinstellungen:

Die 802.1x-Authentifizierung erfordert spezielle Einstellungen sowohl im kundeneigenen Telefonbuch als auch im Clientprofil selbst.

Festlegen der 802.1x-Authentifizierungsmethode

Während der Anpassung von iPassConnect können Sie im Clientprofil eine Standardmethode für 802.1x festlegen. Darüber hinaus kann jeder cbook-Eintrag ein Zugriffsverfahren mit der entsprechenden 802.1x-Authentifizierungsmethode enthalten. Gültige Werte für Beides sind:

- 8021X
- 8021X_MD5

- 8021X_LEAP
- 8021X_TTLS_PAP
- 8021X_TTLS_CHAP
- 8021X_TTLS_MD5
- 8021X_TTLS_MSCHAP
- 8021X_TTLS_MSCHAPV2

Wenn der cbook-Eintrag eine bestimmte Methode enthält, weist das darauf hin, dass der Zugangsknoten ein bestimmtes Protokoll benötigt und dass iPassConnect für den Verbindungsaufbau die angegebene Methode verwendet.

Enthält der cbook-Eintrag keine Angabe zur Methode, wird die Standardmethode aus der Datei `config.ini` verwendet. Wenn sowohl der cbook-Eintrag als auch die Datei `config.ini` einen Wert für 802.1x enthalten, verhandelt iPassConnect mit dem Authentifizierungsserver darüber, welches Protokoll verwendet werden soll.

Zertifikatsvalidierung für 802.1x mit TTLS:

Bei getunnelten 802.1x-Authentifizierungsmethoden (d. h. TTLS), versucht der iPassConnect-Client das Zertifikat des AAA-Servers zu validieren. Dazu muss der Inhalt des Felds **Issued To** (Ausgestellt für) des Serverzertifikats (in der Regel der Hostname des Servers) mit dem cbook-Eintrag übertragen werden.

Anweisungen zum Erstellen der vom kundeneigenen Telefonbuch (cbook) übermittelten Daten finden Sie im Dokument *iPass® Customer Tech Note: Creating a Customer Access Point List (Cbook)*. Das Dokument finden Sie im Portal unter **Tech Info > Documentation > Tech Notes**.

Routing der Nutzerkennung

Standardmethoden für die 802.1x-Authentifizierung:

Wenn ein Nutzer eine Verbindung zu einem kundeneigenen Hotspot herstellt, erstellt iPassConnect Nutzerkennungen standardmäßig durch das Verknüpfen eines möglichen Präfix (Eintrag in `cbook.txt`), des Usernames (wie in iPassConnect in der Maske **Nutzerinformationen** eingegeben) und eines möglichen Suffix, d. h. einer weiteren Routing-Domäne (Eintrag in `cbook.txt`).

Für Standardmethoden zur 802.1x-Authentifizierung (wie MD5 und LEAP) wird diese Standard-Clienteneinstellung verwendet, um die Nutzerkennungen zu erstellen. Wenn dieses Client-spezifische Standardroutingformat für die Anforderungen des Kunden nicht ausreicht (z. B. wenn sich Nutzer mit vielen unterschiedlichen Domänen oder Abteilungs-/Kostenstellenangaben anmelden), kann es durch iPass Customer Care geändert werden.

Methoden für die getunnelte 802.1x-Authentifizierung:

Die getunnelten TTLS-802.1x-Methoden unterstützen während des Authentifizierungsprozesses zwei unterschiedliche Nutzeridentitäten. Die äußere Identität enthält die Informationen, die zur Weiterleitung der Anfrage an den Authentifizierungsserver erforderlich sind. Sie dient dazu, die Anonymität des Endnutzers zu gewährleisten, der versucht auf das Netz zuzugreifen. Die äußere Identität routet die 802.1x-Anfrage beispielsweise über IPASS/anonymous@megacorp.com. Die innere Identität enthält die wirkliche Identität des Endnutzers, der den Service anfordert. Die innere Identität verwendet dann beispielsweise "[johndoe](#)" zur Identifizierung des Endnutzers.

Um die äußere und innere Identität zu erstellen, verwendet iPassConnect 3.2 den Standardwert des Client für kundeneigene Hotspots. Zur Erstellung des NAI für die äußere Identität wird die in der Maske **Nutzerinformationen** festgelegte Nutzeridentität verwendet.

Wenn dieses Client-spezifische Standardroutingformat die TTLS-802.1x-Methoden des Kunden nicht unterstützt, kann iPass Customer Care den Client so konfigurieren, dass eine alternative Methode zur Erstellung der Anmeldeinformationen verwendet wird.

Weitere Informationen

iOQ/SQM-Daten

Für iPassConnect 3.2 und höher werden für jeden Versuch eines Verbindungsaufbaus zu Wireless LAN Roaming-Netzen SQM-Datensätze generiert. Der SQM-Datensatz enthält immer den in der Maske **Nutzerinformationen** eingegebenen Username, die verwendete SSID, die MAC-Adresse des Client und die Installations-ID der Client-Software des Nutzers.

Der Umfang der standortbezogenen Informationen, die mit den SQM-Daten übertragen werden, hängt davon ab, wie der Nutzer eine Verbindung zum Netz hergestellt hat. Wenn der Nutzer die Auto-Erkennung verwendet hat, anstatt diesen bestimmten Zugangsknoten aus dem Verzeichnis auszuwählen (d. h. die SSID wird gesendet), dann enthält der SQM-Datensatz keine standortspezifischen Daten. Wenn der Nutzer jedoch den spezifischen Zugangsknoten auswählt, enthält der SQM-Datensatz Informationen zu Land, Bundesstaat (falls zutreffend), Stadt, Standortname, MAC-Adresse des Zugangsknotens und Signalstärke.

Schlussfolgerung

Der Wireless LAN Roaming-Service weitet die zentralisierte Verwaltung, Netzabdeckung, Sicherheitsrichtlinien und die vom iPass Corporate Access-Dienst gewohnte Nutzerfreundlichkeit auf vom Unternehmen betriebene private Wireless LANs aus. Nutzer profitieren von der gewohnten Nutzeroberfläche und der konsistenten, standortunabhängigen Verbindungsqualität, während die IT-Administratoren alle Richtlinien für den Remote-Zugriff sowie alle Personal Firewall-, Antiviren- und VPN-Ressourcen zentral verwalten und durchsetzen können, um sicherzustellen, dass alle Nutzer des Standort-WiFi-Netztes sicher arbeiten können.

Informationen zu iPass

iPass Inc. (www.ipass.com) stellt Unternehmen softwaregestützte Verbindungsdienste zur Verfügung, die den Mitarbeitern an praktisch jedem Standort der Welt den sicheren Zugriff auf Informationen und Anwendungen im Unternehmensnetz ermöglichen. Als Virtual Network Operator (VNO) bietet iPass den Mitarbeitern eines Unternehmens eine Auswahl IP-basierter Verbindungstechnologien an, wie beispielsweise Wired und Wireless Broadband-Verbindungen auf Flughäfen, in Hotels und Konferenzzentren auf der ganzen Welt. Der iPassConnect™-Client kann problemlos im gesamten Unternehmen bei jeglichen Computertypen und Betriebssystemen eingesetzt werden. Nach seiner Bereitstellung ermöglicht der iPass-Service der IT-Abteilung des Unternehmens die Kontrolle über den Zugriff auf die Netzressourcen. iPass wurde 1996 gegründet und hat seinen Hauptsitz in Redwood Shores in Kalifornien sowie weitere Niederlassungen in Nordamerika, Europa und dem asiatisch-pazifischen Raum.

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

Australien
iPass Holdings Pty Ltd.
Level 1, 80 Waterloo Road
Macquarie Park, NSW 2113
Australien
Tel: +612 8876.8700
Fax: +612 8876 8777

Großbritannien
iPass (U.K.) Limited
139 Piccadilly
London W1J 7NU
Großbritannien
Tel: +44 20.7317.4400
Fax: +44 20.7317.4450

Hongkong
iPass Asia Pte Ltd.
3802A, Lippo Centre
Tower Two
89 Queensway, Admiralty
Hongkong
Tel: +852.2918.8268
Fax: +852.2918.8278

Deutschland
iPass EMEA
Region D/A/CH
Wiener Platz 7
D-81667 München
Deutschland
Tel: +49 89 44 142 - 100
Fax: +49 89 44 142 - 111
infoDach@ipass.com

Niederlande
iPass EMEA
Kingsfordweg 151
1043 GR Amsterdam
Niederlande
Tel: +31 20 491 77 48
Fax: +31 20 491 9090
sales-emea@ipass.com

Schweden
iPass EMEA
Frösundaviks Allé 15
Solna
Stockholm 16970
Schweden
Tel: + 46 (8) 590 041 39
Fax: + 46 (8) 590 041 10
sales-emea@ipass.com

Belgien
Pegasus Park
Pegauslaan 5
1831 Diegem
Tel: +32 2 709 29 40
Fax: +32 2 709 22 22
sales-emea@ipass.com

Dänemark
South Harbour
Sluseholmen 2-4
Copenhagen South 2450
Tel: +45 36 94 45 65
Fax: +45 36 94 45 10
sales-emea@ipass.com

Japan
iPass Inc.
Ginko Kyokai Building, 15th Floor
1-3-1 Marunouchi
Chiyoda-ku, Tokyo 100-0005
Japan
Tel: +81 3.3216.7266
Fax: +81 3.3216.7281

Singapur
iPass Asia Pte Ltd.
7 Temasek Boulevard
#23-02 Suntec Tower One
Singapore 038987
Tel: +65 6334.8783
Fax: +65 6337.033

Lateinamerika
Tel: +1 650.232.4186
Fax: +1 650.232.0229
sales-sa@ipass.com