

iPass® Mobile Data

Vertrauen Sie Verbindungen über Mobilfunknetze

- **Ermöglichen Sie eine einheitliche Nutzererfahrung über sämtliche Verbindungstechnologien hinweg**
- **Setzen Sie die Verwendung von Endpoint Security Produkten auch bei Verbindungen über „Mobile Data“ (Mobilfunknetze) durch**
- **Überwachen Sie die tatsächlichen Verbindungen der Nutzer, um die Kosten für Help Desk und Fehlerbehebung zu senken**

Die Mitarbeiter von heute müssen unterwegs von fast überall auf ihre Daten zugreifen können und nicht nur, wenn ein Einwahlanschluss in der Nähe ist oder sie sich gerade innerhalb der Reichweite eines Wi-Fi-Hotspots befinden. Immer mehr Firmen suchen die Antwort bei UMTS, CDMA2000 und anderen neuen Mobilfunknetz-Technologien.

Sollen auch Mobile Data-Verbindungen dafür sorgen, dass die Produktivität des Personals erhöht wird, ohne die Sicherheit oder IT-Ressourcen zu gefährden, muss auch dieser Zugang zum Unternehmensnetz effizient verwaltet werden. Dafür wird eine Lösung benötigt, welche die verschiedenen Zugangsmöglichkeiten zusammen mit den Sicherheitstechnologien in einem einheitlichen Service mit leicht zu bedienendem Zugriff vereint, der sich noch dazu problemlos verwalten lässt. Und genau das bietet iPass® Mobile Data.

Einheitliche Verbindungen – egal ob über Mobilfunk oder WLAN

iPass® Mobile Data verbindet die Nutzer über den von Mobilfunknetzbetreibern bereitgestellten Zugang einfach und sicher mit den Unternehmensdaten. Remote-User und mobile Mitarbeiter können jetzt mit dem iPassConnect™ Universal Client auf eine ganze Reihe von Mobilfunk-Technologien zugreifen, die breitbandige Datenverbindungen bereitstellen.

iPass stellt den Nutzern „Mobile Data“ über den gleichen Universal Client bereit, den sie bereits durch andere Zugangstechnologien kennen. Außerdem lässt sich iPass® Mobile Data mit Produkten von führenden Herstellern zur Sicherung von Endgeräten integrieren, wie VPNs, persönliche Firewalls und Anti-Virus-Software. Die IT-Manager können so auf eine potentielle Bedrohung der Netzwerksicherheit durch reisende Mitarbeiter reagieren, die veraltete Security Software verwenden.

Universeller Zugang – ein Client

Mit dem iPassConnect™ 3.3 Universal Client bindet iPass den Mobilfunkzugang in die Benutzeroberfläche ein, auf die bereits Nutzer und IT-Personal hinsichtlich der gesamten Einwahlverbindungen und Wi-Fi-Zugang bereits vertrauen. Dies führt zu einer einheitlichen Umgebung, die die Produktivität der Mitarbeiter aufrechterhält, während die Supportkosten gleichzeitig sinken. iPassConnect™ mit Mobile Data bietet darüber hinaus:

- **Automatische Geräteerkennung:** Ermöglicht ein „Plug and Play“, ohne dass die Nutzer den Namen oder den Typ der unterstützten Mobile-Data-Karte kennen müssen.
- **Automatische Netzerkennung:** Gibt sofort Auskunft darüber, welche Optionen für die Mobile Data-Netze zu einem beliebigen Zeitpunkt verfügbar sind.
- **Automatische Konfiguration der Netzkarte:** Kein Ärger mit der Kartenkonfiguration. Sobald ein Nutzer mit einer unterstützten UMTS Datenkarte ein verfügbares Mobilfunknetz auswählt, erledigt iPassConnect™ den Rest.

Erweiterte Sicherheitsrichtlinien

Mit den Funktionen von iPass Policy Orchestration wird die proaktive Verwaltung von Sicherheitsrichtlinien für Endgeräte endlich Wirklichkeit. Diese Funktionen ermöglichen es dem IT-Personal, die gleichen Sicherheitsrichtlinien für den Zugriff mit „Mobile Data“ durchzusetzen, die auch für den Aufbau von Verbindungen über andere Netztechnologien gelten. Mit „Endpoint Policy Management“, einem optional von iPass betriebenen Service, kann das IT-Personal die richtige Konfiguration und Nutzung der Sicherheitssysteme problemlos durchsetzen.

- **Kontrollierte Verwendung der Security Software für Endgeräte:** Stellen Sie sicher, dass VPN, Personal Firewall und Anti-Virus-Software vor dem Aufbau einer Internet-Verbindung gestartet werden und während der gesamten Sitzung aktiv sind.



- **Erzwingen von Software-Updates:** Stellen Sie sicher, dass Systeme, die nicht auf dem neuesten Stand sind, aktuelle Sicherheits-Patches für das Betriebssystem und Aktualisierungen der Anti-Virus-Software erhalten, bevor sie auf das Netz zugreifen dürfen.
- **Zentrale Verwaltung der Richtlinien Einhaltung:** Automatisieren Sie die Patch-Verwaltung von Windows und die Aktualisierung von Anti-Virus-Software, während gleichzeitig detaillierte Prüfberichte bereitgestellt werden.
- **Sichere Verbindungen ohne Eingriff des Nutzers:** Aktualisieren Sie die Security Software automatisch ohne Einflussnahme des Nutzers, sodass die mobilen Mitarbeiter ungestört weiterarbeiten können.

Prüfberichte über die Service-Qualität und Fehlerbehebung

Eine der Herausforderungen für das IT-Personal besteht darin, in der Lage zu sein, die Servicequalität von Mobile Data Verbindungen zu verbessern. Der iPass® Mobile Data-Service erfasst eine Vielzahl von Informationen zu den einzelnen Verbindungen, einschließlich Erfolg oder Misserfolg beim Aufbau einer Verbindung, Kartenzustandsinformationen und Signalstärke. Diese wertvollen Daten stehen dem Help Desk-Personal über iOQ® (Intelligent Online Quality) zur Verfügung. Dieser optionale Service liefert ausführliche Reports, welche die Fehlerbehebung erleichtern, den Kundendienst verbessern und viele Verbindungsprobleme proaktiv lösen helfen.

Verbindungen mit Vertrauen herstellen

Mit iPass® Mobile Data verfügen Ihre mobilen Mitarbeiter über die breiteste Palette an Verbindungsoptionen verteilt über die größtmögliche geographische Abdeckung. Das bedeutet mehr Produktivität, ohne die Sicherheit des Unternehmens aufs Spiel zu setzen. Entdecken Sie, wie leicht Sie die Strategie für sämtliche Anbindungen innerhalb Ihres Unternehmens auf die Integration von Mobilfunknetzen erweitern können. Besuchen Sie www.ipass.de – oder sprechen Sie noch heute mit Ihrem iPass-Betreuer!

Systemanforderungen

Zum Implementieren von iPass® Mobile Data benötigen Sie lediglich einen Laptop mit Windows XP oder Windows 2000, iPassConnect 3.3 und eine der folgenden unterstützten UMTS-Datenkarten:

GSM (GPRS, EDGE, UMTS)			
PC-Karte	Band	Netz	Betreiber: Getestete Region
Sony Ericsson GC-82	850 MHz	GPRS, EDGE	AT&T: USA
	1900 MHz		Cingular: USA
Sony Ericsson GC-83	850 MHz	GPRS, EDGE	AT&T: USA
	1800 MHz		Cingular: USA
	1900 MHz		Roaming: Großbritannien, Deutschland, Frankreich
Sierra Wireless 750	900 MHz	GPRS	O2: Großbritannien
	1800 MHz		T-Mobile: USA
	1900 MHz		AT&T: USA
Option Globetrotter Tri-band	900 MHz	GPRS	Vodafone: Großbritannien, Deutschland, Frankreich
	1800 MHz		O2: Großbritannien
	1900 MHz		Orange: Großbritannien, Frankreich
Vodafone Option 3G	900 MHz	GPRS, UMTS	Vodafone: Großbritannien, Deutschland, Frankreich
	1800 MHz		
CDMA (1xRTT, CDMA2000)			
PC-Karte	Band	Netz	Betreiber: Getestete Region
Sierra Wireless 555D	1X 800	1XRTT	Verizon Wireless: USA
	1X 1900	CDMA2000	Telecom New Zealand: Neuseeland
Sierra Wireless 550	1X 1900	1XRTT CDMA2000	SprintPCS: USA

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