iPass Sales Playbook for Partners

Enterprise

July 25, 2017

IPASS PROPRIETARY AND CONFIDENTIAL

iPass Corporate Headquarters
3800 Bridge Parkway
Redwood Shores, CA 94065
phone: +1 650-232-4100
fax: +1 650-232-0227
www.iPass.com

Table of Contents

Introduction

This document provides a complete guide to how to sell iPass products and services to enterprise customers.

Customer Segment Definition

Who is your buyer?

Any enterprise of 1,000 employees or above is a possible target for the iPass service. Enterprises with a higher proportion of mobile knowledge workers represent better opportunities to realize the full value of the iPass service.

A large consulting practice is the ideal type of enterprise for the iPass service. Appendix A. – Sub Verticals contains a detailed overview of the management consulting space.

CIOs (Chief Information Officers) and CSOs (Chief Security Officers) of medium to large enterprises are managing a significant change in behavior within their user base. This change is being driven by an increasingly mobile workforce and migration of enterprise apps to the cloud.

Over 40 percent of the apps used by enterprise users will be hosted in the cloud (external to the enterprise) by 2020, and cloud UC (Unified Communications) providers are becoming the default choice for enterprises.

The convergence of a mobile user base and cloud UC apps is resulting in 70% of users of a leading cloud UC solution accessing the service via Wi-Fi.

In supporting the migration to a largely mobile workforce and a wholesale migration of enterprise apps to the cloud, many CIOs and CSOs are facing the following issues and challenges:

Cost

Before mobility solutions untethered workers from their desks, IT costs and specifically communication costs were relatively easy to predict and were largely fixed, with little seasonal variation.

With an increasingly mobile workforce, IT managers can face changes in seasonality based on users consuming a mix of connectivity solutions to maintain contact with their customers and co-workers. In addition, with the adoption of high-performance cloud-based UC solutions, including video conferencing, per-user data consumption is increasing over 25% a year.

IT managers are being driven to provide a mix of cost-effective connectivity solutions for their users while they are mobile, including cellular voice and data, paid Wi-Fi services and Mi-Fi devices. Each of these solutions can present cost-containment challenges to IT managers:

Solution	Provisioned by IT	Purchased by user
Cellular Data	Cost control for domestic usage is possible. For roaming users, costs can be highly variable and difficult to manage.	Unpredictable costs for domestic and roaming users.
Public Wi-Fi	IT organizations generally have no ability to provision public Wi-Fi services.	Highly unpredictable. Most spend is expensed and usage patterns are hard to determine.
Inflight Wi-Fi	IT organizations generally have no ability to provision inflight Wi-Fi services.	Expensive and highly unpredictable costs. Most spend is expensed and usage patterns are hard to determine.
Mi-Fi Devices	Can be provisioned and are reasonably easy to manage as a group. Roaming access is generally not available and results in users using cellular data. Becoming increasingly banned within enterprises due to security issues.	Highly unpredictable. Most spend is expensed and usage patterns are hard to determine.

Summary: none of the solutions above allow enterprise IT managers to effectively manage the costs associated with their mobile workers accessing cloud-based apps.

Worker Productivity

CIOs are tasked with not only reducing costs but with increasing user accessibly and by extension employee productivity. This is certainly the case with employees who generate revenue on a billable hour basis (consultants, lawyers, etc.) and also with users who need to be continually connected (medical professionals, sales people, etc.).

Many connectivity solutions that an enterprise can purchase work in some places but not everywhere. This inevitably leads CIOs to build out a patchwork of solutions that work in most places but seldom everywhere that users need connectivity. Users are left to fill in coverage holes, with a resulting rise in costs and reduction in security. This is a pervasive issue with mobile users who spend a lot of time in the air and choose to either be out of reach or buy a variety of inflight offers on an ad hoc basis. This spend often goes onto credit cards and this ‘black spend’ can be both unpredictable and hidden from scrutiny and oversight.

Security

As workers become increasingly mobile, so does the attack surface that the CSO needs to protect from intrusion. BYOD policies also compound the issue surrounding securing corporate data. Now an enterprise needs to secure more authorized and un-authorized platforms and operating systems. Costs to support a mobile workforce with BYOD policies can rapidly increase IT costs.

In addition to the platform/OS challenges, many connectivity solutions for mobile workers present serious security issues.

Solution	Security Issue
Cellular Data	Highly secure radio bearer (for non-governmental intrusion attempts). Backhaul is still over the public internet and users need to secure connections using a corporate VPN. Cloud solutions will use SSL/HTTPS but still can be spoofed with fake sites/certificates.
Public Wi-Fi, hotels, airports, etc.	Extremely insecure, user data is vulnerable to a wide range of attacks including spoofing/man-in-the-middle attacks.
Mi-Fi Devices	Similar issues to public Wi-Fi. In addition, the devices themselves are increasingly banned for use on enterprise campuses.

Lack of simplicity

The complex blend of connectivity solutions consumed by a mobile workforce places a significant burden on enterprise IT managers. Costs and security vulnerabilities escalate as users become more mobile and apps move to the cloud and there are few effective tools available for IT managers to manage mobile users as a single community. Even users who are on campus networks can be challenging to manage as a community and IT managers face persistent issues with securing user access and providing reliable access to corporate apps, especially to Unified Communication apps.

Qualifying

What are your qualifying questions?

These are open-ended qualifying questions that will stimulate an open dialogue with you prospect.

Question	Background
• What is your mobility strategy?	• Get the customer to outline their challenges in defining and executing their mobility strategy.
• How are your mobile users connecting today?	• What solutions are their users using? What are the pain points for both the users and the IT organization?
• How important is cost containment for connectivity solution?	• Costs to support mobile users are escalating with the increasing adoption of mobile data services and the ever-increasing demand for user data.
• How many of your users are frequent air travelers?	• Many enterprises have a substantial hidden spend associated with inflight users.
• How important is securing corporate data on user devices?	• The risks associated with data loss from mobile users can be very damaging for an enterprise.
• Do you have a BYOD policy?	• BYOD policies can exacerbate security and cost control issues.
• Are your apps moving to the cloud?	• As more apps move to the cloud, more of an enterprise's data is sent over public and potentially unsecured infrastructure.

Solution selling

The solution selling approach detailed below will position iPass as a key asset in an enterprise's strategy.

1. Mobile Worker Productivity

iPass allows mobile workers to stay online for longer, boosting worker productivity. Inflight connectivity provides a game-changing capability that allows workers to recover lost time while flying. Additional productivity improvements are gained by not having workers hunting for mobile access and having to expense connectivity.

2. Security

Data consumption is growing at an unprecedented rate. We are consumers of this data and we are mobile. Content is king. More and more content is available and mobile users want to access it in an unlimited fashion and on multiple devices. However, users face serious and escalating issues around securing their data from malicious attacks. Public Wi-Fi (paid or free) if not properly secured represents a serious vulnerability for attack via multiple vectors, including man-in-the-middle/spoofing and fraudulent SSL credentials. iPass has built a secure Wi-Fi solution that uses multiple techniques to detect and deflect attacks and protecting data passing between a user and an app in the cloud or within an enterprise.

The iPass SmartConnect Wi-Fi service protects mobile users from multiple security threats irrespective of the type of network the user is accessing. These threats include Man-in-the-middle attacks, payload sniffing, spoofing, etc. A user can connect to any type of Wi-Fi footprint (iPass or non-iPass) and be assured that their user credentials and data is safe from attack. iPass uses multiple techniques to secure user connections including:

iPass uses multiple techniques to secure user connections including:

- Detection and blacklisting of rogue/malicious hotspots
- Platform validation
  - The iPass client is connected to valid iPass infrastructure
- Authentication
  - Multi-level
  - Multi-factor
- Encryption of all data
  - At rest – In the cloud and on the client
  - In transit – Control, authentication and user data
- User policy control
  - How and when users connect
- Hardening
  - Client and the cloud infrastructure
  - Continuous penetration testing
- Secure development best practices
  - Threat modeling
  - Static code analysis
  - Fuzz testing

The iPass solution supports access for two primary types of networks: commercial networks requiring user authentication and curated amenity Wi-Fi where user authentication is not required.

On commercial networks where authentication is required, iPass certifies that each of its 160 commercial network partners is using verifiable SSL certificates to encrypt authentication traffic. Going above this industry standard to provide enhanced credential security, iPass employs a password encryption technique called iSEEL, which utilizes 131-bit Elliptical Curve Cryptography, the user password string, a

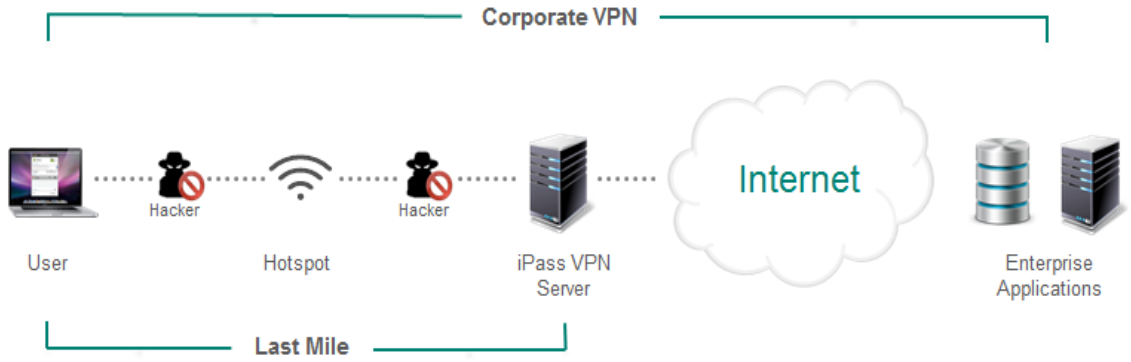
unique Client ID and a session counter to encrypt the user's password between the client connection manager app and the iPass transaction network core, at which point all authentication traffic is protected by SSL VPN tunnels.

For both commercial networks and curated amenity Wi-Fi networks where no user identity is required, iPass offers an integrated VPN service to protect data over the air and through the visited Wi-Fi network to an iPass-hosted termination point on the internet.

As iPass network partners continue to deploy 802.1x roaming support across their networks, iPass will take advantage of this and the associated EAP (Enhanced Authentication Protocol) methods to provide industry standard credential and data security over the air interface.

iPass can optionally activate its last mile VPN service for enterprise users. This capability is invoked as part of the connection sequence and does not require any user intervention.

The last mile VPN secures both a user's data and their sign in credentials – see below.



3. Simplicity

Reliable and efficient iPass is simple to deploy and manage even at large volumes.

For the IT manager, iPass provides powerful cloud-based tools to manage user experience, including all aspects of provisioning and managing enterprise users.

Costs are predictable with no overage charges, irrespective of how or where users consume the service. Users can activate the service on any device which allows BYOD models to be easily supported.

4. Cost Containment

iPass provides enterprises with access to the world's largest Wi-Fi network. With more that 60 million Wi-Fi hotspots globally, iPass provides connectivity in hotels, airports, restaurants, shopping centers and residential/community areas on the ground as well as in the air.

Patented iPass SmartConnect technology delivers the global Wi-Fi service to smartphones, tablets and laptops, running in the background to connect users automatically to Wi-Fi, whenever one of our millions

of hotspots is in reach. Once the user is registered, he or she never again needs to log in, provide credentials or authenticate.

iPass pricing provides a predictable OPEX model, based on unlimited data use, unlimited devices and unlimited connection time for a fixed monthly price. The iPass pricing model is based on fixed cost/per user, which removes the risk associated to capacity usage explosion, fueled by data hungry cloud and mobile applications.

iPass Unlimited includes an option for global inflight access, which allows cost containment and control for a mobile workforce.

Success Stories

These success stories are for internal use only and are not to be used as reference accounts.

McKinsey&Company

McKinsey&Company is a leading global management consulting firm. Founded in 1926. McKinsey&Company employs 25,000 people in 110 offices around the world and in 2015 generated $8.4 billion in revenue.

McKinsey&Company is a decentralized organization with a highly mobile workforce. Their consultants spend a considerable amount of their time travelling:

- $1B/annual spend on travel
- 1,000,000 flight segments a year
- 3rd largest travel spend in the U.S. (behind IBM)

This level of travel has impacted worker productivity, reduced the billable hours for each consultant and negatively impacted the work/life balance of their employees.

McKinsey & Company selected iPass to provide an end-to-end connectivity solution for their employees providing seamless connectivity. McKinsey & Company is targeting 2-4 hours a week of increased productivity and improved quality of life for their employees.

In addition to terrestrial Wi-Fi access, cost-effective inflight Wi-Fi access for their core consulting group (over 4,500 consultants) allows McKinsey & Company to ensure that their consultants are always available. This allows McKinsey & Company consultants to work on customer accounts and generate increased, verifiable billable hours.

In addition to offering a compelling ROI, the iPass product provides a simple and predictable cost model for the IT management team.

Scandinavian Airlines

SAS has introduced an Electronic Flight Bag (EFB) for their flight crews. The existing flight bags contained all the navigation charts, operating manuals and paperwork for the crews to operate SAS routes with the aircraft that they are certified to operate. The EFB initiative allows SAS to make sure that their crews do not have to carry heavy bags of manuals and charts around and ensures they always have access to the most up to date charts, manuals and paperwork. In addition, SAS can realize fleet-wide fuel cost savings by reducing the weight of paper carried on board their fleet. The EFB is tablet based and SAS was using 3G connectivity to keep each tablet up to date.

Before iPass SmartConnect:

- Roaming costs prohibitively expensive
- Unreliable network signals from 3G roaming
- Poor user experience

After iPass SmartConnect:

- Reduces fuel costs
- Cuts mobile costs
- Increases connection reliability and enhances user experience
- Improves employee productivity
- Keeps pilots and crews better connected

Objection Handling

Objection	Response
• My users use cellular data and are on unlimited plans	• iPass supports every device your users carry while they are mobile not just cellular devices. • iPass is available in places that places that cellular doesn't reach including aircraft. • Most unlimited cellular plans are not completely unlimited and generally include some type of overage. iPass usage is completely unlimited, including on aircraft. You will never be charged overage. • Cellular data still has roaming charges which, can easily double a cellular bill. iPass eliminates these roaming charges.
• Additional, unpredictable costs	• iPass Unlimited is billed as a flat monthly fee per user. The amount will not vary based on usage or number of devices a user may use to connect to the service.
• Wi-Fi isn't secure	• iPass SmartConnect provides a multi-layer defense against attacks including: ○ Detection or rogue hotspots

	○ Multi-level authentication ○ Corporate VPN or integrated last mile VPN ○ User policy control ○ Hardened software in both the client and the cloud infrastructure
• I use Mi-Fi type devices	• Many Mi-Fi devices have well known security exploits which will leave user data exposed. This is especially the case for devices which are not carefully configured and use default settings. Mi-Fi devices do not work on aircraft.
• I don't need more stuff to manage	• iPass incorporates simple user management tools which allow management of large user bases with minimum overhead. No ongoing maintenance or management of users is required. In addition, user credentials can be provisioned via API, SSO or synchronized with On-prem AD servers to easily automate provisioning/de-provisioning users.
• Might require user training	• iPass is simple to install and use. Users can sign up for service via an optional company branded sign up page. Once signed up, a user can be activated by simply downloading the client for the platform and clicking on an activation url sent to their e-mail address. In addition, iPass can provide user training and adoption tools for enterprise IT admins to allow them easily on-board thousands of users.

Setting Expectations for the Customer Experience

Your prospects are not Wi-Fi experts. They don't know all that you know, and they certainly don't know iPass. Letting them know what to expect from the customer experience is half the battle, otherwise, prospects will harbor unrealistic expectations:

- iPass will replace home internet
- iPass will connect where there is no hotspot
- iPass can control the quality of the hotspots
- iPass will have a 100% connection success rate

Your responsibility is to set expectations during the pre-sales process, that Wi-Fi is inherently error prone:

- Users are prone to error
- Authentication may fail
- Onboard equipment can fail
- Packets can drop
- Free, public Wi-Fi is not secure
- Quality and availability are never a given

In the addendum, you'll find materials that comprehensive outline how to set customer expectations for the customer experience.

Understanding the iPass Product

The iPass SmartConnect Wi-Fi Service

Today, Wi-Fi is so pervasive, that users tend to notice it only when it's not available. In many places, Wi-Fi has become an equally important mobile data technology to cellular. For instance, mobile device users throughout Southeast Asia routinely spend more than half of their time connected to Wi-Fi. In China, users spend nearly two-thirds of their time connected to Wi-Fi.

Wi-Fi versus Cellular

Wi-Fi operates similarly to cellular, but with a few key differences. Wi-Fi provides local access to the internet like a house, office, coffee shop or airport. Cellular service is usually made available to you from a carrier. Users purchase a cellular plan that entitles you to use a specific amount of data - sometimes that amount is "unlimited". Quite often unlimited isn't really, unlimited.

A cellular signal covers a much larger area than a Wi-Fi signal, more like miles upon miles rather than feet. But what Wi-Fi lacks in reach, it makes up in speed, meaning Wi-Fi is much better than cellular for data-intensive activities, including voice communications, streaming video content, downloading and sharing large data files.

Wi-Fi is also available in places where cellular is not, most notably in airplanes, but also in certain hotels, convention centers and in remote parts of buildings.

As for battery usage, most devices will not use the cellular connection when they are connected via Wi-Fi. When connected to a Wi-Fi network, the device will consume significantly less battery power.

The Role of Free Wi-Fi

Free Wi-Fi does exist; it is available in many coffee shops, airports, hotels, etc. But relying on free Wi-Fi involves a series of significant trade-offs. The most important are security and privacy. By its nature, free Wi-Fi is unsecured, leaving you vulnerable to any manner of security threat, from man-in-the-middle attacks to identity spoofing and tracking by ISPs and other entities. Being completely safe on free Wi-Fi is never a given, especially in crowded venues like airports and hotels, as anyone can gain access to your personal information.

If that's not bad enough, the experience of connecting to most free Wi-Fi hotspots is pretty poor. Speeds tend to be sluggish at best, and time limits usually apply. And that's when you actually get online, which is no small feat. To do so requires extensive effort and patience, wading through promotional videos and captive login pages.

The Value of iPass to iPass Users

Clearly, consumers rely heavily on Wi-Fi to connect to the internet on mobile devices. And therefore, to get the full benefit of iPass mobile devices, iPass customers need to be able to connect automatically to high quality Wi-Fi, wherever they are. Otherwise, they confront many inconveniences, frustrations and friction points (as shown in the table below,) when they just want to connect.

iPass is a Wi-Fi first connectivity service, available as a native application embedded in select devices. Once downloaded, the iPass app gives iPass customers access to the best possible Wi-Fi connection available while on their device. The iPass app connects customers to the world's largest Wi-Fi network, with millions of iPass-enabled hotspots in more than 120 countries, at airports, hotels, train stations, convention centers, outdoor venues, inflight and more.

The value of the iPass service to iPass customers is that simple, secure, always-on Wi-Fi access enhances their mobile experience, eliminating common frustrations and points of friction.

The Mobile Experience without iPass	The Mobile Experience with iPass
Users must search through network IDs to find an available network connection.	Users connect automatically to the best available hotspot, without manual intervention.
User connection options are limited to Wi-Fi in the home, publically available Wi-Fi, or else you have pay for Wi-Fi when you leave your house.	Users get internet access even at locations that don't offer free Wi-Fi access.
Users are not always certain of the quality of the hotspot to which they are connecting. This often results in an unstable connection.	Users connect to hotspots that have already been vetted for quality. Generally, upload and download speeds will be consistently higher than cellular connections.
Users need to pay for Wi-Fi in certain airports and hotels as well as in other locations.	Users no longer need to pay extra for Wi-Fi, where the iPass global footprint is available.
To connect to public Wi-Fi, users are forced to watch ads, give out personal information, and often pay to stay online after a certain period of time.	Users don't have to wait through ads, give out personal information, or pay to stay online.
Users generate cellular roaming fees.	Users do not generate cellular roaming fees.
Users have to deal with Wi-Fi login screens in a foreign language.	Users do not have to deal with foreign-language login screens.
To access inflight Wi-Fi, users need a credit card, which could be stuck in the overhead bin.	Users connect without a credit card.
Users rarely or never access Wi-Fi in non-stationary locations.	Users get Wi-Fi on trains, buses, planes, etc.

About iPass and iPass SmartConnect

iPass is a leading provider of global mobile connectivity, offering simple, secure, always-on Wi-Fi access on any mobile device. The iPass solution is built on a software-as-a-service (SaaS) platform, which allows iPass to keep its customers securely connected by providing unlimited Wi-Fi connectivity on an unlimited number of devices.

iPass provides the world's largest Wi-Fi network, with more than 60 million hotspots in more than 120 countries, at airports, hotels, train stations, convention centers, outdoor venues, inflight, and more. Using patented technology, iPass takes the guesswork out of Wi-Fi connectivity, automatically connecting iPass subscribers to the best Wi-Fi hotspot for their needs.

iPass' structured approach is based on three pillars:

- **Unlimited -** provides unlimited Wi-Fi access to over 60 million hotspots in airplanes, hotels, trains, cafes and other key, public venues worldwide.
- **Everywhere -** addresses our goal to continue to have the world's deepest and broadest global Wi-Fi coverage to create a "cellular-like" model for Wi-Fi global access.
- **Invisible -** allows us to provide the richest Wi-Fi connection experience via a secure, intelligent, seamless platform called iPass SmartConnect.

iPass has forged partnerships with over 160 network providers worldwide and continue to focus on footprint growth in the venues that matter. We also deliver our everywhere promise through key strategic partnerships with large MNOs, OEMs, etc., where iPass is the ubiquitous technology for Wi-Fi connectivity. iPass has stated publicly that its goal is to be accessible on 1 billion devices by the end of 2017. And we are well on our way to achieving that goal.

iPass Invisible leverages our rich patent portfolio to deliver iPass SmartConnect™ allowing us to provide the richest customer experience on the market today. In addition to making the product invisible, iPass SmartConnect also allows seamless connection management between Wi-Fi and cellular data services. New technologies can be integrated as they emerge allowing partners to leverage the power of iPass SmartConnect in their own applications.

The iPass Developer Program enables developers to access to the iPass SmartConnect Software Development Kit (SDK). The SDK has already been deployed by a number of large brands in the MVNO, MNO and applications verticals

In April 2016, the Company announced iPass Veri-Fi™, a big data and analytics service providing in-depth insight into the worldwide connectivity map, connection reliability, Wi-Fi traffic patterns and much more. Veri-Fi can be used by operators to drive significant improvements in user experience, footprint acquisition decisions and operations costs. In addition, Veri-Fi enables new big data-based applications focused on user location and behavior.

Historically, iPass' go-to-market strategy focused on the large enterprise customer segment and over 500 of the Fortune 1000 enterprises are iPass customers with a total of over 900 customers worldwide.

We deliver iPass service to users in two ways:

1. Via a native client application that runs on iOS, Mac, Windows, Android. The application runs on laptops, smartphones and tablets where a customer can simply download the application with a single click to authenticate to the service. iPass leverages our iPass SmartConnect SDK to build our client application.

2. Via our iPass Software Development Kit (SDK) allowing third parties to build iPass capabilities into their application. The SDK can be integrated into iOS and Android. Windows support is currently in beta test.

iPass SmartConnect™ in detail

- Identifies the best hotspots – SmartConnect™ uses advanced analytics to identify and rank access points based on factors such as signal strength, speed, bandwidth availability, and connection success rate. This allows us to blacklist and whitelist the access points for an ALWAYS BEST CONNECTED experience.
- Automatically connects our customers to the best hotspot for their needs - iPass SmartConnect's self-learning algorithm continuously improves its knowledge of global Wi-Fi networks, allowing iPass to select the optimal Wi-Fi networks in real time. Once a customer connects to iPass, they will keep connected to the best Wi-Fi networks.
- Connects our customers securely - As part of iPass SmartConnect™, the iPass Last Mile VPN (Virtual Private Network) connects our customers securely where their data is most vulnerable: between the customer and iPass' secure Internet gateway.
- Adds new hotspots where customers need them most - iPass SmartConnect™ identifies hotspots both inside and outside the iPass network, enabling iPass to pinpoint the most popular hotspots globally. With this visibility, iPass can add new hotspots based on where users need them most.
- Reduces costs through optimal cost routing - iPass SmartConnect™ allows iPass to route traffic over the most reliable and cost-effective networks based on user needs.

Wi-Fi Footprint – The Largest and Growing

iPass provides a secure and easy way to connect to Wi-Fi on more than 60 million hotspots around the world, in airports, trains, hotels and airplanes, but also in your local café or retail outlets. With a single click, you are instantly connected to the world's largest and secure Wi-Fi network.

- More than 800 airports
- More than 2,700 airplanes, with even more on the roadmap
- More than 800 trains
- More than 20 million local businesses
- More than 80,000 hotels
- More than 30 million community hotspots

Added security with Last Mile VPN

iPass delivers an advanced security capability through the Last Mile VPN. The Last Mile VPN provides global hotspot security, offering VPN tunneling between the user and iPass' secure Internet gateway, where a user's data is most vulnerable.

Specification	Last Mile VPN
Apps Supported	iOS and Android
Security	256-bit (IPSec/SSL/OpenVPN)
Speed Limit	None
Server Locations	Europe (U.K.), Asia (Singapore), North America (U.S.)
Stability	Reliable and stable, even behind wireless routers on non-reliable networks and Wi-Fi hotspots.
Administration	Easy-to-use, simple solution, single application and MDM integration (Mobileiron).
Data	Transfer unlimited data, encrypted and decrypted at each end, from your mobile devices to our VPN servers around the world, over iPass networks.
Pricing	Included in the subscription price for iPass Unlimited customers for data transferred over the iPass Network.

Reporting

Account administrators can generate self-service reports, which include information critical to businesses.

- Recent connection data
- Connections by location
- Network types
- Number of total sessions
- Number of unique networks
- Number of unique devices by platform
- Top users by location, business group, cost center

iPass Products For The Enterprise

An Enterprise will typically consume the following products:

Standard Product	Description	Medium Enterprise	Large Enterprise
iPass SmartConnect for Enterprise	The core Wi-Fi service provided by iPass will allow Enterprise users to take advantage of high performance Wi-Fi connectivity.	Yes	Yes

Non- Standard Product	Description	Medium Enterprise	Large Enterprise
Veri-Fi Big Data/Analytics	Provides insight into user behavior to allow optimization of the iPass service. Can be extended to provide Adtech applications to allow an enterprise to attract and retain customers.	No	Yes

Enterprise Specific Features

These are the standard product features for enterprises. Anything not listed below is deemed as non-standard.

Included capabilities:

Category	Description
Subscriber Registration	Subscriber Registration -via Portal UI or via API
Subscriber engagement	Customer-managed Welcome e-mail (sent by iPass) to registered subscribers. English only, additional email languages require iPass assistance. Multiple devices (if activated) are supported via email mechanism.
Client Software Delivery	iPass-branded Self-Service Activation Page. Branded and/or additional language support on SSA page requires iPass assistance.
Authentication	iPass Hosted Authentication w/ACA. Accounts created via portal UI or API.
Reporting	Standard iPass Reports available on the iPass Portal (via UI or API as applicable)

Reporting	Monthly CDRs (via Portal UI or API as applicable)
Customer Support	Standard iPass support
Wi-Fi Network - Terrestrial	iPass Commercial and Open networks, added to profile and automatically updated. Typically no carve outs.
Wi-Fi Network - Inflight	Available with Unlimited Plus subscription
Time Based Session Limits	4 Hour session limits
Connection	Enable / Disable AutoConnect on iPass networks (Standard is ON) via Portal.
VPN	Last Mile VPN included in entitlement.

Excluded capabilities:

Category	Description
Subscriber Engagement	Customized welcome e-mail to registered subscribers
Subscriber Engagement	Tiny URL support
Client Software Delivery	Client Delivery through supported MDM integration
Location Services	Location Services API
Branding	White Label Client
Branding	White Labeled Hotspot Finder
Connection	Integration with 3rd party VPN or other security Software (Win 32)
Connection	On Campus Corporate Network integration.

Pricing and Packaging

The standard pricing model for iPass Wi-Fi services for Enterprises is as below:

Licensing Model:	Registered user, unlimited usage, unlimited devices.	A registered user is a user who has an account with iPass who may or may not use the service during a billing period.
Pricing:	Per registered user/per month, volume discounts.	Billing is triggered on the 1st of each calendar month. Service is billed in arrears.
Ramp:	Three months to reach MMC target Six months to reach full ramp (M4 25%, M5 50%, M6 100%)	
Network Included:	Unrestricted Terrestrial, All Inflight with Unlimited Plus	

Product SKUs and Coverage

iPass Unlimited

iPass keeps teams connected wherever they are with the iPass Unlimited service. With iPass Unlimited, users have access to unlimited data on unlimited devices. No speed limits, no time limits, no usage limits.

iPass Unlimited is easily downloaded from Apple, Google or Microsoft's app stores. Our easy-to-use app runs on virtually any mobile device: smartphones, tablets and laptops.

iPass Unlimited At A Glance

Feature	Service Capability
Time Limit	Unlimited
Data Limit	Unlimited
Speed Limit	Unrestricted
Platforms supported	iOS, Android, Mac, Windows
Hotspots Coverage	More than 60 Million
Inflight Wi-Fi	Included with Unlimited Plus subscriptions

coverage	
Locations	Planes, hotels, convention centers, airports, trains, cafés and public venues

iPass Unlimited
The customer shall have access to all iPass terrestrial footprint globally including free and paid networks. VPN service will also be included at no charge. Unlimited data and devices.

iPass Unlimited Plus
Customers have access to all iPass terrestrial and in-flight footprint globally (Including United, Gogo and any new providers added over time) including free and paid networks. VPN service will also be included at no charge. Unlimited data and devices.

A customer may order and provision Unlimited and Unlimited Plus users in any combination.

iPass Unlimited Enterprise
The customer shall have access to all iPass terrestrial footprint globally including free and paid networks. VPN service will also be included at no charge. Unlimited data and devices.

Coverage	Unlimited	Unlimited Plus	Unlimited Enterprise
All global terrestrial footprint	Yes	Yes	Yes
All global in-flight footprint	No	Yes	Yes

Minimum Monthly Commits –

On signing the sales order form, each customer will be committing to the following:

- One-year initial term with a one-year renewal.
- A minimum monthly revenue commit based on the quantity of each type of user committed to.

This will determine the monthly minimum dollar amount billed to a customer. A customer may increase the number of registered users at will in the portal. Each user will be billed at the rate set when the initial monthly commit is determined. The rate will not adjust based on increased adoption.

If a customer drops below the initially committed number of users, the customer will still be billed at the initial monthly committed rate.

If a customer wants to take advantage of a lower rate, based on increased usage, the customer must recommit to a new one-year term and a new minimum monthly commit.

Order Process

Unlimited, Unlimited Plus and Unlimited Enterprise will be ordered according to the terms between the Partner and iPass.

Appendix A. – Sub Verticals

Management Consulting:

Management consulting refers to the industry and practice of providing guidance to management in order to improve the performance of organizations. Client organizations are typically businesses, but management consultants also advise governmental agencies and nonprofit organizations.

Reputable management consulting firms have a few similarities; they hire bright people who can think well on their feet, solve problems, communicate in teams, and exhibit professionalism with clients. The workaday experience of the consultant is all about gathering information, synthesizing insights, and communicating solutions.

These consultants tend to spend much of their days in team and client meetings, doing data analysis and creating presentations. Their engagements are intended to provide practical insights and solutions that lead to substantial improvements for client organizations.

Although the categorizations of the management consulting universe are imprecise, nearly everyone practicing management consulting could be classified into one of following: strategy consulting, accounting, IT specialists, boutique consulting, internal consulting, and independent consulting.

Industry Fundamentals:

As of 2014, the U.S. consulting market was the largest in the world, representing 55 percent of the $101 billion global market. The U.S. consulting market is nearly eight times larger than the size of the U.K. consulting market, and more than 11 times larger than the Australian advisory market. Not only is the U.S. market the largest, but it is also one of the fastest growing in Western economies, adding nine percent in 2014. The amount by which the U.S. market grew in 2014 actually equals half of the size of the entire German consulting industry, which is the third largest globally, behind the U.K. Growth in 2015 was also expected to be 10 percent.

Yet the U.S. consulting sector is already relatively mature; it is therefore unlikely that it will continue to grow at emerging market rates into the future**.** However, the U.S. consulting sector is undergirded by solid fundamentals, including strong macroeconomic growth, clients' continued use of consultant services, and technological development, with an emphasis on digital transformation. Of the different segments, growth is highest in financial management and risk consulting (12 percent,) followed by technology (10 percent,) strategy consulting (8 percent,) and operational improvement (7 percent).

Within traditional strategy consulting firms, the share of work that is classic strategy has been steadily decreasing though, and is now about 20 percent, down from 60 percent to 70 percent three decades ago.

The Principal Players in Management Consulting

- McKinsey*
- The Boston Consulting Group*
- A.T. Kearney
- Bain
- Strategy&
- Oliver Wyman
- Deloitte
- Roland Berger
- Accenture*
- IBM Consulting
- E&Y
- Mercer
- Alvarez & Marshall

Industry Challenges

The traditional strategy model, opacity and agility, exemplified by McKinsey, Bain, and BCG (MBB) have steadily eroded. Formerly, a team of high-cognitive overachievers developed frameworks and performed analyses behind closed doors. Today, opacity is not a compelling value proposition. For one, clients are less receptive to a separated working arrangement with their advisors (see: growth in collaboration between client and consultant). Secondly, discretionary spending is highly scrutinized, so there is less appetite for big-ticket consulting contracts, especially outside of the Fortune 500. Finally, novel insights are rare, given the wide availability of information. Thanks to video meeting technology like GoToMeeting, virtual collaboration can be achieved at zero marginal costs. Technology has also created digital communities of experts in every industry, function, and geography; all of which can be accessed easily, cheaply, and speedily.

The forces driving change are many and various. Disruptive technology, the rise of new business models, and the pressures exerted by intense global competition are transforming the marketplace. Five challenges, in particular, stand out:

1. **Attracting and developing new clients**
2. **Dealing with a difficult economy/competitive marketplace**
3. **Finding and keeping good people**
4. **Continuing to innovate**
5. **Strategy/planning issues**

Fifteen Strategic Trends in Consulting

Consultancies are adapting to shifts in client demands; clients are becoming more sophisticated or at least complaining that consultancies are unable to offer value-added services in the midst of rapidly evolving needs and expectations (across industry).

1. **Global focus:** The consulting and IT services industry has become truly global with talent pools strategically located to increase the service provider's competitiveness. Local players will only survive if they anticipate global trends and emerging technologies.

2. **Rapid change in core business**: According to 79% of service providers, the declining core business is changing much faster than anticipated. **This is a major issue for CEOs and heads of business units.**
3. **Clients are confused about their vendor's strategy:** Growing divide between clients and vendors at the senior and middle management level, exacerbated by a lack of communication, has left many clients frustrated by vendor. Clients need vendors to offer clear strategy to support long-term business goals.
4. **Lack of differentiation even among the biggest firms:** Many global consulting and IT service providers are offering essentially the same services. Big global consulting and IT services firms are perceived as "supermarkets" by their clients delivering a wide range of services with very little differentiation.
5. **Outliers in every segment:** Every category has one or two outliers who out-perform their competitors by a significant margin. **These service providers have managed to differentiate themselves in terms of leadership, culture, client engagement, service offering and pricing, business strategy, innovation and people management.** When many are growing below 10%, these outliers are growing at 30% on a multi-billion dollar revenue base.
6. **Selective and modular buying:** Clients are becoming much more selective and modular about what they are buying, often seeking services in smaller well-defined scopes of work. **Large traditional outsourced deals that were once so common are now rare.** An exception to this, however, is the government sector, where large deals are still to be found.
7. **Scale and brand less important:** The importance of scale and brand is decreasing, rewarding newcomers over incumbents. Clients seeking innovative solutions are willing to partner with industry newcomers. Of those questioned, 86% indicated that they were currently exploring partnerships with innovative new companies. In fact, scale can become a major disadvantage if the workforce is not suitably skilled to deliver on client expectations.
8. **Small challenge the big:** Startups and small-to-medium enterprises (SME) will fill the gap and deliver new services to clients where large service providers are unable to meet client expectations. **Speed and flexibility will be important factors in winning work.** About 92% of clients already work with SMEs, whereas 87% support startups through funding and other means.
9. **Market Consolidation:** The industry is reaching a stage where clear differentiation is emerging between high growth companies and their competitors. Market consolidation is occurring in a number of tier two IT services companies that have less than $1B in revenues. Several tier two consulting firms are also experiencing growth challenges, exposing them to acquisition risks in the next 12-24 months as their profits decline.
10. **Too much management, too little leadership:** The senior executive teams of some large consulting and IT service providers are very immersed in the managerial functions of planning, budgeting, organizing, recruiting, and controlling. Leaders growing insularity and failure to understand the significance of current changes poses a risk to the future growth of their businesses.
11. **New entrants are changing business models:** New service providers are already disrupting the industry by delivering services using innovative business models. For example, cloud service providers are attempting to redefine the entire service delivery framework.
12. **Acquisition in lieu of innovation:** Almost all major service providers are actively acquiring new businesses as they are unable to innovate internally. We believe that most of the organizations have declared themselves successful too early without waiting for their expensive acquisitions to yield results. In several cases, we observe acquisitions have failed to produce projected benefits because of cultural differences and a significant exodus of talent from the acquired businesses.
13. **"Short-termism" erodes core business:** A number of large global multinational companies (MNC) are struggling as "short-termism" has permanently eroded the capabilities of these companies combined with limited strategic vision. In comparison, a few IT services companies of Indian origin are actively expanding and hiring high caliber individuals and thus enhancing the incremental value to clients. These service providers pose a serious threat not only to MNCs, but also to elite consulting firms, including the Big Four.

14. **Firms consider alternate business models:** We have identified at least two large consulting firms that are actively developing new business models to compete in the Small to Medium Enterprise (SME) marketplace. If the new models are successful, they have the potential to disrupt the almost 100-year-old consulting and 50-year-old IT services industry.
15. **Co-creation with clients:** Consulting and IT service providers will **increasingly be expected to create solutions in close cooperation with clients**. Elite consulting firms are currently leading the way with co-creation of solutions. This will become a major factor in winning work.

iPass Solves for the Following Problems:

Problem	iPass Solution
• Highly mobile teams, whose highly collaborative work revolves around research, analysis, and reporting (all of which has a digital component).	• Stay connected to our global Wi-Fi footprint, +57M hotspots in more than 120 countries. Including high density of coverage in urban areas where consultants will be on engagement.
• Individual consultants have to always be accessible to clients, partners, and colleagues.	• Stay connected to our global Wi-Fi footprint, +57M hotspots in more than 120 countries. Including high density of coverage in urban areas where consultants will be on engagement.
• Certain billing structures incentivize individual consultants to maximize billable time, especially during previously "dead time," i.e. inflight etc. However, firms are shifting from per-diem billing to value-based pricing.	• Our premium inflight offering, Gogo, Panasonic, United, etc. makes previously "dead time," i.e. time spent on flights, count as billable time.
• Recruitment, even for the biggest firms: the traditional HBS to MBB pipeline is drying up, the top MBAs are increasingly looking towards other career opportunities. • Retention, even prestigious firms suffer from 18 to 20 percent turnover per year.	• Focus on the ease of connectivity; iPass SmartConnect dramatically improves the mobile experience, automatically connecting users to the best hotspot. Users don't have to enter personal information in order to log in.

Big data opportunity in data and analytics-enabled consulting; see: McKinsey Solutions. (From "Consulting on the Cusp of Disruption," *Harvard Business Review*)

THE STEADY INVASION OF HARD ANALYTICS AND TECHNOLOGY (BIG DATA) IS A CERTAINTY IN CONSULTING, AS IT HAS BEEN IN SO MANY OTHER INDUSTRIES.

It will continue to affect the activities of consultants and the value that they add. Average costing and pricing analysis have been automated and increasingly insourced; now Salesforce.com and others are automating customer relationship analysis. What's next?

We believe that solutions featuring greater predictive technology and automation will only get better with time. What's more, data analytics and big data radically level the playing field of any industry in which opacity is high. Their speed and quantifiable output help reduce, and perhaps even negate, brand-based barriers to growth; thus they might accelerate the success of emerging-market consulting firms such as Tata Consultancy Services and Infosys.

Consider the disruption that technology has already introduced. The big data company BeyondCore can automatically evaluate vast amounts of data, identify statistically relevant insights, and present them through an animated briefing, rendering the junior analyst role obsolete. And the marketing intelligence company Motista employs predictive models and software to deliver insights into customer emotion and motivation at a small fraction of the price of a top consulting firm. These start-ups, though they lack the brand and reputation of the incumbents, are already making inroads with *Fortune* 500 companies—and as partners to the incumbents.

Consulting firms that hope to incubate a technology-assisted model will want to revisit the lessons Christensen laid out in *The Innovator's Solution.* (See the sidebar "A Checklist for Self-Disruption.") As he has often said, self-disruption is extremely difficult. The day after you decide to set up the disruptive business as a separate unit, the illogic of the new business to the mainstream business is not magically turned off. Rather, second-guessing about the initiative persists, because the logic is embedded within the resource allocation process itself. That second-guessing must be overcome every day.

Resources:

https://hbr.org/2013/10/consulting-on-the-cusp-of-disruption

https://www.linkedin.com/pulse/top-15-strategic-trends-consulting-services-firms-2016-kumar-parakala

https://www.linkedin.com/pulse/future-consulting-thoughts-how-industry-should-evolve-douglas-cole

https://hingemarketing.com/blog/story/top-5-business-challenges-for-management-consulting-firms

Appendix B. – Setting Expectations for the Customer Experience

Connecting to Wi-Fi is almost as much an art as a science. Network standards are notoriously loose – more like guidelines really – and as we know, performance, reliability – and especially security – can vary widely from hotspot to hotspot. And even if the networks were perfect, there are variations in devices (and operating systems – more on this below) that cause different user connection experiences. We know all of this – we live it every day. But our customers are not Wi-Fi experts. Nor should they be. So before going into a POC, or a new customer implementation, it is important that we set some expectations on what they can expect when using iPass.

First, a few basics…

We call it iPass SmartConnect, not *MagicConnect*, for a reason. It's not magic. That is, iPass in not a network. We don't own hotspots, and if there is no iPass Wi-Fi network in the vicinity of the customer device, they will not connect. Don't laugh: we've had customers upset about this: "I've never had Wi-Fi at home, so when my company bought iPass, I was excited because now I can get online at home! But it still doesn't work – what's up?" I'm serious.

The corollary to this is the customer who buys iPass, thinking that even at $50/month, it's a steal, thinking that with iPass, they can drop their ISP (e.g., Comcast), and instead of paying $75 for just in-home Internet access, for $25 bucks less they think they get in home Internet, plus connectivity around the world! Of course, this is not how it works – but that has been the expectation of some.

And finally, we are the Uber of Wi-Fi in that, just like Uber doesn't own any cars, we don't own any Wi-Fi networks or hotspots. Basic, I know, but don't assume all of our users get this.

Moving ahead to more subtle expectations…

First, as noted above, not all operating systems are created equal. On one end of the spectrum is Android, which extends to its partners very open access to the connectivity APIs, and therefore gives us the greatest degree of flexibility (and invisibility). iOS and Mac OS are on the other end of that spectrum. With an iPhone or Mac, for example, you will still have to manually connect through our app the first time to a new hotspot (after the first time it will remember). This is currently a limitation of the OS – not our app. (Note that Apple is beginning to allow deeper access to these APIs, which will help, but still not expected to the level of Android accessibility). Windows is somewhere in the middle, and since Windows phones are largely non-existent, it is safe to say we can explain how laptop usage and SmartPhone usage differs. *But don't forget to tell your customers that behavior is not the same, depending on the OS/device they are using.*

And by the way, all Androids are not necessarily equal either. There are literally thousands of different Android devices and manufacturers, and *they do not all work the same way*. Because of the open nature of the Android API, device manufacturers can add (or not include) specific functions or capabilities. While we test with the most popular brands, and use Google simulation tools to test others, we can never guarantee the same experience on different devices, especially in a BYOD world.

How does curation work, and what can customers expect?

As you know, SmartConnect will detect, catalogue, and *curate* networks. In this context, curation is the process of adding to our footprint new networks/access points that are 1) free, and 2) meet our quality and reliability standards. How do we determine if our criteria are met? Essentially by collecting data – a lot of data – about 200 records – from every network connection our customers' devices discover. *Our customers are part of this process – they are actually testing for us.* Now, the important part to convey to your customers is that 1) the constant improvement of the Quality of Service (QoS) and 2) the expansion of the network via curation is basically a trial-and-error process. That is, as we detect new access points, we probe them, and collect this data. If this appears to be an access point that will result in a good user

experience, and we've collected enough data to validate this, we'll add this hot spot to our network. So the next customer that "sees" it will automatically connect (except iOS – see above). However, the other side of this are the hotspots or networks that, based on the data, consistently result in poor user experiences. These hot spots will be *blacklisted* – eventually – by the same process in reverse. But it does require enough data from users to make this determination. In other words, *customers having a bad experience are actually helping improve the quality of the experience - over time*. And the more users we get, the more data we collect, and the faster the quality improves. So in a trial, for example, we will have users that will fail to connect in locations where they know Wi-Fi is available. They need to be aware that just because Wi-Fi is available, it may not be adequate – or secure. And therefore SmartConnect may not complete the connection…

Which leads us to the bane of our existence, at least for now: False Positives.

Our single biggest complaint and reason for unsuccessful connections is a *False Positive*. A False Positive is a hotspot that looks like it should be an iPass network, but isn't. This is especially true in hotels, which have multiple service providers, some part of our network, and many more that are not. Take Marriott, for example. All Marriott hotels use the same network identifier – or SSID. The SSID cannot tell an iPass-enabled hotel from one that is not. So even though a Hot Spot may indicate iPass is available, it may not be one of ours. Which really frustrates users – understandably. But SmartConnect is doing some clever things. In addition to seeing only the SSID, SmartConnect, with Demeter and Kronos and Spartan, pull additional data – BSSID/Mac addresses – which are unique to that access point. Now, through the curation process above, these access points not part of our network *will* be weeded out – blacklisted. The problem is we are not yet collecting enough data from enough users to cull out all the false positive hotspots not in our network fast enough. But our big data team as been working on a technique called "grouping" which, without going into detail, will significantly improve this process, speeding up the blacklisting, and eventually eliminating (almost) false positives.

So in conclusion…

Just talk to your customers and prospects. They are not experts. They don't know all that you know, and they certainly don't know iPass – even if they think they do. Letting them know what to expect is half the battle – and will lead to a better experience even when they are having a bad one.