



iPassConnect™ 2.4 for Windows

Technical Documentation

Executive Overview	4
End User Benefits	4
Administrative Benefits	5
How iPass Works Diagram	7
iPassConnect Client Screen Shot.....	8
General Functionality.....	9
Dial Up Networking (DUN).....	9
Network Adapter	9
TAPI	9
Windows Registry	9
User Controlled Policies.....	9
Administrator Controlled Policies.....	9
Logo	9
Domain	10
Billing Code	10
Session Management	11
Redial	12
Smart Redial	12
Save Password	13
Cache Password	13
Show Pricing	13
Help	14
Proxy	14
Phonebook filtering	15
Customer owned access points	15
Local Number Lookup.....	15
Launch Programs	16
Connect Actions	16
Updating Functionality.....	16
Policy.....	16
Phonebook.....	16
Configuration Settings	17
Software	17
Integrated Service Quality Measurement (SQM)	18
Troubleshooting and Monitoring.....	18
SQM Timing Settings	18
Connection Type	18
VPN Integration Options.....	19
Default	20
Auto-launch.....	20
One-click.....	20
Auto-teardown.....	22
Personal Firewall Integration.....	22
SecureConnect & Auto-teardown	22
Built-in iPassConnect Security.....	23
User Credentials.....	23
Customer Configuration Policies	24
Global Broadband Roaming.....	24

Wireless and Wired Broadband	24
Generic Interface Specification	24
Layered Security Recommendation	26
Supported Wi-Fi (802.11b NIC) Cards	26
Cisco	26
Compaq	26
Intel	26
Orinoco	26
Toshiba (Built-In by Agere)	27
Supported Platforms and Languages	27
Platforms Supported	27
Languages Supported	27
System Requirements	27
Operating System Requirements	27
Device Requirements	28
Additional Requirements For Broadband Users	28
Software Requirements	28
General Customization Options	28
Profiles	28
Viewing Client Customization	29
Making Changes to Customization Options	29
Troubleshooting	29
Feedback on this document	29
About iPass	29

iPassConnect Technical Documentation

Executive Overview

The iPassConnect enterprise connectivity client is the user friendly mechanism for an end user to access the iPass network for remote connectivity via a dial-up, ISDN, PHS, wireless (Wi-Fi), wired Ethernet, or home broadband connection. The client is designed to make remote connectivity secure, convenient, productive and simple for the end user. Additional functionality ensures a secure and controlled session to meet IT's demands.

This document provides an overview of the technical functions of the iPassConnect connectivity client for Windows version 2.4.

End User Benefits

The user interface of the client software enables faster, easier lookup to the access points in the iPass Network. Some of the features that end users will have access to include:

Ease of Use/Single Interface – The user simply inputs where they are and looks for the local access point. Users can search by country, state, city or area code. In the U.S., the user may also search by number - iPassConnect will return a list of modem access points that are local to them. Frequently used access points may be stored using the bookmark feature to enable faster access. A single interface is used regardless of connection technology: wireless or wired broadband, dial-up, ISDN, PHS, or home broadband.

Redundant Coverage – Users can always get connected with a number of different access methods from anywhere in the world. And, the Select All feature, instructs the client software to automatically roll over to an alternate dial-up number until it connects so the user does not need to select each number nor perform repeated keystrokes and mouse clicks.

Automatic Phonebook Updates – Users always have the most current phonebook because the client automatically checks for updates upon successful connection each day. iPass adds access points as more access providers are added to the iPass virtual global network and as current providers expand their networks and periodically deletes access points as a part of the iPass proactive network quality management program.

Automatic Software Updating – iPass releases new versions of the iPassConnect software at regular intervals. iPassConnect will automatically receive program

.....

upgrades and can be designed to receive configuration file updates, freeing administrators from having to deploy new versions of the client.

Dialing Intelligence – Administrators no longer need to train end users to remember or understand the need for all the dialing rules for different countries. And, in the United States, iPassConnect knows which U.S. areas require an area code or 1 + area code to connect a local call.

Calling Card Support – For users on the run, iPassConnect can connect end users even from a payphone with the use of a calling card or PIN.

Type Ahead Feature – Many fields in the iPassConnect user interface come equipped with the Type Ahead feature. Users simply enter the first few letters of the word or phrase they are looking for, and the client will fill in the rest. This feature reduces the need to type out long phrases, prevents spelling errors and speeds up the connection process.

Connection Status Screen – The connection status screen displays the connection time to the user during each connection attempt. The connection time is separated into two categories: modem negotiation time and authentication time. iPassConnect displays these times to the user separately to allow a better understanding of what is happening as he or she is attempting to connect.

Straightforward Help – iPassConnect includes a comprehensive, on-line help and troubleshooting guide.

Administrative Benefits

iPass can assist with the most important features for the configuration and management of remote access. These administration features allow the IT administrator to simplify and control the end-user experience through such means as a common user interface and preset defaults. The customizable administration features include:

Corporate-Wide Settings – Defaults can be set for domain names, saving passwords, maximum connect times, idle time outs, and launching programs. IT administrators can even designate an alert to warn end users that their hard connect time is about to expire.

Customized Phonebook – Control the iPassConnect phonebook based on a list of predetermined parameters and filters. Hide/show access point prices, add/delete corporate RAS numbers or even designate different connection behaviors for corporate own access points or iPass' access points.

Common User Interface – A single client makes it easier for end users to stay connected even when they are connected via a home broadband connection. All iPass access points, including corporate RAS numbers are seamlessly integrated into the iPassConnect client. There's no need to switch networks, software, or change configurations to take advantage of the world's largest network.

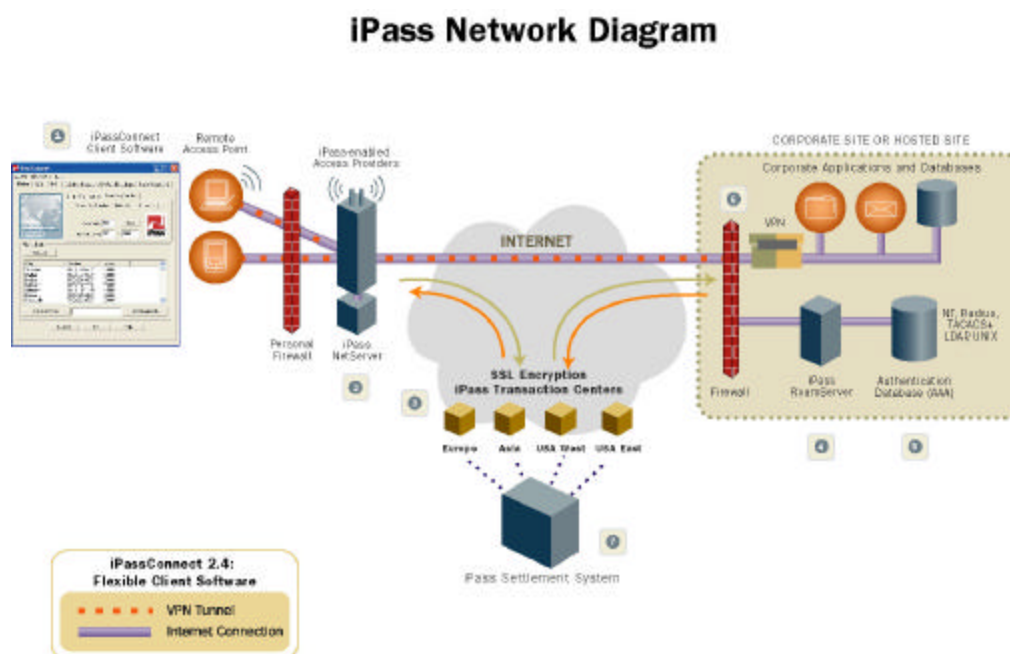
.....

User Quality Data - Client captures quality data for each user connection attempt which can be used by IT groups to identify user issues for troubleshooting and monitor usage.

Post-Connection Actions - The post-connect actions feature allows users to configure the client to automatically run programs after connecting to the Internet via the iPass Network. This feature allows users to launch a web browser, connect to the corporate network using a VPN solution, or to launch other software programs.

Customized Corporate Look - Insert the corporate logo in the primary co-branding space on the client's user interface. Include corporate help desk number in the logo to remind end users where to call for assistance.

How iPass Works Diagram



1. Remote user launches the iPassConnect client software from their laptop to connect to the Internet via dialup, ISDN, PHS, or broadband.
2. The iPass NetServer, located at the remote access point, encrypts the user ID and password, then forwards the information to one of the globally located iPass Transaction Centers.
3. The Transaction Center decrypts the user ID, identifies the domain name, and then re-encrypts to forward to the authentication database located at the corporate or hosted site.
4. The iPass RoamServer receives the request and passes it to the corporate or hosted authentication database.
5. The corporate authentication database grants the authorization approval. The Yes/No response is sent from iPass RoamServer back to the provider, via the Transaction Center. Shared secrets are never sent to the providers in order to maintain a distinct, secure separation between iPass customers and providers. iPass is the trusted third party.
6. Once the iPass-enabled access provider is given the "OK" by iPass to allow access to the Internet, the iPassConnect client can automatically launch the user's VPN to securely tunnel back to the corporate LAN.
7. When the internet "transaction" is complete, a record of the session is forwarded to iPass Settlement. The iPass Settlement system is responsible for the rating of each transaction. The corporation receives a single, detailed monthly invoice for all usage incurred.

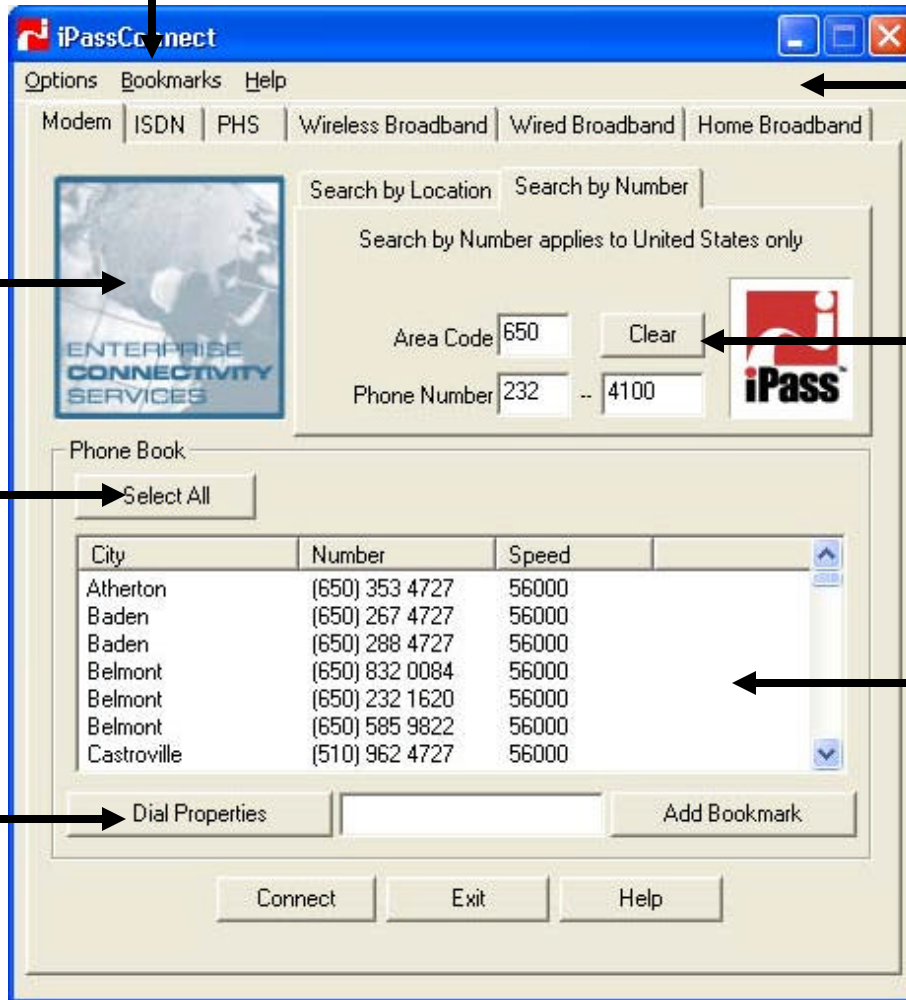
iPassConnect Client Screen Shot

Quick connections made possible with bookmarks for frequently visited locations

Set policies: idle disconnect, VPN 1-click, or placement of company logo

Dial all select numbers in turn automatically

Easy to adjust to different environments



Use multiple technologies with one account

Easy to use interface allows user to search by country, city, state area code, number

Multiple access points per city in a phonebook that is automatically updated for the end user



General Functionality

Dial Up Networking (DUN)

iPassConnect creates an iPassConnect connectoid, also known as a DUN entry, this DUN entry is used for making dial connections. iPass uses DUN, a standard part of the Windows operating system, to ensure consistent functionality across different modems.

Network Adapter

iPassConnect overwrites network adapter settings when making a broadband connection so the user does not need to manually change their connection setting to use the iPass service. These settings are re-set after the connection is ended or cancelled.

TAPI

iPassConnect overrides Microsoft OS' Telephony Application Programming Interface (TAPI) dialing rules because dialing rules such as the US 10-, 11-digit dialing and international dialing rules change frequently. iPass ensures that the user has a positive connection experience by proactively managing the access point phonebook and iPassConnect software to accommodate the changes in dialing rules.

Windows Registry

In general, iPassConnect does not make changes to the registry so the user does not need to have any administrative privileges to install the software. This makes installs easier. iPassConnect does require registry access for customization options when iPass controls third party applications for security policy enforcement, such as VPN and personal firewall integration settings.

User Controlled Policies

Please review the *iPassConnect User Guide* document for specific user information.

Administrator Controlled Policies

Many features can be customized to support IT's security and control preferences.

Logo

iPassConnect can support a customized corporate look. The customer can submit a logo to replace the iPass logo on the left side of the main screen in iPassConnect. The iPass logo on the right side will still be present. This logo should be submitted as a

.....

114 pixel x 123 pixel Windows bitmap (.bmp) file. The default logo is the "Enterprise Connectivity Services" logo.

Domain

Blank Domain Name

By default, the roaming domain is blank. This allows the user the flexibility to fill in their domain.

Pre-set Domain(s)

iPassConnect can be configured to include the customer's roaming domain. If the customer has multiple roaming domains, iPassConnect can present a drop-down menu of all domains. A drop-down domain menu is often used to assist customers who choose to use the same iPassConnect client profile for use for multiple regions e.g. @domain.us.com, domain.jp.com, and domain.de.com. In this environment, IT only has to support one client for all regions of the world. Note: A total of 1024 characters for all of the domains may be used. Character space is taken up by commas which need to be placed between each domain name. The formula is $(1024 - (N - 1))$ where N equals the number of domain names.

Non-editable Domain (s)

iPassConnect can be configured to make the domain(s) non-editable. This feature may prevent a user from accidentally changing or deleting their domain and having difficulty connecting.

Domain not present

iPassConnect can be configured to completely hide the domain. (This feature requires one valid roaming domain name hard-coded and hidden.) This feature is often deployed to help avoid confusion when the user's email address e.g. bob@domain.com is not the same as their iPass login information, e.g. bob@domaincorp.com.

Billing Code

The Billing Code feature is useful for companies who wish to bill back connection charges to different departments. At the end of the month, the company's call detail records (CDRs) will indicate connections to the various billing codes to allow for easy segmentation and dissemination e.g. user@sales.domain.com. iPass will not use the portion that indicates the billing code i.e. "sales" for authentication. Note: A total of 1024 characters for all of the billing codes may be used. Character space is taken up by commas which need to be placed between each billing code. The formula is $(1024 - (N - 1))$ where N equals the number of domain names.

By default, the billing code feature is off.

Blank Billing Code

iPassConnect can be configured with a blank billing code field where a user can enter a value. There is an 8 character limit to this field. This field is not mandatory.

Pre-set Billing Code(s)

iPassConnect can be configured to include a drop-down menu of billing codes for the user to select. This can be set to allow or not allow a user to add their own menu item. The user will not be required to make a selection.

Session Management

Idle Timeout

The Idle Timeout feature helps to control connection costs by automatically disconnecting the user if the system is idle.

By default, iPassConnect is configured with no idle timeouts.

Idle Timeout Duration

iPassConnect can be configured to include an idle timeout which will disconnect the user if the machine is idle for a period of time. The duration should be submitted in the form of minutes.

Idle Timeout Warning Message

When an idle timeout is configured in iPassConnect, the default action is for the user to be immediately disconnected. It can be configured to include a dialog box which gives the user the option to remain connected. If the warning dialog box is desired, a value must be submitted for how long the box should appear. If the user takes no action within the time period specified, the user will be disconnected.

Idle Timeout Traffic Threshold

iPassConnect can be configured with a threshold which needs to be reached to enforce the idle timeout. The default threshold is 0 bps – meaning that there needs to be NO traffic passing over the connection for the idle timeout to be invoked. For example, if a 1024 bps threshold is configured, if the traffic remained under 1024 bps for the specified idle timeout duration, the user would be disconnected or prompted with the warning message, depending on configuration. Setting the threshold to 1024 will generally keep a “chatty” application like Outlook from keeping the connection active. A threshold should be submitted in the form of bytes per second (bps).

Note: The idle timeout feature is not available for wired or wireless broadband connections.

Maximum Session Length Timeout

Maximum Session Length Timeout helps to control costs by preventing very long connection sessions.

By default, iPassConnect is configured with no maximum session length timeouts.

Maximum Session Length Timeout

iPassConnect can be configured to include a maximum session length timeout. The period of time should be submitted in the form of minutes.

Maximum Session Length Timeout Warning Message

When a maximum session length timeout is configured in iPassConnect, the default action is for the user to be immediately disconnected. It can be configured to include a dialog box which gives the user the option to remain connected. If the warning message box is desired, a value must be submitted for how long the box should appear. If the user takes no action within the time period specified, the user will be disconnected.

Redial

The Redial feature saves the user time by automatically re-trying the same access point multiple times. The user does not need to reenter their selection information to connect to the same access point successive times.

Attempts

By default, iPassConnect is configured for two redial attempts. This value can be pre-configured and optionally disabled so the user cannot modify it.

Connection timeouts

By default, iPassConnect is configured to attempt another access point if the user is not connected within 120 seconds. This value can be pre-configured and optionally disabled so the user cannot modify it.

Smart Redial

The Smart Redial feature will automatically try another access point in the same city and the same area code if the previous connection attempt failed. This feature saves the user time by connecting to the next access point in the phonebook without user intervention.

By default, iPassConnect is configured with Smart Redial off and the user has the ability to change it.

Allow User to Enable Smart Redial

The administrator can request that iPassConnect be configured to prevent the user from turning off this setting. The advantage to this configuration is that the user will always make use of the Smart Redial feature.

Save Password

The Save Password feature saves the user time. There is no need to input their password with each connection attempt.

By default, iPassConnect is configured with save password off and the user has no ability to change the setting. The user password is secured on the client; it is encrypted on iPassConnect using a proprietary algorithm.

User ability to change setting

iPassConnect can be configured with the Save Password setting enabled on or off. If the setting allows the user to save their password, it is still optional for the user to actually do so.

Cache Password

By default, iPassConnect will securely cache the password so if another access point is attempted, the user is not prompted for user credentials again. This feature saves the user from inputting their credentials with each connection attempt.

Turn off cache password

iPassConnect can be configured with the cache password feature off, so the user is prompted for user credentials every connection attempt. This feature is particularly useful if a customer is using two-factor strong token authentication (e.g. SecurID) for the iPass authentication. And it can help if a customer's authentication server is configured to lock out users after a specific number of bad password attempts.

Show Pricing

By default, iPassConnect does not show the pricing column in the phonebook section of the main screen. The Pricing feature can be used to educate users on differences in connection fees in different parts of the world.

Display Modem/ISDN/PHS pricing

iPassConnect can be configured to display pricing on the Modem/ISDN/PHS tabs next to each access point. The pricing is displayed as an hourly rate.

Currency

iPassConnect has the ability to show the pricing in different currencies and different multiples to support a service markup. The default currency is US dollars (\$) per hour.

Help

By default, iPassConnect is configured with an iPass Help File and with no specific help information for the customer.

Technical Support Message

iPassConnect can be configured with a custom support message, that is accessed from the main screen of iPassConnect by selecting Options | Technical Support, telling users where to call for assistance. This message must be submitted in the form of a text file and must be able to fit inside of the iPassConnect window using 10 point System Font. There is no specific technical character limit. However, if the message is longer than approximately 1,500 characters, the text box will fill the screen with no scroll bars making it difficult for the users to read.

Customer Specific Help File

Customer can submit an .hlp file (with corresponding .cnt file) which can be used in parallel with the iPassConnect Help File. It will appear as a second "chapter" in the help contents section of iPassConnect. A company may wish to provide a help file relating to the corporate VPN – the user only needs to go to one Help drop down to find information about both connectivity mechanisms, iPass and their VPN.

Proxy

By default, iPassConnect is configured with no proxy settings.

Proxy server for Internet access from the LAN

iPassConnect can be configured with the proxy settings to allow for LAN phonebook (pbook)/configuration updates to function.

Proxy support for customer access points

iPassConnect can also be configured for proxy support for connections made with customer access points (cbook) to allow phonebook/configuration updates to function. The customer must submit the proxy server name and port.

Phonebook filtering

By default, iPassConnect includes all production access points. Customers may request removal of specific cities, countries, or toll-free access points. In some cases, the removal of US Toll free numbers can reduce costs. Filtering can be done by country, city, price, access-type, or provider. Filtering can not be done by individual access point.

Customer owned access points

Access methods

A customer may submit their own modem and ISDN numbers to be included in iPassConnect. These access points must use the user credentials from the User Info screen for authentication. Typically, these access points provide direct dial access to a customer's internal network - which implies that no VPN client is required. If necessary, iPassConnect can supply static, customer-provided DNS and WINS settings for these access points. These settings will apply to all customer-owned access points. iPass does not support the authentication and connection to customer-owned wireless broadband or wired networks. Please note that there is a contractual limit to the number of customer access points that can be added to iPassConnect.

Roaming Domain

If the roaming domain is needed for authentication to a customer owned access point, iPassConnect can send it. By default, iPassConnect does not include the roaming domain when sending an authentication request to a customer-specific access point.

Local Number Lookup

Local Number Lookup assists end users with determining the local number to dial in the US. For example, a user is attempting to connect in a Los Angeles hotel. They are not likely to know which of the several iPass access points in the 213 area code will incur a local toll charge. With this new feature, the user enters the area code and exchange (the first three numbers) of the location they are connecting from, and iPassConnect will return a list of dial access points that are closest to them. This helps companies reduce costs without burdening the end user to know what numbers are local within the vicinity that they are dialing from.

By default, the Local Number Lookup feature is enabled. iPassConnect can be configured to not include this feature.

Customer Owned Access Points

Local customer owned access points will always be presented at the top of the returned local list regardless of their distance to the central office (CO).

Toll Free

If Toll Free access is enabled, Toll Free numbers will be presented if no local numbers are found.

Launch Programs

By default, the user is allowed to launch programs after connection. iPassConnect can be configured by the user to run programs after connection. Typically, the user will configure the client to launch a web browser or their email program (e.g. MS Outlook). This feature saves the user time. iPassConnect can be configured to disable this feature.

Connect Actions

iPassConnect can be configured for any command line action or specific .exe file given to iPass by the customer. These actions can take place before iPassConnect attempts a connection, just after a successful connection (after the phonebook/software download, but before the VPN launches), on error, on cancel, or upon disconnection (just after the user clicks "disconnect" and just prior to iPassConnect actually disconnecting from the access point). Connect actions can be specified to be performed on iPass access points, customer access points or both. Typically, customers ask iPass to automatically launch the VPN for the user after successful connection. This makes connecting via a secure tunnel simple for the user; they don't have to remember to find and launch the VPN .exe.

Updating Functionality

Policy

By default, iPassConnect is configured for phonebook and configuration updates to occur automatically after the first successful login each day to ensure the user has the most current phonebook and profile settings. The user is not able to disable the updates.

Phonebook

No Automatic phonebook/configuration updates

iPassConnect can be configured to turn off the automatic phonebook/configuration updates. iPass strongly recommends against this configuration since the user

.....

experience is greatly improved with frequent updates. Even if this configuration is chosen, an automatic update will occur if the phonebook or configuration is more than 14 days out of date.

User ability to disable updates

iPassConnect can be configured to allow the user to disable automatic phonebook/configuration updates.

Delay Phonebook Update

This feature (which must be used in parallel with the SQM Delay feature) makes the automatic phonebook update wait x seconds before attempting to update. iPassConnect will attempt to retrieve the phonebook update y times (Count). If the customer has a VPN that has split-tunneling disabled, the phonebook update will go through the customer's internal network. If the customer has a proxy server, iPassConnect simply needs the network name of IP address of the proxy server and port. This ensures that phonebook updates are successful and that user always have the most current phonebooks.

Size of Phonebook Updates

Phonebook updates are sent as compressed files. A full phonebook update is typically 170 KB in size.

Configuration Settings

IT manager can push out policy changes to all users. This feature may be used for new password controls, VPN settings, proxy settings and security mechanisms. The user receives the new configuration file upon next successful connection and ensures uniform adherence of all policy settings.

Software

Default setting

By default, iPassConnect is configured to migrate to the next version of software when it is available. This feature makes it easy for the user to get the new version of software and gives the administrator confidence that the user is running the most current version of the software. The user is prompted and has the choice whether to accept the software. If the user selects no, the user will be prompted each time they connect until it is accepted.

Automatic update

iPassConnect can be configured so the user is not prompted to accept the new software, but instead receives it as part of the automatic phonebook/configuration update. This feature may be used to prevent users from selecting "No" at the prompt and, therefore, running out of date software. Software updates are a delta file and are typically 500 KB compressed.

No update

iPassConnect can be configured to not accept the newest version of the software. iPass recommends against this option as it may result in users running out of date software and therefore not having access to new features and capabilities.

Integrated Service Quality Measurement (SQM)

SQM is a software module within iPassConnect that lets iPass measure service delivery proactively and identify potential user training issues or access point issues. SQM works by tracking and logging all user attempts. These results are sent to an iPass database, which generates statistics showing the connection performance of every access point. This feature is integrated into every iPassConnect client and is the basis for iPass Service Level Agreements.

Troubleshooting and Monitoring

The SQM data is available to customers' IT group via the iPass Intelligent Online Quality™ (IOQ) service to identify user issues for troubleshooting and monitor usage.

SQM Timing Settings

By default, iPassConnect sends SQM data after it completes a phonebook update (if applicable). This occurs at the same time as all other post-connect options.

SQM Delay

iPassConnect can be configured to wait x number of seconds before sending SQM information. X can be a maximum of 300 seconds. This feature will be helpful to customers who use proxy servers and have a VPN launched by iPassConnect (regardless of whether it is a one-click VPN launch or not) that has split-tunneling disabled. This will ensure that SQM will always be sent through the customer's VPN via proxy settings. See also the Delay Phonebook Update feature.

Connection Type

By default, iPassConnect is configured with the Modem, ISDN and Wireless Broadband Tabs displayed. Optional tabs include: PHS, Wired Broadband and Home Broadband. All tabs can be configured on or off. The connection tabs provide a simple visual indication to the user to select the correct connection technology.

Modem Tab

The modem tab is used most often by roaming users. It is for any connection attempt using a standard modem. iPassConnect is compatible with all modem types, both v.90 and v.92. If the user is connecting with a v.92 modem a v.90-only enabled access point will simply negotiate to v.90.

ISDN Tab

The ISDN tab is used for ISDN connections.

PHS Tab

You will see this access type tab only if your ISP or corporation has enabled the option. It only applies to access within Japan for users with a Personal Handyphone System (PHS) mobile phone.

Wired Broadband Tab

The wired broadband tab is used for any connection attempt via a wired broadband line, such as DSL (digital subscriber line) or high-speed cable access.

Wireless Broadband Tab

The wireless broadband tab is used for any connection attempt via a Wireless LAN (802.11b WLAN) hotspot.

Home Broadband Tab

The home broadband tab allows a consistent interface for establishing a secure connection while using an existing broadband connection. It does not provide a connection through the iPass Network. As such, use of the home broadband tab is only valid if the end user already has an established DSL or a cable connection.

User Credentials

By default, the Home Broadband Tab will prompt for iPass user credentials and then launch any post-connect actions. This option is for customers who pass their iPass credentials to the VPN.

iPassConnect can be configured to not prompt for iPass user credentials and simply launch post-connect actions. This option is for customers who use different credentials for iPass and their VPN.

User Message

By default, the Home Broadband Tab will present the following message to the user: "I am already connected to the Internet."

The message can be customized. The maximum number of characters is 56.

VPN Integration Options

iPass has a very successful strategy of partnering with leading technology companies to bring comprehensive remote access solutions to the enterprise markets. These partner technologies, include Authentication/Authorization/Accounting (AAA) databases, IPsec VPNs and personal firewall. Many partners have integrated the iPass technology into their remote networking and security solutions.

This integration approach allows iPass to support established corporate security policies. iPass has extensive partnering experience with these technologies. iPass has a Solutions Lab corporate customers can visit to gain a better understanding of potential integrated iPassConnect solutions.

The customization options are:

Default

The default settings for iPassConnect include no VPN customization.

Auto-launch

iPassConnect can launch any executable file when given the specific path name of the file. Auto-launch can be set up to occur on only iPass access points, customer-provided access points, or both. All users must have the executable file installed in the same common directory (not the same as iPassConnect install directory). This feature saves the user the inconvenience of finding and enabling the VPN executable after iPass connection.

One-click

Definition: After successful authentication to the Internet, iPassConnect will launch the VPN Client, securely pass the iPassConnect user credentials to the VPN Client and connect the user to the VPN gateway. The user only enters credentials once, and is authenticated to both iPass and the VPN.

Cisco 3000

Requirements: The customer must have the Cisco VPN Client version 3.1 or higher and a single connection entry name (.pcf file name) common on all users' VPN clients. The .pcf file used for Cisco one-click can have locked attributes inside it, but the following attributes can not be locked: Host and SaveUserPassword. Please note that the pcf file can still have the ability for a user to save the password disabled, but simply can't lock the attribute inside of the .pcf file. On Windows 2000, XP and NT 4.0, users must have full registry rights for the Cisco VPN client. For Cisco one-click, the customer must provide the connection entry name. User credentials for both iPass and the VPN must be the identical. Cisco one-click is a global setting – meaning that it will be applied to all access points, regardless whether the access point is iPass-owned or customer-provided.

Nortel Contivity

Requirements: Customer must have a single externally routable network DNS name or IP address for their Contivity Switch as well as a single group ID and group PW. In order for iPassConnect to be configured for the Nortel one-click, the customer must provide the following information: Destination switch name (or IP), group ID and group PW name. For customers storing VPN user credentials locally on the Nortel VPN gateway, only the gateway destination name (or IP) is needed (no group ID or group PW is needed) Furthermore, the authentication for both iPass and the VPN need to point to the same database (unless VPN users are stored local on the VPN gateway). Nortel one-click can be configured for iPass access points only, customer-provided access points only or both.

Aventail

Requirements: The customer must provide the installation path, .exe name, and the destination IP or network name of the Aventail gateway.

.....

Microsoft PPTP

Customers who wish to use the 1-click PPTP VPN option within iPassConnect need to provide the following information:

(Note: The questions below pertain ONLY to the 1-click PPTP option within iPassConnect)

- 1) Same username and password for iPass Dial-up and PPTP VPN? (yes or no)
- 2) If #1 is No, then Allow PPTP password to be saved?
- 3) PPTP VPN server IP address or DNS name? (DNS name preferred)...one server only...backups NOT supported
- 4) NT Domain name?
- 5) NT Domain name editable?
- 6) Logon to network? (yes or no) default = yes
- 7) Software Compression? (yes or no) default = yes
- 8) Require encrypted password? (a.k.a. MS-CHAP) (yes or no) default = no
- 9) Require data encryption? (yes or no) default = no
- 10) Use IP header compression? (yes or no) default = yes
- 11) Use default gateway on remote network? (yes or no) default = yes
(a.k.a. split tunneling) defaulted to OFF ...can only see LAN and not Internet
- 12) Use specific DNS/WINS server? If so, please specify IP's for DNS1, DNS2, WINS1, and WINS2 (no DNS names)
- 13) If using Windows 2000 PPTP, please provide info for following:
 - a) EAP? (yes or no) default = no
 - b) PAP? (yes or no) default = yes
 - c) SPAP? (yes or no) default = no
 - d) CHAP? (yes or no) default = no
 - e) MSCHAP? (yes or no) default = no
 - f) MSCHAP2? (yes or no) default = no
 - g) w95MSCHAP? (yes or no) default = no



h) Encryption type (none, 40-bit, 128-bit)

Note: 128-bit requires High Encryption installed

Others

Other vendor VPN clients are supported for 1-click and include: Intel (formerly Shiva) and CheckPoint. The only information required for 1-click integration with these VPN clients is the installation path and .exe name of the launch executable for the VPN client.

Auto-teardown

Definition: After successful iPass authentication and phonebook/configuration updates, iPassConnect allows 60 seconds to connect to the VPN. If the user does not successfully connect to the VPN within 60 seconds, iPassConnect will disconnect the user from the Internet. If the user connects to the VPN and then disconnects the VPN during the session (without manually disconnecting from iPass), iPassConnect will terminate the Internet connection. This feature ensures that when connected to the Internet the user always has the VPN running, (and when the VPN is not running the user is not connected to the Internet) In order to use this feature, the customer must have a One-Click or Auto-Launched VPN.

Cisco

Requirements: Customer must use the 3.1 version or higher to use auto-teardown.

Nortel Contivity

Requirements: Customer must supply iPass with the Nortel Contivity switch name.

Microsoft PPTP

PPTP auto-teardown is automatic and cannot be disabled if using 1-click PPTP integration.

■ *All of these products are available for demonstration in the iPass Solutions Lab*

Personal Firewall Integration

The default settings in iPassConnect include no personal firewall customization.

SecureConnect & Auto-teardown

Definitions: SecureConnect – iPassConnect will check and ensure that the personal firewall is running before allowing a user to make a connection. Auto-teardown – if the personal firewall is terminated during the connection, iPassConnect will disconnect the user from the Internet. SecureConnect and Auto-teardown MUST be used together.

ISS

Requirements: RealSecure Desktop Protection Agent 3.1 (formerly BlackICE Agent 3.0)
Note: this integration does NOT work with BlackICE PC Protection (formerly BlackICE Defender), ISS' consumer product.

Sygate

Requirements: Sygate Personal Firewall 5.0 and higher. Sygate Secure Enterprise 3.0 and higher. Note: For Sygate Secure Enterprise, administrators can give the user the ability to disable the firewall without disabling Sygate Secure Enterprise. By default, this setting is turned off and must explicitly be enabled by the administrator of the Sygate Management Server. If this setting is enabled and a user disables the firewall portion of Sygate Secure Enterprise, iPassConnect will NOT disconnect the user.

Zone Labs

Requirements: ZoneAlarm Pro 3.0 or Integrity 1.0 or higher. Note: this integration does NOT work with ZoneAlarm, Zone Lab's consumer product.

Built-in iPassConnect Security

User Credentials

User password is secured on the client

The user password is encrypted on iPassConnect using a proprietary algorithm.

Security to the iPass NetServer

User credentials are sent via Password Authentication Protocol (PAP) because this is universally supported across all providers. In most countries the security of the dial connection between the client and the providers NAS is not at risk. Credentials are fully encrypted once they reach the provider's infrastructure (NetServer).

Wireless Broadband Security

For Wireless broadband connections, iPassConnect encrypts user credentials via SSL from the client to the provider's Access Gateway. This ensures the privacy of credentials when connecting to a Wireless broadband hotspot.

Customer Configuration Policies

The customer's configuration policy file is encrypted in the client to prevent unsolicited modification of the customer IT group's preferred settings.

Global Broadband Roaming

Wireless and Wired Broadband

In late 2000, iPass launched Global Broadband Roaming in partnership with Cisco Systems. This is the first deployed and operational roaming service to support broadband connectivity from airports, hotels, and convention centers.

Generic Interface Specification

The Advent of Access Gateways

Initially, wireless broadband providers, hotspot operators, created an infrastructure by simply combining Wi-Fi access points (APs) with other components to fashion a network that provided not only Access, Authentication and Accounting (AAA) security mechanisms, but also, provided a web portal to present the service to the end-user. The challenge was that these were proprietary networks; they were difficult to create, manage, and use. And they were not interoperable with Wi-Fi hotspots from other providers. In addition, since the Wi-Fi providers wanted to be in the business of operating hotspots, not be in the hardware / software business, they ran into challenges when they attempted to scale the solution to meet the demands of the market.

In response to this growing need, many networking equipment vendors have created a new device called an Access Gateway (AG). All the access points for a venue are connected back into an Access Gateway (AG) which provides the following:

AAA – Allocates IP addresses, transforms the login request into a RADIUS or other protocol, and performs basic local accounting.

Web Portal – Presents web pages to the user, describing the venue (price, capabilities, features, etc.)

Walled Garden – The ability for a user to see pre-defined portions of the Internet (limited access to sports, news, or weather) without charge. When the user attempts to go outside of the Walled Garden, they are directed back to the Web Portal to purchase the service.

Port Hopping - The ability for the user to move across multiple wireless broadband or wired ports, access points, without the need to re-authenticate.

Using iPassConnect and Wireless Broadband (802.11b WLAN)

iPassConnect communicates with access gateways from the vast majority of manufacturers using the open standard called the Generic Interface Specification (GIS). The GIS defines a robust method for smart clients to authenticate subscription users at Wi-Fi hotspots. The GIS is designed to be compatible with the existing web based authentication methods found today at Wi-Fi hotspots while allowing subscribers to leverage the inherent advantages of using a smart client instead of a web browser. The GIS reduces the time needed to approve integration of a Wi-Fi provider into the iPass virtual network. The GIS is freely available for download and implementation at www.ipass.com/gis.

The GIS defines how a client such as iPassConnect can communicate with the Access Gateway. The communication uses the HTTPS protocol, which gives a standard and secure means of communications between the iPassConnect client and the Access Gateway.

Access gateways that support the GIS contain a public 128-bit SSL certificate for iPass sessions. The manufacturers include this certificate in their products so they are capable of working with iPass client right out of the box. The private SSL certificate that is the mate of the public certificate is included in the binary of the iPassConnect client. This allows iPassConnect to secure both the logon process, and the data contained within the process. The 128-bit SSL certificate allows the secure movement of the logon data when it is transmitted between the radios in the Wi-Fi adapter and the Wi-Fi access point, and then all the way through the infrastructure until the logon data reaches the access gateway. Once at the venue access gateway, the 128-bit SSL is removed from the logon data by the access gateway and is transmitted via RADIUS to the iPass NetServer at the venue. The iPass NetServer then re-encrypts the data using a separate and unique SSL certificate and sends the data to one of the many iPass Transaction Centers. The iPass Transaction Center determines where this logon request should be routed and sends it to the iPass RoamServer that is on the customer premise. There, the second 128-bit SSL is removed and presented to the customer AAA for authentication. This unique process keeps the user logon data secure from the iPassConnect client laptop all the way to the customer infrastructure.

In addition to securing the logon data, the use of the HTTPS protocol in the iPassConnect client also greatly secures the user from an attack known as "Rogue Access Point". This is a Man in the Middle attack where a foreign Access Point sits between the end-user and the real Access Point. The Rogue Access Point pretends to be part of the real venue. The user is presented with a web page that appears to be the hotel or airport and asks for their name, password or a credit card they may reveal this personal information to the rogue access point.

iPass precludes this type of attack by requiring two-way authentication: the user has to prove their identity to the access point, and the access point has to prove its identity to the user. This is done via SSL certificates on iPass-enabled access points.

Layered Security Recommendation

Due to the open nature of Wi-Fi technology iPass recommends the enterprise secure the:

- Connection via iPassConnect SSL-based authentication
- Laptop via a personal firewall and anti-virus software
- Data via a VPN tunnel

Supported Wi-Fi (802.11b NIC) Cards

iPass Global Broadband Roaming service is fully compatible and has been tested with the following NIC Cards:

Cisco

- Model: AIR-PCM352
- Driver: NDIS 8.01.06
- Firmware: 4.25.30
- (Aironet 350 Series WLAN adapter)

Compaq

- Model: WL100
- Driver: 3.6.7.0
- Firmware: 0.8.0
- (Compaq Wireless PC Card)

Intel

- Model: WPC2011BWW
- Driver: NDIS 3.0.18.10
- Firmware: F3.00-18
- (Intel Pro/Wireless 2011 LAN PC Card)

Orinoco

- Model: PC24E-H-FC
- Driver: 7.14.01
- Firmware: Not applicable
- (IBM/Lucent/Orinoco)

Toshiba (Built-In by Agere)

- Model: 9000/9100
- Driver: 7.16.0.189
- Firmware: Not applicable

Supported Platforms and Languages

Platforms Supported

- Windows 95
- Windows 98
- Windows NT
- Windows 2000
- Windows ME
- Windows XP Home and Pro

Languages Supported

- English
- Traditional Chinese
- Simplified Chinese
- Worldwide French
- Worldwide German
- Japanese
- Brazilian Portuguese
- Worldwide Spanish

System Requirements

Operating System Requirements

Windows OS

- Win95 OSR (original release) with Dial Up Networking 1.2b or higher
- Win95 OSR-1, 2, 2.1, 2.5 (a.k.a. Win95 "Gold")
- Win98 OSR (with or without Service Pack 1) and Second Edition
- WinNT Workstation 4.0 and Server 4.0 with Service Pack 3 or later
- Windows 2000
- Windows ME
- Windows XP Home or Pro

Device Requirements

- Windows Laptop
- Installer is 2.5 MB
- 8 MB free disk space
- Pentium 133 Mhz or faster CPU
- 32MB RAM
- Microsoft TCP/IP protocol installed
- Microsoft Dial Up Networking (DUN) 1.2b or higher installed

Additional Requirements For Broadband Users

To support broadband options, your system must meet the following minimum requirements:

Wired Broadband

- Networking interface card with Ethernet interface

Wireless Broadband

- Networking Card
 - Wireless 802.11b LAN card
- *802.11b card may have special operating system requirements*

Software Requirements

- .xe size is 2.9MB. The .exe is 2.4 MB if the Local Number Lookup is not included.
- RAM requirement: 10 MB

General Customization Options

Profiles

Each build of iPassConnect has a unique profile number and may have different customization settings selected. This allows a customer to create one profile and a certain group of customization options for one type of user and another profile with a different set of customization options for a different type of user. For example, the IT manager may elect to not show Toll Free access points in the common user profile and

.....

provide Toll Free access points in the executive user profile to help maintain costs. A fee may apply for multiple profiles.

Viewing Client Customization

Customers may view customization options by profile on the secure iPass website at <https://www.ipass.com/secure/dialer>.

Making Changes to Customization Options

Customers may request changes be made to their iPassConnect by submitting an SOS ticket via the secure web site. Customers must provide profile ID of the iPassConnect client to be modified.

Troubleshooting

For troubleshooting information, please refer to the *iPass Troubleshooting Guide* available from the Training department.

For end user troubleshooting information, please refer to the *iPassConnect User Guide*.

Feedback on this document

Please send feedback on this document to marketing@ipass.com.

About iPass

iPass Inc. solves the complex issues of increasingly mobile workforces accessing their corporate networks, e-mail and the Internet from anywhere in the world. iPass enables secure access via wireless and wireline broadband, ISDN, dial-up and other access media, over multiple computer platforms and devices, all through the award winning easy-to-deploy and easy-to-use iPassConnect™ client. iPass counts among its enterprise and service provider customers many of the most recognizable corporate brands and "Global 1000" companies. Founded in 1996, iPass is headquartered in Redwood Shores, Calif., with offices throughout North America, Europe and Asia Pacific.

Note: The following are trademarks of iPass Inc.: iPass, the iPass logo, RoamServer, NetServer, iPassConnect, iOQ, iPass Managed Access and iPass Corporate Access. All other marks used herein are the property of their respective owners.