

iPassConnect™ Universal Client

Zuverlässige Zugänge für Remote-Nutzer und mobile Mitarbeiter

- Durch eine einheitliche Lösung für alle Endgeräte und Zugangstechnologien wird der mobile Zugang erheblich vereinfacht
- Der Mobilfunkzugang ist mit iPassConnect ohne jeglichen Konfigurationsaufwand möglich
- Internetzugang, AAA und VPN lassen sich zu einer Single-Sign-On-Lösung integrieren
- Richtlinien können bei jedem Netzzugang durchgesetzt werden, indem sowohl das Endgerät als auch die Aktualität von Software-Patches geprüft werden

Mobilität hat in unser modernes Geschäftsleben Einzug gehalten. Bewaffnet mit Laptop und PDA können Mitarbeiter heute arbeiten, wo und wann sie möchten – auf dem gesamten Firmengelände, im Büro ihrer Kunden, in Flugzeugen und Zügen, zu Hause und manchmal sogar im Café um die Ecke. Um stets effizient arbeiten zu können, benötigen die mobilen Mitarbeiter von heute eine einheitliche Zugangsmöglichkeit, um auch mobil auf ihre Informationsbasen zugreifen zu können und mit Kunden, Kollegen und Partnern in Kontakt zu bleiben. Je einfacher der Zugriff, desto besser. Alles was der mobile Mitarbeiter von heute will, ist verbunden zu sein – ohne wenn und aber.

Mit iPassConnect™ haben Remote-Nutzer und mobile Anwender einen einheitlichen universellen Client zur Hand, der bei jedem möglichen Verbindungsszenario überzeugt. Er unterstützt die Nutzer beim Verbindungsaufbau – und dies schneller, einfacher und sicherer als jemals zuvor.

NUTZEN SIE UNSER NETZ - ODER IHR EIGENES

iPassConnect bietet Nutzern eine einfache Möglichkeit des Zugriffs auf das Internet und firmeninterne Netzwerke, wobei eine Vielzahl an Zugangstechnologien verwendet werden kann. iPassConnect dient als zentrale Schnittstelle des iPass Mobile Office Services, der Zugang zum größten globalen Breitbandnetz mit globalen Einwahlmöglichkeiten in sich vereint. Weiterhin bietet der Service Zugangsmöglichkeiten zu Mobilfunknetzen sowie derzeit ca. 80.000 Ethernet und WLAN Hotspot Zugangspunkte, einschließlich des T-Mobile® HotSpot Netzes in den USA und Europa.

iPassConnect hilft Anwendern aber nicht nur beim Zugriff auf das iPass Netz. Die selbe Nutzererfahrung wird auch auf Netze

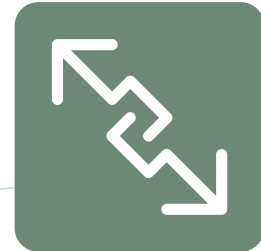
und Zugangspunkte übertragen, die nicht Teil des virtuellen iPass-Netzes sind. Hierzu zählen unternehmenseigene WLANs, öffentliche Hotspots sowie private WLANs. Dies hat für die IT-Abteilung den Vorteil, dass mit iPass für alle Verbindungen vom Unternehmen definierbare Sicherheitsrichtlinien angewendet und detaillierte Nutzungsdaten zur Verfügung gestellt werden.

Mit dem iPassConnect Universal Client kann Ihr Unternehmen alle Vorteile einer einheitlichen Schnittstelle genießen:

- Nutzer können über eine Vielzahl mobiler Endgeräte und unter Verwendung praktisch jeder Netztechnologie problemlos und sicher auf das Unternehmensnetz zugreifen.
- IT-Verantwortliche haben die Gewissheit, dass sie durch zentral verwaltete Richtlinien für Zugang, Sicherheit und Nutzung steuern können, wie, wo und unter welchen Bedingungen Nutzer eine Verbindung herstellen können.
- Mit iPassConnect können IT-Mitarbeiter die Betriebskosten minimieren, da sowohl Rollout als auch Aktualisierungen einfach und schnell ablaufen.

EIN CLIENT, ALLE ZUGANGSPUNKTE UND VERBINDUNGEN

iPassConnect ist ein Client, der für alle Verbindungen verwendet werden kann – ob öffentlich oder privater Zugangspunkt, ob über das iPass Netz oder andere Netzwerke. Indem Unternehmen ihren remote arbeitenden und mobilen Mitarbeitern iPassConnect zur Verfügung stellen, können diese die verschiedenen Zugangstechnologien - öffentliche WLAN Hotspots, unternehmenseigene WLANs, private WLANs, Mobilfunknetze, Ethernet, usw. - einfacher erkennen und nutzen. Dadurch wird die Verbindung mit dem Internet und dem Firmennetz noch einfacher, während zugleich Sicherheitsvorgaben automatisch eingehalten werden und Zugangs- und Support-Kosten sinken.





Nutzen Sie die Vorteile der folgenden iPassConnect Zugangsfunktionen:

Mittels der Funktion zur **drahtlosen Netzerkennung**** erkennt iPassConnect automatisch alle WLAN- und Mobilfunknetze, die sich in Reichweite des Nutzers befinden. Hierzu zählen auch öffentliche Hotspots und Ethernet Verbindungen, sobald ein Netzkabel mit einem aktiven Ein-/Ausgang verbunden ist.

VORTEILE VON iPASSCONNECT:

Universal Client

- Mobile Mitarbeiter nutzen einen Client zum Netzzugriff – unabhängig davon, welche Zugangstechnologie sie verwenden
- Erkennt Ethernet, WLAN- und Mobilfunknetze automatisch und benachrichtigt die Nutzer, wenn Netze verfügbar sind
- Bietet die Möglichkeit der automatischen Verbindung mit präferierten Netzen, wie dem unternehmenseigenen oder einem privaten WLAN
- Unterstützt Nutzer, eine Verbindung zu einem iPass-fremden WLAN Hotspot herzustellen, wobei ein Webbrowser und das VPN automatisch gestartet werden können

Optimierte Anmeldung im Netz

- Standort-basierte Suche zeigt alle verfügbaren Zugangsoptionen auf
- Schneller Zugriff über die Taskleiste auf Breitbandnetze und Standorte, die mit einem Lesezeichen versehen wurden
- Integration mit führender VPN-, Personal-Firewall- und Anti-Virus-Software vereinfacht den Verbindungsprozess
- Windows Live Logon bietet Nutzern die gleiche Erfahrung für die Anmeldung an der NT Domäne, ob im LAN oder beim mobilen Zugriff

End-to-End-Sicherheit auf Richtlinienbasis

- Setzt die Sicherheit der Verbindungen über VPNs, Personal Firewalls und Anti-Virus-Software durch
- VPN-Enforcement gewährleistet, dass nur Geräte auf das Unternehmensnetz zugreifen können, die alle geltenden Richtlinien erfüllen
- Durch Integration mit dem optionalen Device Management™-Service wird eine automatisierte Analyse und Schwachstellenbehebung mobiler Endgeräte erreicht

Senkung der Betriebskosten

- Niedrigere Kosten für Support und Schulung
- Schnelle und flexible Implementierung
- Kostenkontrollmechanismus für verschiedene Zugangstypen
- Eine Rechnung für alle Zugangsoptionen und Unterstützung einer Kostenstellenabrechnung
- Windows-, Mac-, Windows Mobile und Symbian für Nokia Smartphones-Unterstützung

Durch die **Unterstützung iPass-fremder Netze*** wird das Finden eines lokalen WLAN-Hotspots oder einer Mobilfunkverbindung noch einfacher. iPassConnect erkennt alle verfügbaren Mobilfunknetze, einschließlich iPass-fremder Netze, und zeigt diese automatisch an. Wenn ein iPass-fremdes Netz eine weitere Authentifizierung erforderlich macht, startet iPassConnect automatisch einen Webbrowser und das VPN.

Durch die Möglichkeit, über iPassConnect auf **Mobilfunknetze*** zuzugreifen, stehen Nutzern noch mehr Verbindungsoptionen zur Verfügung. Mit einer Reihe von Mobilfunk-Karten kann über iPass sowie Mobilfunkbetreiber sicher und einfach auf das Internet und Unternehmensnetz zugegriffen werden.

On-Campus Roaming ermöglicht die Integration von unternehmenseigenen WLANs, so dass Anwender die gleiche Nutzererfahrung haben, egal ob sie den Zugang auf dem Bürogelände oder von einem anderen Ort aus aufbauen. Bezüglich der firmentypischen zertifikatsbasierten Authentifizierung durch 802.1x bestehen mit EAP-TLS und PEAP-TLS nun zusätzliche Optionen für einen einfachen Userzugang.

Personal Wireless Support* vereinfacht den Zugriff auf die steigende Anzahl privater WLAN-Zugangspunkte. Nutzer können private Netze zu ihrem iPassConnect-Verzeichnis hinzufügen, wobei diese automatisch erkannt und die Netzwerkkarte entsprechend konfiguriert wird.

Indem **drahtlose Netze in einer bestimmten Reihenfolge*** angezeigt werden, ist der Nutzer in der Lage, das jeweils beste Netz auszuwählen. Dabei werden die „Enterprise Ready“ WLAN- und Mobilfunknetze nach Zuverlässigkeit priorisiert aufgelistet und mit einem iPass-Symbol gekennzeichnet. Andere zusätzlich verfügbare WLAN-Netze sowie die Signalstärke aller erkannten Standorte werden ebenfalls angezeigt.

AUTOMATISIERTE UND KOMFORTABLE ANMELDUNG

iPassConnect wurde unter der Prämisse entwickelt, dem Nutzer eine optimale und intuitive Anwendung zu bieten. Zahlreiche Funktionen des neuen iPassConnect Universal Clients machen es für den Nutzer noch einfacher, eine Verbindung aufzubauen, produktiv zu bleiben und dort zu arbeiten, wo er gerade ist.

Durch den **WindowsLive Logon*** steht Remote-Nutzern die gleiche Funktionalität wie im Büro zur Verfügung. Nutzer von Windows 2000 und Windows XP profitieren von der Erstellung von Domänen-Anmeldeskripts, von Funktionen für eine nutzerdefinierte Laufwerkszuordnung sowie von einem automatischen Hinweis, bevor das Domänenpasswort abläuft.

System Tray Launch* ermöglicht es Nutzern, über ein iPass-Symbol in der Taskleiste eine Verbindung zu verfügbaren Breitband-Zugangspunkten und mit einem Lesezeichen versehenen Standorten herzustellen.

Automatische Verbindung zu bevorzugten Netzwerken vereinfacht den Verbindungsprozess mit bestimmten vorab definierten Netzen, indem der Zugang zu präferierten Netzen (private WLANs, Firmen-WLANs und 802.1x Ethernet-Verbindungen) automatisch hergestellt wird.

Die **Standort-basierte Suche**** ermöglicht eine schnelle und einfache Wahl der optimalen Verbindung für jeden beliebigen Standort. Dabei werden die verfügbaren WLAN Hotspots und Ethernet-Verbindungen

automatisch angezeigt. Bei Eintritt in einen Standort werden alle lokalen Zugangsoptionen bereitgestellt.

VPN Autoconnect und Flexible Launch* - iPassConnect kann den Nutzernamen und das Passwort automatisch an den VPN-Client übergeben, wenn eine Verbindung aufgebaut wird. Sollten sowohl SSL und IPSec basierende VPNs verfügbar sein, wählt iPassConnect die beste VPN-Option basierend auf dem gewählten Verbindungstyp automatisch aus.

Updates im Hintergrund - das iPass Verbindungsverzeichnis ist mit Hilfe dieser Funktion stets aktuell, selbst wenn der iPassConnect Client länger nicht verwendet wurde. Die automatischen Updates finden regelmäßig statt, unabhängig von der gewählten Verbindungsart. So wird das Verbindungsverzeichnis auch aktualisiert, wenn der Nutzer mit dem LAN im Büro verbunden ist, solange iPassConnect im Hintergrund aktiv ist.

END-TO-END-SICHERHEIT AUF RICHTLINIENBASIS

Wenn mit iPassConnect eine Internetverbindung aufgebaut wird, gewährleistet iPass, dass das Endgerät geschützt ist bevor eine Verbindung zum Unternehmensnetz hergestellt wird. Die zunehmende Mobilität der Anwender und vielfältige Verbindungstypen machen diese Sicherheitsanforderung für den Netzzugang unbedingt erforderlich.

Zentrale Management Richtlinien ermöglichen es den IT-Mitarbeitern, die erforderliche Sicherheit des Clients problemlos zu definieren und an die iPass-Nutzer zu verteilen, so dass bei jeder Anmeldung die neuesten Richtlinien durchgesetzt werden. Hierzu zählen Richtlinien bezüglich der Verwendung des Netzwerkzugangs und von verschiedenen Zugriffsmethoden, bezüglich der Security Software der Endgeräte, des Vorhandenseins von Betriebssystem-Patches, deren Version und Konfiguration.

Sicherheitskompatibilität mit Drittherstellern - wird über die iPass Alliance™ mit Technologiepartnern erzielt. Diese Partnerschaften ermöglichen die Integration von iPassConnect mit den Sicherheitslösungen führender Anbieter, einschließlich VPN-, Personal Firewall-, Intrusion Detection- und Anti-Virus-Software. Dies hat zweierlei Vorteile: Zum einen erhalten Nutzer einen sicheren Zugang und zum anderen wird der Verbindungsprozess vereinfacht.

Pre-Connect Security* - stellt sicher, dass der Nutzer nur dann eine Verbindung zum Internet herstellen kann, wenn Anti-Virus-Software, eine Personal Firewall oder Intrusion Detection-Systeme aktiviert sind. Sollten diese Systeme vor Beginn einer Sitzung nicht aktiv sein, kann iPassConnect die entsprechenden Sicherheitservices automatisch starten, bevor eine Verbindung zum Internet hergestellt wird.

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

Device Protection - ein optionaler von iPass gehosteter Service, integriert die Symantec Sygate Enterprise Protection Firewall mit iPassConnect, wodurch Sicherheitsrichtlinien im Rahmen des Verbindungsprozesses durchgesetzt werden können; Risiken in Bezug auf die Nutzung von Internet, USB-Schnittstellen und so genannter Rogue Applications lassen sich verringern.

Durch die **VPN-Enforcement-Funktion***** - kann die IT-Abteilung sicherstellen, dass nur Geräte, die festgelegte Sicherheitsstandards erfüllen, eine VPN-Verbindung zum Unternehmensnetz herstellen können. In Verbindung mit dem DeviceID™-Service kann iPassConnect verwendet werden, um den VPN-Zugriff zu steuern. In Kombination mit dem Device Manage-

ment-Service können zudem Security Software und Betriebssysteme vor dem Starten des VPNs aktualisiert werden. So lassen sich Richtlinien durchsetzen, ohne dass die Geräte vom Netz ausgesperrt werden müssen.

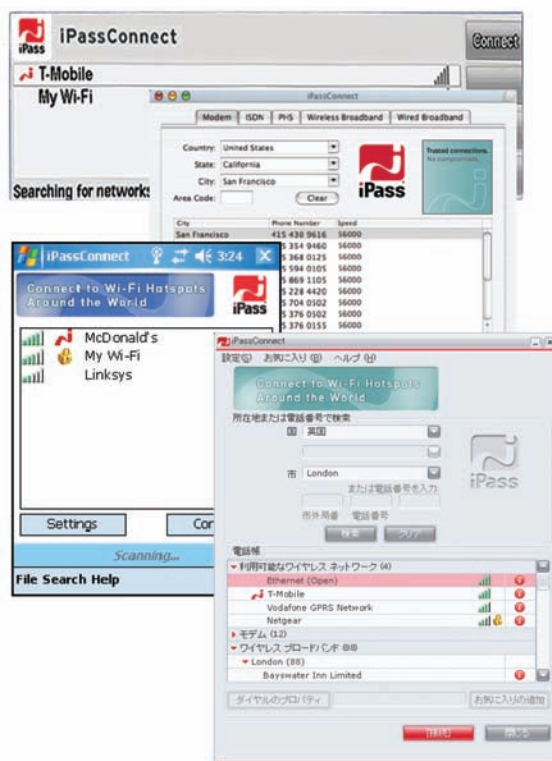
Secure Wi-Fi Networking - bietet durchgehend sichere Verbindungen über öffentliche und private Netze. Zugangsanbieter im iPass Netz authentifizieren Hotspots durch den Austausch digitaler Zertifikate, bevor eine Verbindung aufgebaut wird. Für Verbindungen mit unternehmenseigenen und privaten WLANs, bieten die Protokolle WPA2 und WPA1 Sicherheit, insbesondere über 802.1x Verbindungen. Zudem werden TKIP und AES Pre-shared Keys unterstützt.

Encrypted Login* - schützt die Kennwörter vom Client bis hin zum Unternehmensserver über drahtgebundene und WLAN-Zugänge. iPassConnect verwendet eine komplexe „Public-Key“-Kryptografie, um Kennwörter zu schützen. Indem jeder Sitzung eine eindeutige ID zugewiesen wird, lassen sich zudem Replay-Angriffe verhindern.

SENKUNG DER BETRIEBSKOSTEN

iPassConnect bietet umfassende Kontrollmöglichkeiten, ohne dabei kompliziert zu sein. Der iPass-Service erleichtert Nutzern das Herstellen von Verbindungen, bietet Administratoren einfache Verwaltungsmöglichkeiten und stellt darüber hinaus zusätzliche Funktionen zur Kostensenkung bereit.

Die **qualitätsbasierte Sortierung im Zugangsverzeichnis** überprüft automatisch bei jeder hergestellten Verbindung, ob ein aktualisiertes Verzeichnis der Zugangspunkte vorhanden ist. iPass fügt häufig neue Zugangspunkte hinzu und entfernt



iPassConnect Software-Client für verschiedene Endgeräteplattformen. Von vorne nach hinten: iPassConnect 3.5 für Windows, iPassConnect 3.1 für Windows Mobile 5, iPassConnect 2.4 für Mac OS X und iPassConnect 1.0 für Symbian (Nokia Communicator)



problematische. Durch diese Funktion stehen den Nutzern immer die aktuellsten Nummern zur Verfügung, die entsprechend der gemessenen Zuverlässigkeit aufgeführt sind. So ist gewährleistet, dass alle Verbindungen erfolgreich hergestellt werden können.

Die so genannte **intelligente Einwahl** hilft, die Anrufe beim Help-Desk deutlich zu reduzieren. Nutzer können innerhalb der USA nach einer lokalen Zugangsnummer suchen. Die Zugangsnummern werden automatisch nacheinander aufgerufen, bis eine erfolgreiche Verbindung hergestellt ist. Dabei werden Vorwahlen automatisch hinzugefügt und internationale Einwahlregeln korrekt angewendet. In ihrer Gesamtheit tragen diese Funktionen zur Zeitersparnis bei und machen die Endanwendererfahrung noch besser.

Universal All-Cities Nummern, die in bestimmten Regionen zur Verfügung stehen, sind preiswerte, landesweit verfügbare 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 nicht für unbestimmte Zeit geöffnet bleiben. Damit wird sichergestellt, dass der Zugriff nur für die Zeit berechnet wird, in der der Nutzer den iPass-Service tatsächlich verwendet.

Mittels der Funktion **Gebührenabrechnung nach Kostenstelle** können IT-Abteilungen problemlos Rückschlüsse auf die Nutzung ziehen, indem Nutzer den entsprechenden Abteilungen, Projekten oder Domännennamen zugeordnet werden. Zudem ist es möglich, eine Firmenkreditkarte mit den

Verbindungsgebühren zu belasten. Dies vereinfacht die Verwaltung von Kosten und Kostenstellen.

iPass Connect lässt sich **einfach anpassen**. Dabei besteht eine Vielzahl von Optionen, die größte 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 eigene Firmenlogo und die Nummer des firmeninternen Help-Desks angezeigt wird.

NETZZUGANG FEST IM GRIFF

Mit sicheren, einfachen und effektiven Zugängen bleiben Remote-Mitarbeiter und mobile Nutzer produktiv, während das IT-Personal in punkto Sicherheit unbesorgt sein kann. iPassConnect ermöglicht dies unabhängig davon, ob die Nutzer von unterwegs, von zu Hause oder aus dem Büro auf das Unternehmensnetz zugreifen.

Unter www.ipass.de erfahren Sie, warum sich immer mehr Global 1.000-Unternehmen für iPass entscheiden, um die Verbindung mit ihren Remote- und mobilen Mitarbeitern sicherzustellen, so dass diese produktiv bleiben können, wo immer sie gerade sind. ■

KOMPATIBILITÄT UND SYSTEMANFORDERUNGEN

Der iPassConnect-Client ist kompatibel mit den IT-Security-Produkten der folgenden führenden Hersteller (eine Liste der einzelnen Produkte ist unter www.ipass.de abrufbar). Der iPassConnect-Client ist in den unten aufgeführten Sprachversionen erhältlich und unterstützt die folgenden Plattformen.

VIRTUAL PRIVATE NETWORKS

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

PERSONAL FIREWALLS UND INTRUSION DETECTION SYSTEMS

- Check Point/Zone Labs
- Internet Security Systems
- Symantec/Sygate

ANTI-VIRUS-SOFTWARE

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

UNTERSTÜTZTE PLATFORMEN

- Windows XP und Windows 2000
- Windows Mobile 5 und Windows Mobile 2003

- Symbian für Nokia Smartphones (auf ausgewählten Endgeräten, darunter 9300, 9300i, E60, E61, E70, N80)

- Mac OS X (ab Version 10.2, einschließlich Intel Mac)

UNTERSTÜTZTE SPRACHEN

- Englisch
- Französisch
- Deutsch
- Japanisch
- Portugiesisch (Brasilien)
- Koreanisch

- Chinesisch (vereinfacht & traditionell)
- Spanisch

iPassConnect für die Benutzeroberflächen Mac und Symbian stehen nur auf Englisch zur Verfügung.

iPassConnect für Windows Mobile ist auf Englisch, Deutsch und Japanisch verfügbar.

* Wenn nicht gegenteilig erwähnt, steht diese Funktion ausschließlich in iPassConnect für Windows zur Verfügung.

** Verfügbar unter iPassConnect für Windows und und iPassConnect für Symbian (Nokia Smartphones).

*** iPassConnect für Windows und DeviceID-Integration erforderlich. Device Management Integration optional.

iPass Deutschland GmbH
Wiener Platz 7 / RG
D-81667 München

+49 (0)89 44 142 – 100
+49 (0)89 44 142 – 111 fx

www.ipass.de

