

# iPassConnect™ Universal Client

Zuverlässige Zugänge für Remote-Nutzer und mobile Mitarbeiter

- Vereinfachen Sie den Zugang durch eine einheitliche Lösung für alle Endgeräte und Zugangstechnologien
- Ermöglichen Sie einen Mobilfunkzugang ohne jeglichen Konfigurationsaufwand
- Integrieren Sie den Internetzugang, AAA und VPN zu einer Single-Sign-On-Lösung
- Setzen Sie Ihre Richtlinien bei jedem Netzzugang durch, indem sowohl das Endgerät als auch Software-Stände geprüft werden

Geschäftsreisende, mobile Mitarbeiter und Telearbeiter brauchen einen benutzerfreundlichen und zuverlässigen Zugriff auf Unternehmensdaten und das Internet. Gleichzeitig kämpfen die IT-Abteilungen damit, einen komfortablen und sicheren Netzzugang für Nutzer bereitzustellen, der sich zentral verwalten lässt und noch dazu kompatibel zur bestehenden Infrastruktur ist. Wi-Fi-Hotspots, mobile Datenübertragung und Internet-Zugriff von Flugzeugen aus versprechen zwar eine höhere Produktivität, können aber unter Umständen das Herstellen einer Verbindung erschweren und die Verwaltung der Zugangsmöglichkeiten für die IT-Abteilung komplizierter gestalten.

iPass richtet sich nach den Anforderungen von Nutzern und IT-Personal gleichermaßen, indem es einen sicheren, einfachen und effektiven Fernzugriff auf Netzwerke Wirklichkeit werden lässt. Über iPass® Corporate Access™ erhalten Nutzer durch eine Vielzahl von Zugriffsmethoden in ca. 150 Ländern mobile On-Demand-Verbindung zum Unternehmensnetz. iPass ermöglicht dies durch eine weltweite Einwahlabdeckung und dem größten globalen Breitband-Roaming-Netz. Über den Zugriff auf Mobile Data Netze, einen drahtlosen Zugang während des Fluges durch Connexion by Boeing<sup>SM</sup> sowie über 20.000 Ethernet- und Wi-Fi-Hotspots, einschliesslich einer Fülle von T-Mobile® HotSpot-Standorten in den USA, ist die Wahrscheinlichkeit sehr groß, dass Sie unabhängig von Ort und Zeit immer einen Zugang bekommen, wenn Sie sie brauchen.

iPass lässt die Nutzer produktiv sein, indem es Verbindungen über iPass-fremde Netze, wie öffentliche Hotspots, Personal Wireless LANs und Ihr firmeneigenes drahtloses LAN, ermöglicht. Für die IT-Abteilung liegt der Vorteil darin, dass

dank iPass diese Verbindungen mit der Durchsetzung von Sicherheitsrichtlinien und detailliertem Nutzungsreporting bereitgestellt werden.

Dies alles wird durch den iPassConnect™ Universal Client ermöglicht, eine einzige Schnittstelle, die perfekt auf mobile Mitarbeiter und IT-Personal zugeschnitten ist.

- Nutzer können über eine Vielzahl von Datenverarbeitungsgeräten und praktisch jede Netztechnologie problemlos und sicher auf Unternehmensnetze zugreifen.
- IT-Verantwortliche haben die Gewissheit, dass sie mit zentral verwalteten Richtlinien für Zugang, Sicherheit und Nutzung steuern können, wie, wo und unter welchen Bedingungen die Nutzer eine Verbindung herstellen.
- Mit iPassConnect kann das IT-Personal die Betriebskosten durch schnelle und einfache Verteilungs- und Aktualisierungsfunktionen minimieren.

## AUTOMATISIERTE UND KOMFORTABLE ANMELDUNG

Basierend auf Beobachtungen von iPass-Nutzern in der ganzen Welt wurde iPassConnect für eine optimale und intuitive Nutzung konzipiert. Anhand der Ergebnisse konnten die folgenden Funktionen definiert werden.

Die **Voranmeldung für Windows-Domänen**<sup>1</sup> stellt Remote-Nutzern die gleiche Funktionalität wie im Büro bereit. Nutzer von Windows 2000 und Windows XP profitieren von der Erstellung von Domänenanmeldeskripts, von benutzerdefinierten Laufwerkszuordnungsfunktionen sowie von Hinweisen zum Ablauf des Domänenpassworts.

**System Tray Launch**<sup>1</sup> ermöglicht es den Nutzern, über ein iPass-Symbol in der Taskleiste eine Verbindung zu verfügbaren Wi-Fi-Zugangspunkten, Mobile Data Netze und mit einem Lesezeichen versehene Standorten herzustellen, wenn iPassConnect beim Systemstart ausgeführt wird.





Die **Standort-basierte Suche**<sup>ii</sup> ermöglicht eine schnelle und einfache Wahl der optimalen Verbindung für jeden beliebigen Standort. Die verfügbaren Mobilfunknetze werden automatisch angezeigt, und bei Eintritt in einen Standort werden alle lokalen Zugangsoptionen bereitgestellt.

**One-Click VPN Integration**<sup>i</sup> übergibt den Nutzernamen und das Passwort automatisch an den VPN-Client, wenn iPassConnect gestartet wird.

#### **VORTEILE VON IPASSCONNECT: ZUGÄNGE ZUM MOBILFUNKNETZ SO EINFACH WIE WÄHLVERBINDUNGEN**

- Erkennt alle Wi-Fi- und Mobile Data Netze automatisch
- Konfiguriert die Netzwerkkarten der Nutzer automatisch
- Benachrichtigt die Nutzer, wenn Wi-Fi- und Mobile Data Netze verfügbar sind
- Unterstützt Nutzer beim Herstellen einer Verbindung zu einem iPass-fremden Wi-Fi HotSpot durch Starten eines Webbrowsers und eines VPN
- Zeigt die Signalstärke der Wi-Fi- und Mobilfunknetze an

#### **Optimierte Anmeldung im Netz**

- Standort-basierte Suche zeigt alle verfügbaren Zugangsoptionen an
- Schneller Zugriff auf Mobilfunknetze und mit einem Le-sezeichen versehene Standorte über die Taskleiste
- Integration per Mausklick in führende VPN-, persönliche Firewall- und Anti-Virus-Software
- Unterstützung von Windows GINA Prelogon

#### **End-to-End-Sicherheit auf Richtlinienbasis**

- Integrierte Endgeräte-Richtlinienverwaltung führt Analyse und Schwachstellen-Behebung aus
- Setzt Verbindungssicherheit über VPNs, persönliche Firewalls und Anti-Virus-Software durch
- VPN-Enforcement gewährleistet, dass nur Geräte auf das Unternehmensnetz zugreifen können, die die geltenden Richtlinien erfüllen

#### **Senkung der Gesamtbetriebskosten**

- Niedrigere Kosten für Support und Schulung der Nutzer
- Schnelle und flexible Implementierung
- Mechanismus zur Kostenkontrolle für verschiedene Zugangstypen
- Eine Rechnung für alle Zugangsoptionen, mit Unterstützung für die Kostenstellenabrechnung
- Windows-, Mac- und PDA-Unterstützung

#### **ZUGANG ZUM MOBILFUNKNETZ, SO SICHER UND EINFACH WIE WÄHLVERBINDUNGEN**

Die Akzeptanz von Wi-Fi- und Mobile Data Netzen nimmt zwar immer weiter zu, allerdings ist die Verwendung dieser Netze immer noch recht komplex. Die iPassConnect-Funktionen wurden im Hinblick darauf entwickelt, den Zugriff auf Mobilfunknetze genauso einfach zu gestalten wie die Einwahl. Durch neue Funktionen (einschließlich Anzeige der Signalstärke und Unterstützung iPass-fremder Netze) lassen sich die Mobilnetze noch einfacher nutzen als jemals zuvor.

Die **drahtlose Netzerkennung und -konfiguration**<sup>ii</sup> erkennt automatisch alle Wi-Fi- und Mobile Data Netze, die sich in Reichweite befinden, einschließlich öffentlicher Hotspots. Sobald ein Mobilfunknetz ausgewählt wurde, wird die Netzwerkkarte des Nutzers automatisch mit den korrekten Verbindungseinstellungen konfiguriert.

Mit der **Unterstützung für iPass-fremde Netze**<sup>i</sup> wird das Ausmachen eines lokalen Wi-Fi-Hotspots oder einer Mobilfunkverbindung noch einfacher. Jetzt erkennt iPassConnect alle verfügbaren Mobilfunknetze, einschließlich der nicht iPass-fähigen Netze, und zeigt diese an. Wenn ein iPass-fremdes Netz eine weitere Authentifizierung erfordert, startet iPassConnect einen Webbrowser und ein VPN für den Nutzer.

Die **Filterung von Mobile Data Netzen**<sup>i</sup> ermöglicht es den Nutzern, das beste Netz auszuwählen, indem die „Enterprise Ready“ Wi-Fi- und Mobilfunknetze priorisiert und mit einem iPass-Symbol versehen als erstes aufgelistet werden. Andere zusätzlich verfügbare WLAN Netze sowie die Signalstärke aller erkannten Standorte werden ebenfalls angezeigt.

**Mobile Data**<sup>i</sup> erweitert die Verbindungsoptionen, die den Nutzern zur Verfügung stehen. iPassConnect kann verwendet werden, um über iPass und Mobilnetzbetreiber mit einer Reihe von breitbandigen Mobilfunk-Verbindungen sicher und ohne großen Aufwand auf Unternehmensdaten zuzugreifen.

**Personal Wireless Support**<sup>i</sup> vereinfacht den Zugriff der Nutzer für eine steigende Anzahl an privaten Wi-Fi-Zugangspunkten. Die Nutzer können private Netze zu ihrem iPassConnect-Verzeichnis hinzufügen und die Konfiguration der Netzwerkkarten automatisch erkennen lassen.

Die **sichere Wi-Fi-Authentifizierung** bietet vollständigen Schutz zwischen den einzelnen Stationen. iPass-Zugangsanbieter haben einen Sicherheitsstandard für Wi-Fi-Access-Gateways implementiert, der Hotspots über den Austausch digitaler Zertifikate authentifiziert, bevor eine Verbindung hergestellt wird. Die Zugangsdaten des Nutzers werden anschließend über einen SSL-Tunnel gesendet, sodass eine sichere Authentifizierung zwischen Client und Unternehmensnetz gewährleistet ist.

#### **END-TO-END-SICHERHEIT AUF RICHTLINIENBASIS**

iPass gewährleistet, dass die Endgeräte beim Herstellen einer Verbindung zum Netz mit iPassConnect und vor dem Herstellen einer Verbindung zum Unternehmensnetz gesichert sind.

Im Zeitalter gestiegener Mobilität und vielfältiger Breitbandop-

tionen ist diese Sicherheitsanforderung für den Netzzugang unabdingbar.

**Central Management Policies** ermöglichen es dem IT-Personal, die erforderliche Clientsicherheit problemlos zu konfigurieren und an die iPass-Nutzer zu verteilen, sodass die neuesten Richtlinien bei jeder Anmeldung des Nutzers durchgesetzt werden. Es können Richtlinien durchgesetzt werden, die die Verwendung des Netzwerkzugangs und die verschiedenen Zugriffsmethoden, die Security Software der Endgeräte, das Vorhandensein von Betriebssystem-Patches sowie die Version und die Konfiguration regeln.

**Endpoint Policy Management™** schützt mobile Nutzer bei jedem Zugang ins Internet, indem die Verwaltung der Sicherheitsrichtlinien, die Durchsetzung der Richtlinien und die Schwachstellen-Behebung automatisiert werden. Dieser wertvolle Service optimiert und automatisiert das Patch-Management für Microsoft Windows-Betriebssysteme und Anti-Virus-Updates.

Die **Sicherheitskompatibilität mit Drittherstellern** wird über die iPass Alliance™ der Technologiepartner erzielt, die eine iPassConnect-Integration mit Anbietern von Sicherheitslösungen für Unternehmen erlaubt, einschließlich führender VPN-Produkte, persönliche Firewalls, Intrusion Detection-Produkte und Anti-Virus-Software. Dies hat zwei Vorteile: Zum einen wird den Nutzern ein sicherer Zugang bereitgestellt und zum anderen wird der Verbindungsprozess vereinfacht.

**SecureConnect Integration** verhindert, dass der Nutzer eine Verbindung zum Internet herstellen kann, es sei denn, Anti-Virus-Software, persönliche Firewall oder Intrusion Detection-Systeme sind aktiviert. Wenn diese vor Beginn einer Sitzung nicht aktiv sind, kann iPassConnect die entsprechenden Sicherheitsservices automatisch starten, bevor eine Verbindung zum Internet hergestellt wird.

**Auto-Tear-down Integration** kann so konfiguriert werden, dass die Internet-Verbindung automatisch beendet wird, wenn ein VPN-Tunnel, eine persönliche Firewall oder eine Anti-Virus-Sicherheitslösung deaktiviert ist oder nicht ausgeführt wird.

Mit der **VPN-Enforcement™** kann die IT-Abteilung sicherstellen, dass nur die Geräte, die die festgelegten Sicherheitsstandards erfüllen, eine VPN-Verbindung zum Unternehmensnetz herstellen können. iPassConnect kann in Verbindung mit dem DeviceID-Service zum Steuern des VPN-Zugriffs verwendet werden. Zusätzlich können Security Software und Betriebssysteme in Verbindung mit Endpoint Policy Management vor dem Starten des VPNs aktualisiert werden, sodass die Richtlinien durchgesetzt werden können, ohne die Geräte vom Netz aussperren zu müssen.

**iPass Secure End-to-end Encrypted Login (iSEEL)** schützt die Kennwörter vom Client bis zum Unternehmensserver über drahtgebundene und Wi-Fi-Zugänge. iPassConnect verwendet eine komplexe „Public-Key“-Kryptografie, um die Kennwörter vor Lauschangriffen zu schützen. Außerdem weist es jeder Sitzung eine eindeutige ID zu, um Replay-Angriffe zu verhindern.

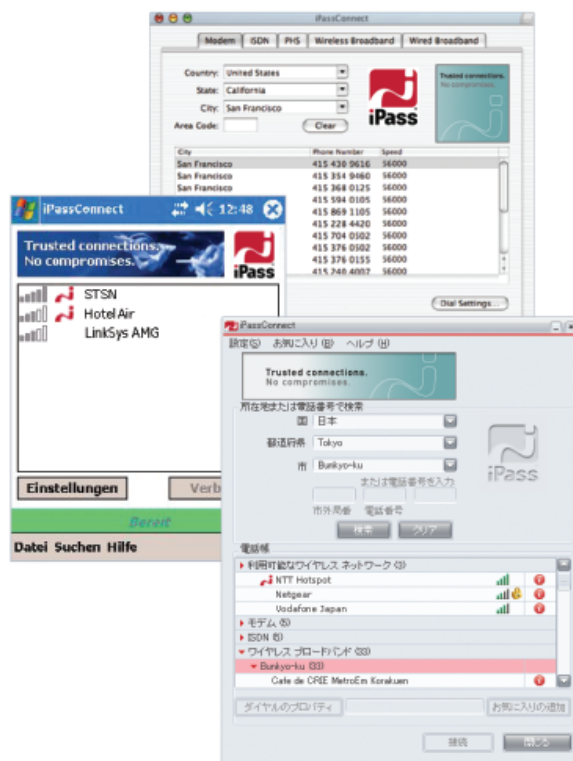
## SENKUNG DER GESAMTBETRIEBSKOSTEN

iPassConnect ermöglicht eine Steuerung, die alles andere als komplex ist. Der iPass-Service erleichtert den Nutzern das Herstellen von Verbindungen, bietet Administratoren eine einfache Verwaltungsmöglichkeit und stellt noch dazu mehrere Funktionen bereit, mit denen sich die Kosten senken lassen.

Die **qualitätsbasierte Telefonbuchsortierung** überprüft automatisch bei jeder hergestellten Verbindung, ob ein aktualisiertes Verzeichnis der Zugangspunkte vorhanden ist. iPass fügt häufig neue Zugangspunkte hinzu und entfernt problematische. Dadurch stehen den Nutzern die neuesten Nummern zur Verfügung, die entsprechend der gemessenen Zuverlässigkeit aufgeführt sind, sodass alle Verbindungen erfolgreich hergestellt werden können.

Die **Einwahlintelligenz** reduziert die Anrufe beim Help-Desk und die Probleme der Nutzer in erheblichem Maße. Bei Einwahlzugängen erkennt iPassConnect automatisch, ob innerhalb der USA eine Vorwahl hinzugefügt werden muss. Internationale Einwahlregeln werden ebenfalls korrekt angewendet.

Bei der **Suche nach der lokalen Rufnummer** wird nach einem lokalen Einwahlzugang in den USA, nach schnellen Verbindungen sowie nach Möglichkeiten gesucht, mit denen die Kosten für Fernverbindungen gesenkt werden können.



iPassConnect 3.35 für Windows, iPassConnect 3.0 für PocketPC und iPassConnect 2.4 für Mac OS X.



**Smart Redial**, die intelligente Wahlwiederholung, spart dem Nutzer Zeit und Unannehmlichkeiten, indem sie den redundanten Aufbau des iPass-Netzwerks nutzt. iPassConnect wählt automatisch alle lokalen Zugangspunkte an, bis eine Verbindung hergestellt wurde.

**Universal All-Cities Nummern**, die in bestimmten Regionen zur Verfügung stehen, sind preiswerte, landesweite Zugangsnummern. Toll-free Zugangsnummern, die die separaten Rechnungen der lokalen Telefongesellschaften niedriger ausfallen lassen, sind ebenfalls verfügbar.

**Timeout-Richtlinien** für Leerlaufzeiten oder die maximale Sitzungsdauer verhindern, dass Verbindungen unendlich lang geöffnet bleiben. Damit wird sichergestellt, dass der Zugriff nur für die Zeit berechnet wird, in der die Nutzer den iPass-Service tatsächlich nutzen.

Eine **Gebührenabrechnung nach Kostenstelle** ermöglicht es den IT-Abteilungen, problemlos Rückschlüsse auf die Nutzung zu ziehen, indem sie die Nutzer den entsprechenden Abteilungen, Projekten oder Domännennamen zuordnen.

Mit der **Gebührenabrechnung über Kreditkarte** kann eine Firmenkreditkarte mit den Gebühren für Nutzerverbindungen belastet werden, um die

Verwaltung von Kosten und Kostenstellen zu vereinfachen.

Eine **einfache Anpassung** wird möglich durch eine Vielzahl von Optionen, die eine außergewöhnliche Flexibilität bieten. So können Administratoren z. B. RAS-Nummern hinzufügen oder löschen und das Verbindungsverhalten für einzelne Zugangspunkte definieren. iPassConnect kann auch so konfiguriert werden, dass das Firmenlogo und die Nummer des Help-Desk angezeigt wird.

#### NETZZUGANG FEST IM GRIFF

Mit sicheren, einfachen und effektiven Zugängen bleiben Remote-Mitarbeiter und mobile Nutzer produktiv, während das IT-Personal gleichzeitig unbesorgt sein kann. iPassConnect ermöglicht dies unabhängig davon, ob die Nutzer lieber mit einem Desktop, einem Notebook oder einem PDA auf das Unternehmensnetz zugreifen. Erfahren Sie, warum sich immer mehr Global 1.000-Unternehmen für iPass entscheiden, damit ihre Remote- und mobilen Mitarbeiter sowohl mit dem Büro als auch mit ihren Kunden in Verbindung bleiben.

Besuchen Sie doch gleich unsere Webseite unter [www.ipass.de](http://www.ipass.de).

#### KOMPATIBILITÄT UND SYSTEMANFORDERUNGEN

iPassConnect ist mit den im Folgenden genannten führenden Sicherheitsclients kompatibel. Eine Liste der spezifischen Produkte finden Sie unter [www.ipass.com](http://www.ipass.com). iPassConnect unterstützt die unten aufgeführten Sprachen und Plattformen.

##### VIRTUAL PRIVATE NETWORKS (VPNs)

- Aventail
- Check Point
- Cisco Systems
- Juniper
- Microsoft
- NCP
- Nortel

##### PERSÖNLICHE FIREWALLS UND INTRUSION DETECTION-SYSTEME

- Internet Security Systems
- Sygate
- Zone Labs

##### ANTI-VIRUS-SOFTWARE

- Network Associates/McAfee
- Symantec/Norton
- Trend Micro

##### UNTERSTÜTZTE PLATTFORMEN

- Windows XP
- Windows 2000
- Windows Mobile 2003
- Mac OS X (10.1.5 und höher)

##### UNTERSTÜTZTE SPRACHEN

- Englisch
- Französisch
- Deutsch (weltweit)
- Japanisch

- Portugiesisch (Brasilien)

- Koreanisch

- Chinesisch (vereinfacht & traditionell)

- Spanisch (Mittlerer Atlantik)

Mac-Benutzeroberfläche nur auf Englisch verfügbar. PDA-Benutzeroberfläche auf Englisch, Deutsch und Japanisch verfügbar.

<sup>i</sup> Nur bei iPassConnect 3.x für Windows verfügbar. Version 3.3 oder höher ist für Mobile Data und Endpoint Policy Management erforderlich. Für den Zugriff auf iPass-fremde Netze und Connexion by Boeing In-Flight-Hotspots fallen zusätzliche Gebühren an.

<sup>ii</sup> Verfügbar unter iPassConnect 3.x für Windows und iPassConnect 3.x für Windows Mobile 2003.

<sup>iii</sup> iPassConnect 3.35 für Windows und DeviceID-Integration erforderlich. Endpoint Policy Management-Integration optional.

iPass Deutschland GmbH  
Wiener Platz 7  
D-81667 München

+49 89 44 142 – 100  
+49 89 44 142 – 111 fx

[www.ipass.de](http://www.ipass.de)

