iPassConnect 3.0 Reference Guide

Customer Version, July 2003

Corporate Headquarters

iPass Inc.

3800 Bridge Parkway

Redwood Shores, CA 94065 USA

http://www.ipass.com

T: +1 650.232.4100

F: +1 650.232.0227

TABLE OF CONTENTS

Introduction

This document is to be reference guide intended for iPass customers, providing answers to common questions regarding iPassConnect 3.0.

The content of this iPassConnect 3.0 Reference Guide ***is proprietary and confidential information of iPass. You may use this Guide solely for purposes of understanding iPassConnect 3.0 and assisting authorized iPass users with installing and operating iPassConnect 3.0 In connection with your and their use of the iPass Service. Any unauthorized disclosure or use of the Guide may result in the cancellation of your license to use iPassConnect 3.0 and termination of your iPass Service.***

For a complete discussion on installing, configuring, using and troubleshooting iPassConnect 3.0, refer to the *iPassConnect 3.0 User Guide*.

New Features

iPassConnect is the preferred method for a user to connect to the iPass Virtual Network. Its goal has always been to make connections simple and to hide the complexity of aggregating multiple networks from both the user and our customers' IT groups. Throughout the lifecycle of iPassConnect, new features have been added to make connecting easier, as well as simplify the use of third-party security products, such as VPNs and personal firewalls. The three main goals of iPassConnect 3.0 are to:

- update the GUI
- improve wireless usability
- provide more policy settings, including prelogon, VPN auto-teardown and anti-virus integration.

New Features and Benefits Summary

The following table lists and describes the new features in iPassConnect 3.0, whether the feature is optional, as well as the benefit for both the user and IT staff. Details of these features are available in later sections of this Guide.

Feature	Description	Optional?	Benefit
Automatic wireless network detection	iPassConnect will be able to automatically determine whether a wireless network is available and will present the user with the option to connect to it without having to enter any location information.	Yes	User: Allows users to have available wireless networks presented with no interaction necessary. IT: Less support calls and training for wireless connections since the user does not have to do anything except launch the client to find an available wireless network.

Automatic wireless NIC configuration for following authentication types:
• Wayport
• Nomadix
• GIS
• no authentication
• WEP (40/128 bit)
• 802.1x - TTLS
  ○ MD5
  ○ MSCHAPv2
  ○ PAP
  ○ CHAP
• Cisco LEAP
	Once a user elects to connect to a wireless network, iPassConnect will automatically configure the NIC for the user.	Yes	User: Allows users to automatically get the correct configuration for an automatically detected wireless network and allows the user to connect with no interaction with the wireless NIC software.
			IT: No training on the wireless NIC software. Users are already familiar with using iPassConnect for connectivity. Makes wireless much easier to support since no NIC configuration is necessary.

Feature	Description	Optional?	Benefit

Anti-virus integration
• SecureConnect
  ○ Symantec/Norton
  ○ McAfee
• Auto-teardown
  ○ Symantec/
  ○ Norton
  ○ McAfee
• Auto-launch
	iPassConnect can detect whether Anti-virus software is running and keep the user from the getting connected to the Internet without it running. iPassConnect will also monitor the anti-virus software during the connection and if it is ever not running, the user will be disconnected from the Internet.	Yes	User: System is protected. Auto-launch allows the user to easily start the anti-virus software if it is not running when the user attempts to connect.
			IT: can ensure that any iPassConnect user accessing the corporate network has anti-virus software running – meaning the system and the network is protected. Auto-launch means fewer support calls as users will have an easy remedy to the error message if anti-virus software is not running.

Bookmarks • ability to store at City Level • better error handling when bookmarked access point is no longer in the network	A user will have the ability to Bookmark an entire city (for modem, ISDN or PHS). iPassConnect will then determine which access number is the best one to use. If a user Bookmarks an individual access point, the client will determine if the access point is still part of the Phonebook before using it. If it is not part of the Phonebook, the software will present the user with an error message giving the user the opportunity to select a new access point to bookmark.	No	User/IT: Automatic Bookmark updates: when the user stores at the city level, allows for the access point at the top of the Phonebook to be used every time. Bookmarks are more effective now because if the access point is removed from the Phonebook, iPassConnect informs the user if the access point itself was stored and is transparent to the user if the city name was stored.
End user license agreement: ability to suppress	As long as the legal agreement between iPass and the customer includes the End User License Agreement Language and the customer has signed it on behalf of all of the users, iPassConnect can suppress the license agreement during installation.	Yes	User: One less step is needed for installation of the iPassConnect software. IT: No support calls regarding acceptance of the end user agreement.
Graphical User Interface (GUI)	Every menu and screen inside of iPassConnect has been updated.	No	User: Improved usability for multiple connection types that continue to keep the non-technical user in mind. IT: iPC 3.0 will be easier to support as usability is improved for emerging technologies.

Feature	Description	Optional?	Benefit
ISDN: ability to select multiple devices	iPassConnect now has two fields which can be used to select RAS capable devices – this is needed for some ISDN TAs to do 128K access.	No	User/IT: Allows ISDN users who have terminal adapters that require selection of two devices to now get 128K access.
Local Number Lookup • ability to sort cbook access points to the top of the list • removal of city names from the resulting access point list	When a user enters a 10 digit phone number, iPassConnect will not only have the ability to display the cbook numbers, it will have the ability to sort it to the top of the list. The city names will also be removed for access points found with Local Number Lookup.	Yes	User: Removal of the city names eliminates confusion where we have multiple city names. IT: Ability to drive users to RAS access points whenever the RAS access point is local.
Modem: option to hide modem numbers and dial from the city level	iPassConnect will have the option to suppress all of the numbers from the client. A user will be able to simply select the city name and dial.	Yes	User: Eliminates confusion of having to select from a list of local number. IT: Fewer calls regarding specific number issues

Personal firewall
• Auto-launch
• ability to launch the software if needed
• supports:
  ○ BlackICE
  ○ Sygate
  ○ ZoneAlarm
	When iPassConnect presents an error message because the user's personal firewall is not running,	Yes	User: Auto-launch allows the user to easily start the personal firewall software if it is not running when the user attempts to connect.
			IT: Fewer support calls as users will have an easy remedy to the error message if the personal firewall is not running.

System tray icon • ability to exit application • ability to access Bookmarks • ability to launch application	iPassConnect will run at system startup by default and be placed in the system tray.	Yes	User/IT: Gives the user an alternative way to launch iPassConnect. Gives the user a very quick way to access Bookmarks. Running in the system tray allows the available wireless networks to be presented more quickly.
Update • new update process • ability to read automatic • proxy settings in IE • ability to separate • Phonebook and software	iPassConnect will have the ability to read from a list of proxy servers – using the automatic configuration script in Internet Explorer to be more robust in facilitating Phonebook updates and software updates in a proxy environment.	No	User: The ability to work with automatic proxy scripts will allow the LAN update to work in more complex proxy server environments. IT: LAN updates are much easier. If IT ever decides to turn off a software update, users will be able keep their Phonebooks current.

Feature	Description	Optional?	Benefit

Enhanced VPN Support
• Aventail
  ○ auto-teardown
• Check Point
  ○ auto-teardown
• Cisco
  ○ prelogon
• Nortel
  ○ prelogon
	Prelogon: iPassConnect will have the ability to be launched from the Windows logon desktop and launch a Cisco or Nortel VPN.
	Auto-teardown: iPassConnect will have the ability to teardown the Internet connection if the user disconnects from the VPN – newly supported VPNs include Check Point and Aventail.
		Yes	User: Prelogon – Easier to decide when and when not to use it by checking or unchecking a checkbox on the main Winlogon screen. User-defined drive maps can be enabled.
			IT: Auto-teardown – ensures all iPass traffic is sent over the VPN – meaning firewall rules can be applied.
			Prelogon – NT scripts can be enforced for security or policy; NT domain password expiration notification can be enabled.

Graphical User Interface (GUI)

The biggest change to the iPassConnect interface is that users now enter location information once and have all available connection types presented. In iPassConnect 2.x, users needed to pick the connection technology first, and then enter location information. Although this seems like a fundamental shift in the user experience, it is a positive and logical change that has been validated by over 60 of our customers in 4 countries who were interviewed during the design process.

We added the **Find** button for more effective, faster searching. When iPassConnect was originally designed, it was built for a dial network consisting of 2000 to 4000 access points. iPassConnect now must be able to handle over 15,000 access points and 5 different connection types. As the network has grown, loading all of these access points in to the GUI slows down the client. As the iPass network grows, especially the Wi-Fi network, the speed of access point searches will remain quick and consistent.

iPass was assisted by a firm named Meetinghouse with some of the automatic network detection and NIC configuration functionality. They also assisted with the 802.1x development in the client. Meetinghouse's name appears in the **About iPassConnect** dialog on the **Help** menu.

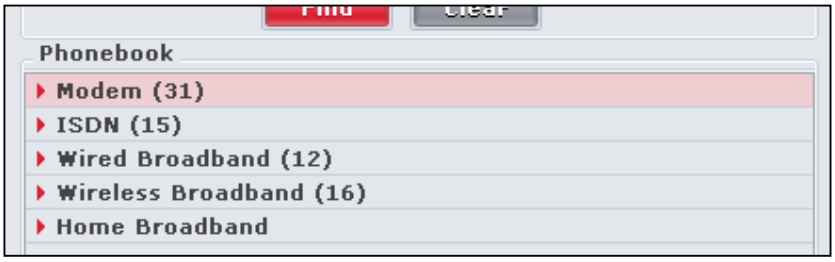
The Customer Logo

For branding purposes, you may insert a logo in the upper portion of the client GUI. The logo must be 267 x 58 pixels, which is a different size than the iPassConnect 2.x logo. Also, for test clients only, a descriptor may be put after the name "iPassConnect" for the purpose of distinguishing it from another client.

You must provide a new logo as part of the request for an upgrade. Without a custom logo, the client will display the iPass standard "Enterprise Connectivity Services" logo.

Using the New Phonebook

A *norgy* is one of the small red triangles that appears on the left side of any line in the Phonebook whenever further data needs to be displayed. Open a norgy and display the data by clicking on the triangle or anywhere across the entire line to the right of it. A norgy will be opened by default anytime that there is only one data item to be displayed under it.



In the Phonebook, only Modem, ISDN, PHS, Wired Broadband and Wireless Broadband norgies are enabled by default. Home Broadband is not enabled by default, as it should only be added to the configuration if the client has a post-connect action.

You can check the last Phonebook update by selecting **Settings > Update iPassConnect>Phonebook.** The date of the last update will be shown in parentheses.

The System Tray Icon

iPassConnect runs at system startup because it makes wireless network detection more effective. By running in the system tray, iPassConnect can detect if a wireless network is available and is able to present it to the user more quickly when the user opens the software.

A profile can be set not to run at system startup. If so, the client will take longer to launch because it will attempt to find a wireless network before presenting anything to the user.

iPassConnect runs as an application, not a service.

System Tray Options

When not connected, you can access the following options by right-clicking on the system tray icon:

- Exit – removes the application from the system tray
- Update iPassConnect – presents the user an option to update the Phonebook or the software
- Open iPassConnect –opens the main GUI of the application
- Connect to any Bookmarks the user has added

When a user is connected, you can access the following options by right-clicking on the system tray icon:

- Exit –disconnects the user remove the application from the system tray
- Update iPassConnect –presents the user with an option to update the Phonebook or the software
- Disconnect –disconnects the user from the connection
- Open iPassConnect –brings up the connection status window

Exiting iPassConnect

The only way to exit the application is to right-click the iPass icon in the system tray and select **Exit**. Selecting **Close** in the main GUI only closes the GUI. Selecting **Exit** from the main GUI when using the client in Prelogon, exits the prelogon version of the client, but the client will still appear in the system tray if configured to run at system startup.

The Connection Log

The Connection Log is a replacement for Dial History in iPassConnect 2.x. The Connection Log shows all of the user's connection attempts. The file will grow to 30K in size and once it does, it will truncate back to 20K, keeping the most recent information.

Bookmarks

A Bookmarked access point in the Phonebook is indicated by a red ribbon icon.

Bookmarks in iPassConnect 3.0 have been

improved in several ways:

- Bookmarks are now accessible from two different areas:
  - *The Windows System Tray:* Adding Bookmarks to the system tray allows for access to a commonly used access point without having to navigate the main GUI.
  - *Bookmarks menu:* Bookmarks are also available from the main menu on the Bookmarks menu, just as they were in iPassConnect 2.x.
- Bookmarks have improved error handling. If an access point is ever removed from the Phonebook, iPassConnect will present the user with an error message. This feature is only available for modem, ISDN and PHS access points.
- Bookmarks can now be made at the city level. For example, instead of Bookmarking a particular phone number in Schaumburg, Illinois, the user can simply Bookmark the entire city. Each time the user attempts to access with this Bookmark, iPassConnect will select the access point at the top of the iPass sort order. This ensures that a user will be able to connect to iPass' highest quality access point each time.
- Bookmarks for modem, ISDN and PHS access points contain much more information such as prefix for outside line and from location.

Although there is no limit to the number of Bookmarks a user can add, a Bookmark list that is too long will not scroll correctly. Accordingly, a user should keep the number of Bookmarks limited to 15 or less.

Although Bookmarks do not show connection type information by default, a user can give a saved Bookmark a unique name. By default, the city name is assigned to the bookmark, but the cursor on the save Bookmark screen defaults to the Bookmark name field, giving the user an opportunity to customize it with the connection type. The type of connection assigned to a Bookmark can also be found when accessing the Edit Bookmarks option.

Bookmarks in iPassConnect 2.x will not migrate to iPassConnect 3.0 because the Bookmark has added functionality and is stored in a new file within the client.

EULA (End User License Agreement)

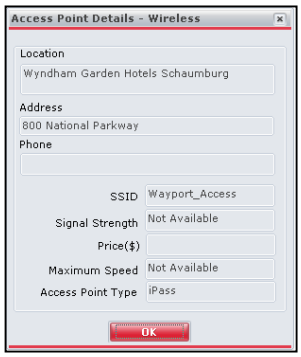
The End User License Agreement is now displayed during the installation process. (iPassConnect 2.x presents the end user agreement when the software is first run.) Please see page 27 for more information concerning the End User License Agreement.

Access Point Information

The  icon displayed in the Phonebook stands for *information*. Click on it to find more information about the selected access point. For modem, ISDN and PHS, a user will receive a dialog box illustrated here. By default, pricing is not displayed.

Wireless Broadband Access Points

If the Wireless Broadband location had been automatically detected, it would display signal strength with one of the following terms: Excellent, Good, Fair, Poor, None. This keeps the user from having to open another program to determine network status and other attributes of the wireless network. If the Wireless Broadband location had been automatically detected, but iPassConnect is unable to determine its unique location, the display will contain as much information as iPassConnect is able to determine.



A Wired Broadband location looks very similar except the SSID and Signal Strength fields are not present.

Access Point Pricing Display

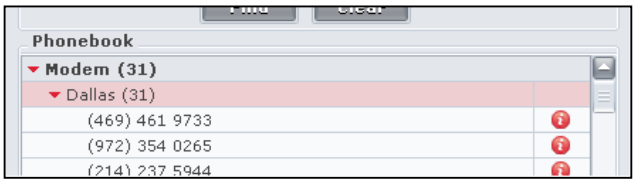
Modem, ISDN and PHS pricing can be displayed in this details screen, but pricing display is not yet available for broadband locations (although the pricing field is shown). We anticipate broadband pricing display to available in late 2003.

Connection Types

Modem

Modem access points appear as the first norgy in the Phonebook after a user enters search criteria and clicks **Find**. Click anywhere on the **Modem** line to open the norgy. The number in parentheses next to the word **Modem** indicates the number of modem access points found based on the search criteria.

After a user opens the norgy, the individual access point phone numbers will be displayed.



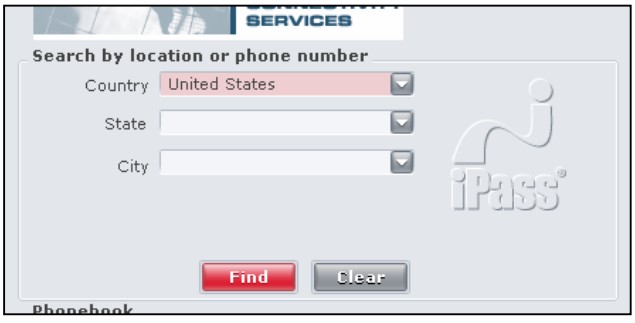
At the point, the **Connect** button at the bottom of the main interface becomes active. The user can select any one of the access points listed below the word *Dallas* to connect to a specific modem number. If the word *Dallas* is highlighted and the user clicks **Connect**, the first number on the list is selected automatically and the connection process begins.

Hiding Modem Numbers

iPassConnect can be configured by the IT department to not display any modem numbers to the user. If modem numbers are hidden, only city names will appear under the **Modem** norgy, not specific modem numbers. Upon selecting a city and clicking **Connect,** iPassConnect will attempt to connect to the first modem number in that city, in the iPass sort order.

Local Number Lookup

The Local Number Lookup feature allows a user in the United States to enter a 10 digit phone number and have a list of nearby numbers returned. Numbers are sorted in order by distance – meaning the access point at the top of the list will generally be the closest to the area code/exchange pair entered by the user.



iPassConnect displays POPs based on common rate plans in the particular calling area. Some calls that have toll charges may appear to the user. By always choosing access points at the top of the list, the user has the best opportunity to reach the best number for that particular area code/exchange and calling plan.

By default, Local Number Lookup is enabled. You may request that Local Number Lookup is disabled. If so, the Local Number Lookup fields will be not be shown.

Enhancements to Local Number Lookup

Local Number Lookup is now on the main client dialog, rather than its own tab on one of the dial-up tabs. Local Number Lookup fields are not active unless both of the following criteria are met:

- The profile has local lookup enabled
- The user has selected United States as a country (or the user has cleared the search criteria and has the United States listed as the default country). Local number lookup currently only does searches in the United States. We are researching the addition of Canada at some point but this is out of the scope of iPassConnect 3.0.

With active Local Number Lookup fields, the user can enter information in *either* the **State** field or the local lookup fields. Once data is entered in the **State** field, the local lookup fields become inactive. Once data is entered in the local lookup fields, the **State** and **City** fields become inactive.

Although Local Number Lookup access points are still sorted by distance, they are presented without the city name associated with the access point. The city name of the access point is irrelevant since in some cases iPass has access points that have multiple city names anyway. To check which city name is associated with the point of presence, simply click on the **Info** button.

If customer-owned modem numbers are included in iPassConnect, a customer can request that cbook access points are sorted to the top of the Phonebook output for Local Number Lookup.

Local Number Lookup and Broadband

Local number lookup only shows modem access points. We do not have a mapping of NPA/NXX to broadband locations – and since a user needs to be at the particular venue to connect to the broadband location, this method of searching for an access point doesn't make sense. However, we do recognize that users do use the client as a search utility for locations they may visit in the future. We are considering enhancements to later versions of iPassConnect for handling searches by other mechanisms to meet this need.

ISDN

ISDN functionality has been enhanced in iPassConnect 3.0.

- ISDN terminal adapters that require the user to select two ISDN devices to make bonded ISDN connection (128K) are now available in iPassConnect. (iPassConnect 2.x does not allow a user to select two RAS capable devices.) iPassConnect will not bond two modem connections or two ISDN devices that do not support bonding.
- ISDN access point speed can be found by clicking on the **Info** button to the right of the access point in the Phonebook.

ISDN Billing

Single-channel ISDN (64K) is billed just like regular modem access. Dual-channel ISDN access (128K) is billed like two separate modem connections and in fact, two separate call detail records are generated.

PHS

The Personal Handyphone System (PHS) standard is a TDD-TDMA based wireless communications technology operating in the 1880 to 1930 MHz band, used by millions of subscribers in Japan. The PHS data transmission technology is based on the PIAFS data protocol whose use in existing public networks already occupies a significant market share. PHS is actually a cordless phone that can be used like a mobile phone all over Tokyo - even in underground locations like subway stations.

Within the iPass network, we have aggregated the 32K PHS footprint of 2 DDI Pocket and NTT DoCoMo. The user is required to have an account with either DDI or NTT.

Air 128H is a new implementation of PHS that combines four 32kbps PHS channels into a single 128K channel. The service was launched in late Feb 2002 by DDI Pocket (one of our providers). This service is not a part of the iPass network at this time.

A PHS connection is handled exactly like a modem connection. The device is configured by selecting **Settings > Connection Settings > Dialup** tab.

In the Phonebook, PHS city names have a 2.0 or 2.1 at the end. This allows the user to tell if the number is a NTT (2.0) or DDT (2.1) number.

Wired Broadband

There are no new improvements to the wired broadband functionality in iPassConnect 3.0. The main difference between iPassConnect 2.x and 3.0 is how a user searches for the wired broadband access point.

Wireless Broadband

iPassConnect 3.0 includes automatic wireless network detection and automatic wireless NIC configuration. The goal of this feature is to make searching and connecting to a wireless network as easy as using a dialup connection.

NDIS-5.1 Compliance

In order for automatic wireless network detection and NIC configuration to work, the Wi-Fi NIC must be NDIS-5.1 compliant. NDIS stands for the *Network Driver Interface Specification*. The primary purpose of NDIS is to define a standard API for Network Interface Cards (NICs). The details of a NICs hardware implementation are wrapped by a Media Access Controller (MAC) device driver in such a way that all NICs for the same media (e.g., Ethernet) can be accessed using a common programming interface.

NDIS also provides a library of functions (sometimes called a "wrapper") that can be used by MAC drivers as well as higher-level protocol drivers (such as TCP/IP). The wrapper functions serve to make development of both MAC and protocol drivers easier as well as to hide (to some extent) platform dependencies.

There is no way to generically tell if a Wi-Fi NIC is NDIS 5.1-compliant. but this information is often available from the NIC manufacturer. iPass will publish a list of NICs that were successfully used during testing of the client. Cards used in iPass testing include the following:

- Cisco Aironet 340 Wireless Adapter
- Cisco Aironet 350 Wireless Adapter
- Intel Pro/Wireless 2011
- Intel Pro/Wireless 2011B
- Intel Pro/Wireless 5000 LAN Cardbus Adapter (802.11b)
- Lucent Orinoco PC Card Gold World Card PC24E-H-FC (802.11b)
- Nokia C110/C111 Wireless Adapter
- D-Link Air DWL-650 (802.11b)
- Microsoft wireless USB adapter (802.11b)
- Linksys wireless USB adapter (802.11b)
- Built-in wireless found in Centrino-based laptops
- Built-in wireless found in Toshiba Tecra & Portege laptops

Automatic Wireless Detection

If the user's profile has wireless broadband enabled and the user has an NDIS 5.1-compliant Wi-Fi NIC active, iPassConnect will attempt to detect Wi-Fi networks as soon as it is either in the system tray (when running at system startup) or when the client is launched by the user (when not running at system startup). iPassConnect will detect any Wi-Fi network that is broadcasting.

Although iPassConnect is able to detect all broadcasted wireless networks, it will not display all of them. iPassConnect will display wireless access points if it meets one of the following conditions:

- iPass access point
- Customer-owned wireless network added to the cbook.
- User-added wireless network in the personal wireless settings of iPassConnect

If a network is detected and eligible to be displayed, the Phonebook will have an Available Wireless Networks norgy with as much information as possible regarding the access point. In some situations, iPassConnect will be able to determine everything about the particular venue. If iPassConnect can not determine the exact venue, iPassConnect will display *iPass-enabled access point.* Despite the fact that the exact venue is not known, iPassConnect still has the necessary information to connect the user.

To connect to an automatically detected wireless network, select the access point in the Phonebook and click **Connect**.

Note that If the access point is automatically detected, the user still has the ability to manually select the access point in the Wireless Broadband norgy and connect.

SQM Data

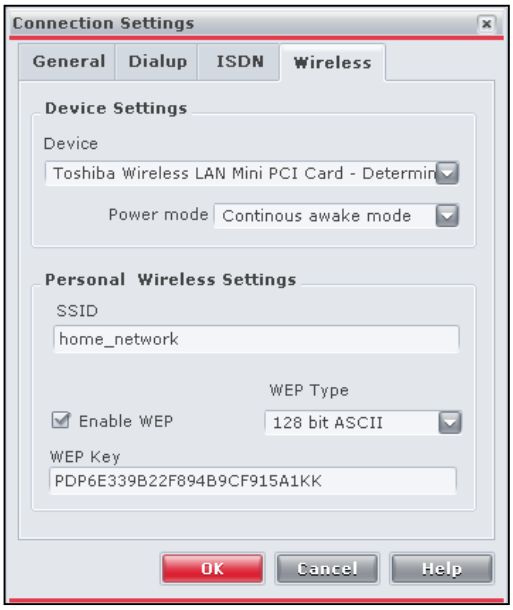
For GIS access points, iPassConnect does *location discovery* once the connection is made and sends this information as part of the uploaded SQM data. Location discovery is iPassConnect's ability to determine which location the user is actually connecting from, even if the client can't determine it initially. The SQM servers at iPass currently do not do anything with this information. Enhancements to SQM and iOQ are being made to handle this and will be available soon after the release of iPassConnect 3.0.

Windows XP Zero Configuration

iPassConnect 3.0 overrides the Windows XP zero configuration utility. If iPassConnect didn't override the Windows XP zero configuration utility, users would have their connection experience interrupted by messages which present the names of our network partners if they didn't already have the SSID on their preferred network list. If you want to use the XP zero configuration utility, you must exit iPassConnect to do so. If you have a wide XP deployment and want to use the XP zero configuration utility for non-iPass connections, you may want to consider configuring iPassConnect not to run at system startup.

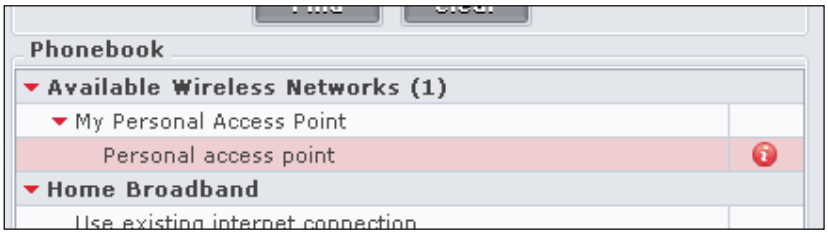
Personal Wireless Connections

iPassConnect allows you to add one wireless hotspot of your own to the client. A likely scenario where this would be used would be for a home wireless network. Select **Settings>Connection Settings>Wireless** tab, and enter the appropriate information. The user must enter at least the SSID. If WEP is required, the user must select **Enable WEP** and enter the appropriate WEP key as well as select the appropriate type of WEP key. An example of a completed personal wireless entry is shown here.



If a user-added wireless network is detected, the following is displayed when the user starts iPassConnect.

iPassConnect only allows a user to enter only a single wireless network into the client. iPass is considering adding the ability for the addition of multiple networks in a later release of iPassConnect.



The personal wireless network section of the client is directly tied to the wireless norgy and cannot be disabled. If the Wireless Broadband norgy is enabled in the client, then the personal wireless network section of the client is enabled. If the Wireless Broadband norgy is not enabled in the client, then the personal wireless network section is not enabled.

SQM Data

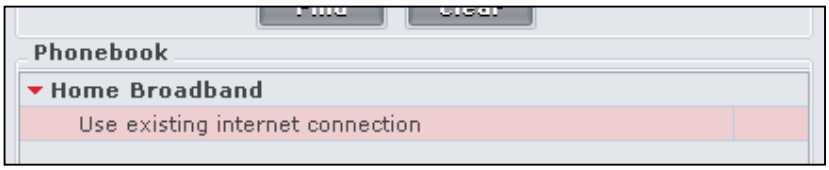
No SQM data is captured regarding the personal wireless connection. As well, SQM data from previous failed connection attempts is not uploaded when a user connects using a personal wireless connection. The only time SQM is uploaded is after a successful connection to an iPass or customer-owned network.

Home Broadband

Home Broadband in iPassConnect is for use with an already always-on Internet connection such DSL or cable. The Internet connection needs to be already live; iPassConnect does not perform any authentication to a user's home DSL or cable connection. When a user "connects" with Home Broadband, iPass immediately runs all pre-connect and post-connect actions – perhaps launching a personal firewall or VPN client. The purpose of Home Broadband is to give a user the same user experience for connecting to the corporate network, even when using a non-iPass connection.

Using Home Broadband

If Home Broadband is enabled in the profile, a Home Broadband norgy will appear in iPassConnect all the time, even when a user clears the Phonebook, as well as when the client does automatic wireless network detection.



The *Use existing internet connection* label is configurable. This label can be customized with up to 56 characters. Customized messages in iPassConnect 2.4 will automatically appear in 3.0.

By default, iPassConnect asks the user for iPass user credentials because this feature was originally designed for "one-click" connectivity, and these user credentials are passed to the VPN client (assuming the client is configured for one-click). A customer does have the ability to customize the client to remove the iPass user credential prompt. This should be requested by the Account Manager and/or customer when "1.5-click connectivity" is used.

Policy Enforcement

If iPassConnect is configured to stay active (connected) in the system tray, iPassConnect will enforce anti-virus & personal firewall policies such as SecureConnect and Auto-teardown. If the user disables the anti-virus or personal firewall software, iPassConnect will "disconnect" from Home Broadband, tearing down the VPN connection. The DSL or cable connection is still live and the user does still have the ability to launch and connect the VPN client manually, but iPassConnect will not let the user launch the VPN though iPassConnect.

Cisco recently introduced a command-line only version of its VPN client. If a customer runs the client in command line only mode and gives the user no access to the GUI, the user would have no ability to launch the VPN manually and would hence have no ability to get access without iPassConnect, meaning the personal firewall and anti-virus policies would be enforced.

SQM Data

No SQM data is captured regarding the Home Broadband connection. SQM from previous failed connection attempts are not uploaded when a user connects using a Home Broadband connection.

Security and Policy Enforcement

VPN Integration

iPassConnect 3.0 has new auto-teardown integration with the Aventail 5.1 or later, and Check Point NG FP3 or later VPN clients. VPN auto-teardown is also available for Cisco, Nortel & PPTP VPN clients.

In order to make use of one-click integration or auto-teardown, the user must have Read rights to the Windows Registry.

Auto-Teardown

After successful iPass authentication and Phonebook/configuration updates, iPassConnect allows 60 seconds to connect with the VPN. If the user does not successfully connect to the VPN within 60 seconds, iPassConnect will disconnect the user from the Internet. This 60 second grace period is configurable, but generally isn't changed.

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. iPassConnect checks the status of the VPN tunnel every 15 seconds, so it may take up to 15 seconds for a user to be disconnected. 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 profile must be configured with a 1-click or 1.5-click VPN.

Prelogon

Prelogon is the ability to perform operations on a Windows NT-based computer (NT, 2000, or XP Professional) *before* logging into a Windows NT Domain. Any operation that occurs when the computer is in this state occurs on what is referred to as the Winlogon Desktop. iPassConnect 3.0 will have the ability to operate on the Winlogon Desktop.

iPassConnect 3.0 has an option to integrate with the Microsoft GINA which will provide the ability to access iPassConnect from the Winlogon screen (that is, the screen that is typically presented after the user clicks CTRL+ALT+DEL). Prelogon for iPassConnect when used in conjunction with a 1-click or 1.5-click VPN will allow a user to perform a live logon to the NT Domain.

GINA stands for Graphical Interactive Network Authentication. The GINA is a replaceable DLL component that is loaded by the Winlogon executable. The GINA implements the authentication policy of the interactive logon model and is expected to perform all identification and authentication user interactions.

If prelogon is configured in the profile, iPassConnect will load its own GINA named ipgina.dll. This GINA sits in front of the Microsoft GINA.

Enabling Prelogon

Prelogon *must* be enabled in a profile before it is installed. It can be configured as part of an upgrade from iPassConnect 2.x to 3.0, but can not be "pushed" to a user who already has 3.0. If

a customer has a non-prelogon version of iPassConnect 3.0 installed and wants to add prelogon capability, the client must be reinstalled.

Prelogon can be enabled for all users and then users can have the ability to enable or disable it from the Connection Settings menu by selecting the "Start Before Logon" option. If the client does not have the GINA installed, this menu item does not appear.

Benefits of Prelogon

Typically, customers want prelogon to assist with the following:

- *Windows NT Domain Password expiration notification:* Customers who have a password expiration policy typically have a notification message that informs the user that the password will expire in after a certain number of days. If a user is remote all of the time, they will never see a password expiration message and could be locked out of the NT Domain after the password expires.
- *NT scripting:* Some customers have scripts that are initiated when a user logs into the NT Domain. These scripts can enforce security policies by checking for particular versions of anti-virus software, or similar policy applications.
- *User-defined drive mapping:* Some end users who use folders or applications on systems on the NT Domain may have drives that are automatically mapped when the computer starts up. An example of this would be naming //mtvoffice/groups/sales/ as drive Z so a user can get to this directory more easily. These drives must be mapped manually each time.

These functions can only occur when a user makes a live logon to the NT Domain.

Logon Scenarios

Without Prelogon

A typical logon scenario without prelogon might go as follows:

1. User powers on laptop
2. User is presented with CTRL+ALT+DEL screen
3. User clicks CTRL+ALT+DEL screen and is presented the Winlogon dialog box.
4. User enters password (the username and domain are cached from a previous logon) and clicks **OK.**
5. This action logs into the local computer only and the user is taken to the user desktop.
6. User opens iPassConnect and connects to the Internet and VPN.
7. This action logs the user onto the NT Domain used the cached credentials that were entered into the Winlogon screen at the initial start up of the computer.

When a user logs onto the NT Domain with cached credentials, no Windows NT Domain password message can be sent to the user, no NT scripts can be forced onto the user and user-defined drive mappings are not enabled.

Prelogon Enabled

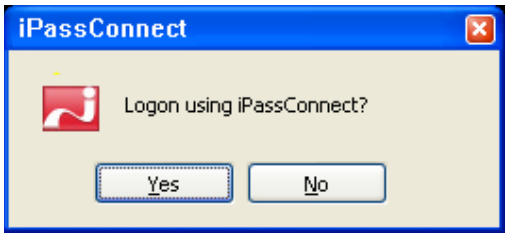
With Prelogon enabled, this scenario will change.

There are four basic steps in prelogon:

1. Establish Network Link
2. Connect to the Internet
3. Establish VPN connection
4. Live Logon to the NT Domain

The following scenario describes the user experience when remotely connecting with iPassConnect 3.0 and attempting to make a live logon to the NT Domain.

1. User turns the laptop on
2. User is presented with CTRL+ALT+DEL screen
3. User presses CTRL+ALT+DEL
4. User is presented with the below dialog box:



1. User clicks YES
2. iPassConnect GUI is displayed.
3. User connects to the Internet using iPassConnect GUI
4. iPassConnect GUI launches the VPN client
5. User establishes tunnel to the Corporate Network using the VPN client
6. iPassConnect GUI detects that the tunnel is established and communicates this to the iPassConnect GINA
7. iPassConnect GINA calls the Microsoft GINA which presents the Microsoft Username/Password/Domain screen
8. User enters credentials and clicks OK
9. Microsoft GINA performs the live logon to the NT Domain
10. After successful logon, the iPassConnect GINA migrates the iPassConnect GUI and the VPN GUI to the user desktop.

The following scenario describes the user experience when connecting with iPassConnect 3.0 and attempting to logon to the system and NOT the NT Domain.

1. User turns the laptop on
2. User is presented with CTRL+ALT+DEL screen
3. User presses CTRL+ALT+DEL
4. Logon using iPassConnect dialog box is displayed.
5. User clicks “No”
6. iPassConnect GINA calls the Microsoft GINA which presents the Microsoft Username/Password/Domain screen
7. User enters credentials and clicks OK
8. Microsoft GINA performs a logon to the system only.

The following scenario describes the user experience when a user is in the office connecting directly to the NT Domain, but has iPassConnect with prelogon enabled.

1. User turns the laptop on
2. User is presented with CTRL+ALT+DEL screen
3. User presses CTRL+ALT+DEL
4. Logon using iPassConnect dialog box is displayed.
5. User clicks “No”
6. iPassConnect GINA calls the Microsoft GINA which presents the Microsoft Username/Password/Domain screen
7. User enters credentials and clicks OK
8. Microsoft GINA performs the live logon to the NT Domain

VPN Integration with Prelogon

Since the purpose of prelogon is for the user to make a live logon to the NT Domain and since the domain controller is inside the corporation network, a VPN configured as 1-click or 1.5-click must be used with iPass’ prelogon service.

The Cisco and Nortel VPNs are supported with configured with 1-click or 1.5-click. Nortel logoff on connect is supported in the same fashion as iPassConnect 2.x. We will likely add support for Aventail’s Connect VPN client, Check Point’s VPN and Microsoft PPTP in later releases of iPassConnect. VPN auto-teardown is also available.

Personal firewall and anti-virus monitoring are not available in conjunction with prelogon.

Anti-Virus (AV) Integration

Anti-virus integration is very similar to what iPassConnect already does with personal firewalls: SecureConnect and Auto-teardown. There is also new functionality named Auto-launch.

With Anti-Virus *SecureConnect*, iPassConnect will check and ensure that the anti-virus software is running before allowing a user to make a connection.

With Anti-virus *Auto-teardown*, if the Anti-Virus software is ever terminated during the connection, iPassConnect will disconnect the user from the Internet.

With Anti-virus *Auto-launch*, if the Anti-Virus software is ever not running before the connection, iPassConnect can launch it for the user automatically to prevent SecureConnect from blocking the connection.

SecureConnect and Auto-teardown must be used together and can be configured with or without Auto-launch. Auto-launch can only be used if SecureConnect and Auto-teardown are enabled – it can not be used without it.

In order to make use of AV integration, the user must have Read rights to the Windows Registry.

Supported Products

iPassConnect 3.0 can enforce use of the following AV solutions:

- iPass is testing against McAfee VirusScan Enterprise version 7.00. We are working with McAfee to determine if other versions will be supported.
- iPass is testing against Norton AntiVirus Corporate Edition version 8. We are working with Norton/Symantec to determine if other versions will be supported.

Personal Firewall (PFW) Integration

The same integration in iPassConnect 2.4 is available in iPassConnect 3.0: SecureConnect and Auto-teardown. iPassConnect 3.0 also offers a new feature: Auto-launch.

With PFW *SecureConnect*, iPassConnect will check and ensure that the personal firewall software is running before allowing a user to make a connection.

With PFW *Auto-teardown*, if the personal firewall software is ever terminated during the connection, iPassConnect will disconnect the user from the Internet.

With PFW *Auto-launch*, if the personal firewall software is ever not running before the connection, iPassConnect can launch it for the user automatically to prevent SecureConnect from blocking the connection.

SecureConnect and Auto-teardown must be used together and can be configured with or without Auto-launch. Auto-launch can only be used if SecureConnect and Auto-teardown are enabled – it can not be used without it.

In order to make use of PFW integration, the user must have Read rights to the Windows Registry.

Supported Products

iPassConnect 3.0 can has been tested against, and can enforce use of the following PFW solutions:

- ISS RealSecure Desktop Protection Agent 3.1 and 3.5
- ZoneAlarm Pro version 3.7 and Zone Labs Integrity
- Sygate Personal Firewall 5.0 and Sygate Secure Enterprise 3.0

Installing & Upgrading iPassConnect 3.0

Installing the Software

Operating System Requirements

iPassConnect 3.0 can only be installed on computers running Windows 98 Second Edition, Windows ME, Windows NT 4.0 SP6 and later, Windows 2000, Windows XP Home and XP Professional.

The installer file for iPassConnect 3.0 is about 4.5 MB.

In addition, a user's system have the following:

- Internet Explorer 5.01 or later: Internet Explorer is needed because iPassConnect uses portions of IE to facilitate secure sending of quality data, Phonebook updates as well as creating an SSL tunnel for securing user credentials for broadband authentication.

- Support for 16-bit color (65536 colors) 16-bit color mode is needed to display all of the customized graphics in the iPassConnect GUI.

If installation is attempted on a system that does not meet these requirements, the iPassConnect installer will present the user with a message that tells the user which of these criteria is not met.

RAM and Disk Space Requirements

iPassConnect 3.0 has requirements for RAM, disk space, processor power, etc, but failure to meet these requirements does not prevent installation. These requirements are the following:

- 133Mhz or higher processor
- 64MB of RAM
- 12MB of hard drive space
- TCP/IP protocol
- One or more of the following connection devices:
  - Modem
  - ISDN Terminal Adapter
  - PHS Mobile Phone or Network Interface Card
  - 802.11b compliant NIC which is also NDIS 5.1 compliant.
  - Ethernet Card and Interface

iPassConnect will place files in the following directories as well:

- `C:\WINDOWS\inf`
- `C:\WINDOWS\System32.`

There may be other directories inside of these folders – the variations depend on operating system.

In order to be able to install the application, a user must have the ability to write to the HKEY_LOCAL_SYSTEM portion of the registry.

Installations on Windows 2000 and XP do not require a reboot. Most installations on NT 4.0 do not require a reboot. Installations on Windows 98SE and ME require a reboot. If a reboot is required, the user is prompted by the installer.

Currently, iPass only provides .exe versions of the installer. Other methods, such as .msi, are being investigated for future releases of iPassConnect.

Supported Languages

The July 7, 2003 release of iPassConnect is English only. A build of iPassConnect which supports Brazilian Portuguese, French, German, Japanese, Korean, Simplified Chinese, Traditional Chinese and Spanish will be made available sometime in late August. An exact release date has not yet been confirmed.

Installation Bundling

If requested, iPass can still provide a bundled installer of iPassConnect and a VPN client.

EULA Suppression

iPassConnect 3.0 presents the End User License Agreement (EULA) when the software is installed – not when it is first run like in iPassConnect 2.x. We now have the ability to suppress display of the EULA during installation, but *only* if the customer has accepted the End User License Agreement as part of the iPass contract. There are no exceptions to this.

Upgrading the Software

In order to upgrade, a user must be using iPassConnect 2.20 or later. Even if a profile is set to iPassConnect 3.0, a user who is on a version of iPassConnect previous to 2.20 will never receive a prompt to upgrade.

Since there is no automated method of updating to iPassConnect 3.0 from a version previous to 2.20, a user with an earlier version must do a new installation of iPassConnect 3.0 to use the new version.

If upgrade is attempted on a system that does not meet the operating system requirements discussed on 26, the iPassConnect installer will present the user with a message that tells the user which of these criteria is not met.

Upgrade Mechanism

After July 7, 2003, all customers running iPassConnect clients versions 2.20 and later in English, will be eligible to upgrade to iPassConnect 3.0. If the customer profile has been set to 3.0, the client will receive three very small files just like any Phonebook push. One of these files will then check the user's eligibility to upgrade.

If the user is not eligible for iPassConnect 3.0, (meaning the system is using an unsupported version of Operating System or Internet Explorer) the user will never see anything else regarding

the update until the system is upgraded to meet the minimum requirements. iPassConnect does log the fact that the user is ineligible and reports it in a new file in the log directory of iPassConnect 2.x named Ipcheck.log.

If the user is eligible for iPassConnect 3.0, on the user's next connection, iPassConnect will attempt the download of the iPassConnect 3.0 installer, as well as move one of the small downloaded files to a run directory, so this small file will run the next time the user logs onto the system.

The download of iPassConnect 3.0 will begin immediately and run in the background. A second iPassConnect icon will appear in the system tray next to the icon that normally appears. If the user double-clicks the icon, a small GUI will appear indicating the status of the download. The user can cancel or stop the download. If the download is stopped or cancelled, iPassConnect will remember how much was downloaded and will keep it so the user does not have to download it a second time.

The next time the user logs onto the system, a small .exe will check to see if the download is complete and if is not complete, will run to attempt to download the installer for iPassConnect. If the user is on a LAN connection, the download will begin immediately. If the connection is ever lost in the middle, the downloader will be able to recover from the point at which it was interrupted.

When the download is complete, the installer checks to determine if iPassConnect is running. If iPassConnect is not running, the installation of iPassConnect 3.0 will begin immediately. If iPassConnect is running, it will move the installer to the startup folder so the installer will begin upon next system startup. When iPassConnect 3.0 is installed, all of the files that were placed in the startup folder will be removed.

Support and Logistics

iPassConnect 3.0 will made publicly available on July 7, 2003. The software will not be pushed automatically to any profiles, either test or production.

Ordering an Upgrade

An existing customer orders a 3.0 upgrade in the exact same fashion as any other iPassConnect client upgrade. A customer (or Account Manager, Channel Manager or Partner) logs an SOS ticket for the upgrade.

The SOS Ticket

The ticket must be submitted under your Customer Number. The ticket must include the following in the Ticket Information section:

- **Case Type:** Request
- **Product:** iPassConnect
- **Topic:** Modify Dialer Profile
- **Version:** 3.00

The **Additional Information Required Based on Reported Problem** section must have the correct profile ID in it. If a custom logo is necessary it must be uploaded in this section. A customer's 2.x custom logo will not display in iPassConnect 3.0.

The **Description** section should clearly state the profile is to be updated to 3.0. The profile will receive the same settings that are in the previous version of the client. This is important – if your wireless tab is turned off in 2.4, it will also be turned off in 3.0, unless otherwise stated in the SOS ticket.

Put as much detail as possible in the ticket to ensure that the ticket is processed correctly. A separate ticket should be opened for each profile ID.

Dates for Submission

SOS tickets for 3.0 can be submitted beginning on Wednesday, June 25, 2003. No work will be done on these tickets until July 7, 2003, but the tickets will be processed on first come, first serve basis. There will likely be a large ticket backlog on July 7, 2003 and for a few weeks after the release. iPass Customer Operations will make reasonable efforts to support their 72 hour turnaround for ticket resolution, but please be patient as it may take longer for some tickets to be resolved. Also, work on production clients will always take priority over work on test clients. The turnaround for getting changes to test clients will likely be higher.

Test Clients

An upgrade for a test client will be handled in the exact same manner as a production client, except that Customer Operations will always put a production client work ahead of a test client. The turnaround for test client changes will likely be longer than 72 hours for a period of time after July 7, 2003.

Training & Documentation

The iPass training Web sites will be updated to include information on iPassConnect 3.0 before the public release on July 7, 2003.

The following documentation will be released on or before July 7, 2003:

- iPassConnect 3.0 Sales Presentation
- iPassConnect 3.0 Quick Start Guide
- iPassConnect 3.0 Migration Guide
- iPassConnect 3.0 FAQs – both long and short versions
- iPassConnect 3.0 User Guide
- iPassConnect 3.0 Troubleshooting Guide
- iPassConnect 3.0 Technical Documentation
- iPassConnect 3.0 Technical Deployment Guide
- Upgrading to iPassConnect 3.0