

A background image of a globe with a wireframe grid, showing the Americas. The globe is rendered in a light blue and grey color scheme, with a red vertical bar on the left side.

iPassConnect 3.30 for Windows Technical Marketing Guide

PROPRIETARY AND CONFIDENTIAL

Version: 1.0, September 2004

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	6
Features and Benefits	7
Access Functionality	7
Wi-Fi Integration	7
Security	8
How the iPass Network Operates.....	10
iPassConnect 3.30 Logistics	11
iPassConnect 3.30 Release	11
Ordering the Upgrade.....	11
Installation and Upgrading	12
System Requirements	12
Minimum Hardware Requirements	12
Operating System Requirements	12
Software Dependencies	12
Connectivity Dependencies	12
More Installation Notes	12
Upgrading to iPassConnect 3.30	13
Previous to iPassConnect 2.20	13
For iPassConnect 2.20 or Later	13
Upgrade Mechanism.....	14
Upgrade Matrix.....	15
Installing iPassConnect 3.30.....	16
Installing iPassConnect Software.....	16
Additional Files	16
Supported Languages.....	16
User Rights.....	16
System Reboots.....	17
Installation Options	17



TABLE OF CONTENTS

General Functionality	18
Profiles.....	18
Viewing Client Customizations.....	18
Changes to Customizations.....	18
Connectivity.....	18
Dial-Up Networking (DUN).....	18
TAPI.....	18
Network Adapter.....	18
Administrator-Controlled Policies	19
GUI.....	19
Customized Logo.....	19
Exit, Not Close.....	19
Domain.....	19
Department/Project Code.....	20
Session Management.....	20
Idle Timeout.....	20
Maximum Session Length Timeout.....	21
Redial Settings.....	21
General Redial Settings.....	21
Smart Redial.....	22
Password Settings.....	22
Save Password.....	22
Cache Password.....	23
iPass End-to-end Encrypted Login (iSEEL).....	23
Pricing Settings.....	23
Proxy Settings.....	24
Static Proxy Servers.....	24
Proxy Scripts.....	25
Local Number Lookup.....	25
Phonebook Filtering.....	26
Customer-owned Access Points.....	26

TABLE OF CONTENTS

Help Settings	26
Connect Actions	27
User-defined Actions	28
Updating Functionality	29
Phonebook/Configurations	29
Software Updates	29
LAN Prioritized Update	29
Integrated Service Quality Management (SQM)	31
Description	31
Troubleshooting and Monitoring	31
SQM Timing Settings	31
Connection Types	32
Overview	32
Modem	32
ISDN	32
Available Wireless Networks	32
For Wi-Fi	32
For Mobile Data	34
Tested Locations	34
Tested Networks	34
Wireless Broadband	35
Wired Broadband	35
GSM	35
PHS	35
Home Broadband	35
Third-party Security Software Integration	37
Overview	37
VPN Integration	37
VPN Integration Types	37



TABLE OF CONTENTS

1-click	38
1.5-click	39
Auto-teardown	39
Prelogon	40
VPN Gateway Selection	41
Personal Firewall and Anti-Virus Integration	41
SecureConnect	42
1.5-click Integration	42
Auto-teardown	42
Configuration Example	42

Introduction

iPassConnect makes secure, simple and effective network access a reality. No matter where work takes them, iPassConnect users have on-demand mobile-user connectivity to the corporate network through thousands of dial-up, ISDN, PHS, GSM, Mobile Data and broadband access points in approximately 150 countries. This comprehensive connectivity network, iPass® Corporate Access, also includes over 13,000 Wi-Fi and Ethernet access points in iPass-enabled airports, hotels, conference centers and coffee shops.

The iPassConnect™ 3.30 service interface for client connections enables mobile professionals to access corporate networks using virtually any computing device, and connect to Wi-Fi as safely and easily as dial-up. IT managers can gain peace of mind, knowing that centrally managed policies for access, security and usage let them control how users connect. What's more, iPassConnect lets IT staff quickly and easily roll out and maintain the client interface, for lower total enterprise costs.

iPassConnect can be customized to automatically launch other programs such as a VPN, personal firewall, anti-virus application, or a Web browser. This additional functionality ensures a secure and controlled session to address the critical requirements of today's IT departments.

This document gives an overview of the capabilities of the iPassConnect client. You'll find information on general functionality, product features and benefits, installation and upgrading, administrator-controlled policies, and product logistics.

Feedback, suggestions or comments on this document should be sent to dr-product@ipass.com.

Features and Benefits

The features and benefits of iPassConnect include:

Access Functionality

- **Extensive customization** is available through a variety of options that provide exceptional flexibility. For instance, users can hide or show access-point prices, add or delete corporate RAS numbers, or define connection behaviors for individual corporate access points. Client interfaces can even be configured to display the company logo or help desk number.
- **Multiple connection types** including modem, ISDN, PHS, GSM, Mobile Data, Wi-Fi, Wired Ethernet and Home Broadband, gives users access virtually anywhere.
- **An automated and convenient login process** is an integral part of the service interface. This was based on lengthy research into iPass user needs.
- **Location-based interface** makes it fast and easy to select the best possible connection for any given location. Once a user enters their location, they receive a list of all available connections.
- **Local language versions** of iPassConnect are available in Worldwide English, Brazilian Portuguese, French, German, Japanese, Korean, Simplified and Traditional Chinese and Spanish. All of these languages are available through a single installer.
- **Dialing intelligence** greatly reduces help desk assistance calls and improves the user experience. For dial-up calls, it automatically knows whether to add an area code or 1+area code within the United States. Dialing rules in other countries are correctly applied as well.
- **Local number lookup** searches for local dial-up access throughout the United States, speeding connections and reducing long-distance costs. Mobile users simply enter the area code and first three digits of the phone number to see a list of local access points.
- **Timeout policies** for idle and maximum session times prevent connections from being left open indefinitely, ensuring that access is billed only for the time people actually use the iPass service.
- **All-Cities numbers**, available in select regions, are affordable, nationwide access numbers.
- **Toll-free access numbers**, which cut down on separate billings from local phone companies, are also available.
- **Smart Redial** saves time and reduces user frustration by using the built-in redundancy of the iPass network. The iPassConnect service interface automatically dials all local access points in a round-robin fashion, from usually at least three providers in most major business centers, alternating calls until it makes a successful connection.
- **System Tray launch** runs at system startup and places an iPassConnect icon in the system tray. With just one click, users launch the interface and connect using bookmarked locations.
- **Cost center billing** lets IT departments easily track usage by associating users with departments, projects or domain names.
- **Quality-based Phonebook** sorting that automatically checks for an updated Phonebook upon each successful connection. iPass frequently adds new access points and removes problematic ones. This allows users to have the most current numbers available, displayed in order of measured reliability.

Wi-Fi Integration

- **Secure Wi-Fi authentication** is deployed through the Generic Interface Specification (GIS)—the de facto security standard for smart clients and Wi-Fi hotspot access gateways. The entire iPass Wi-Fi

footprint is GIS-enabled. User credentials are sent through an SSL tunnel from the client to the corporation, providing end-to-end protection.

- **Wi-Fi network detection and filtering** automatically detects when a Wi-Fi network is in range and then checks the user's iPass Phonebook for approved access points, which it then displays it to the user. The client only displays if it is a trusted iPass access point. Unapproved hotspots and rogue access points are never shown to the user, protecting the company from unsecured and costly network access.
- **Wi-Fi card auto-configuration** is performed once a user selects a wireless network. iPassConnect automatically configures the Wi-Fi NIC with the proper connection settings, such as SSID or WEP keys.
- **Home Wi-Fi network support** makes user access easier for the increasing number of residential Wi-Fi networks. Users can add home networks to their Phonebook and receive automated detection and configuration for their home wireless connections.
- **iPass Wireless LAN Roaming** makes internal Wi-Fi access easier by providing users and IT departments a single interface and user experience for Wi-Fi access inside the office as well as outside the office.

Security

- **Policy-based End-to-End Security** ensures that endpoints are secured as they connect to the iPassConnect service interface, and before they access the corporate network. This is an essential security requirement for connectivity in the age of broadband and wireless.
- **iPass Secure End-to-End Encrypted Login (ISEEL)** security functionality will protect passwords from the client all the way back to the corporate server—over wired and wireless links. It uses advanced public-key cryptography to protect passwords against eavesdropping and assigns each session a unique ID to help prevent replay attacks.
- **Central management policies** allow IT staff to easily configure and automatically distribute client security to iPass users, ensuring security is enforced during each user login. Policies can be enforced governing the use of network access and different access methods.
- **Third-party security compatibility** is achieved through the iPass Technology Alliance, which allows enterprise security vendors to tightly integrate the iPassConnect service interface with leading VPN, personal firewall, intrusion detection and anti-virus products. This has the two-fold benefit of giving users a secure access link, while simplifying the connection process.
- **One-click VPN integration** automatically passes user credentials (both username and password) to the VPN client when it launches and connects users, eliminating the need for the user to launch and manage a separate application.
- **VPN Auto-teardown** automatically disconnects a user from the Internet if the VPN is ever disabled. If this functionality is desired, it ensures that users always have the VPN running when using the iPass solution. This is important because when used in conjunction with disabling split-tunneling on the VPN, IT managers can be assured that all iPass users are accessing the Internet through the corporate firewall where corporate filters and policies can be enforced.
- **Windows NT domain prelogon** gives remote users the same functionality they're accustomed to using at the office. Now, Windows 2000 and XP users can benefit from domain logon scripting, user-defined drive-mapping capabilities and domain password expiration notification.
- **SecureConnect integration** blocks the user from establishing an Internet connection unless the appropriate anti-virus software, personal firewall or intrusion detection systems are enabled and running. If they're not running before a session, the iPassConnect service interface can invoke the appropriate security services before connecting the user to the Internet.

- **Auto-teardown integration** can be configured to automatically close the Internet connection when a VPN tunnel, personal firewall or anti-virus security solution is disabled or not running.

How the iPass Network Operates

The iPass network allows users to connect remotely and securely to their corporate resources and the Internet. The complete process works as follows:

1. A remote user launches the iPassConnect service interface from a laptop to connect to the Internet using Wi-Fi, dialup, ISDN, GSM, PHS, Mobile Data, or wired broadband.
2. If the user's company subscribes to the iSEEL service option, the user's password is iSEEL- encrypted at the client.
3. The iPass NetServer, located at the remote access point, encrypts the user ID and password, and then forwards both the username and password with the iPass Secure Protocol to one of the globally located iPass Transaction Centers. The iPass Secure Protocol utilizes certificates and SSL tunnels.
4. The Transaction Center decrypts the username and password, identifies the domain name, and then re-encrypts to forward to the authentication database located at the corporate or hosted site. If the user's company subscribes to the iSEEL option, the password is also iSEEL-decrypted at the Transaction Center.
5. The iPass RoamServer receives the request through the iPass Secure Protocol and passes it to the corporate or hosted authentication database.
6. The corporate authentication database grants the authorization approval. The Yes/No response is sent from iPass RoamServer back to the provider, through 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.
7. 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.
8. When the Internet "transaction" is complete, a record of the session is forwarded to iPass Clearinghouse. The iPass Clearinghouse system is responsible for the rating of each transaction. The corporation receives a single, detailed monthly invoice for all usage incurred. iPassConnect also gathers information regarding the connection experience and uploads the data to iPass SQM Servers. This data is transformed into iOQ data where IT managers can view any user's connection experience data and is the basis for iPass Service Level Agreements.

iPassConnect 3.30 Logistics

iPassConnect 3.30 Release

iPassConnect 3.30 will be available during the 4th quarter of 2004. The software is not automatically pushed to any profiles, either test or production. Upgrades must be requested by the IT Manager or iPass Account Manager before pushed to a company's user population.

Ordering the Upgrade

A customer (or Account Manager, Channel Manager or Partner) must log a ticket with the iPass Customer Care team in order to obtain the upgrade. Please ensure the target upgrade/install machine complies with the minimum system requirements listed in the requirements section of this document.

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

Ticket Field	Input
Case Type	Request
Product	iPassConnect
Version	Enter your present iPassConnect version number
Platform	Enter your Operating System platform
Category	iPassConnect
Topic	Modify Client Profile

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 3.30 due to changes in logo dimensions. Please refer to the Logo specification in the Customization section of this document for additional Logo details.

The *Description* section should clearly state the profile is to be updated to 3.30. By default, the profile will receive the same settings that are in the previous version of the client. For example, if the wireless tab is turned off in iPassConnect 2.4, it will also be turned off in the upgrade to iPassConnect 3.30, unless otherwise stated in the 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.

Installation and Upgrading

System Requirements

iPassConnect 3.30 can only be installed on computers that meet the system requirements shown here. If installation is attempted on a system that does not meet these requirements, the iPassConnect installer will indicate to the user which requirements are not met.

Minimum Hardware Requirements

An IBM-compatible PC with:

- Pentium III processor
- 128 MB RAM
- 50 MB free disk space
- 16-bit color mode or higher

Operating System Requirements

- Windows XP (Professional and Home Editions SP 1 or SP 2)
- Windows 2000
(Please note that Windows 98, NT and ME are no longer supported)

Software Dependencies

- Microsoft TCP/IP Protocol installed
- Microsoft Internet Explorer version 6.01 or later. iPassConnect uses Internet Explorer to facilitate securely sending quality data and receiving Phonebook and configuration updates.

Connectivity Dependencies

To use iPassConnect 3.30, you must have at least one of the following connectivity devices installed.

Connection Device	Connection Type
Modem	Dial-up Access
Ethernet Adapter	Wired Broadband
802.11b Wireless Adapter	Wireless (Wi-Fi)
ISDN Terminal Adapter	ISDN
PHS Phone or Data card	PHS
GSM Phone or Data card	GSM
Mobile Data card	Mobile Data

More Installation Notes

- 16-bit (65536 colors) or greater color mode is needed to display all of the customized graphics in the iPassConnect Graphical User Interface
- NDIS (Network Driver Interface Specification) 5.1 Compliance is needed in a user's Wi-Fi card to facilitate automatic Wi-Fi network detection and card configuration. The primary purpose of NDIS is to define a standard Application Program Interface (API) for Network Interface Cards (NICs). There is no

way to generically tell if a card is NDIS 5.1 compliant. A user should check with the Wi-Fi card manufacturer to determine if the card is NDIS 5.1 compliant.

- The Jet database engine. However, this is an integral component of the supported operating systems listed above, and no further installation will be needed. If the Jet engine or its Registry settings ever become lost or corrupted, you can install the latest version from this URL:
<http://msdn.microsoft.com/data/downloads/updates/default.aspx#jet>
- 802.1x support requires all critical Windows updates, and preferably all recommended updates, for Windows 2000 and Windows XP.

Upgrading to iPassConnect 3.30

Previous to iPassConnect 2.20

In order to upgrade to iPassConnect 3.30, a user must be using iPassConnect 2.20 or later. Even if a profile is set to iPassConnect 3.30, a user who is on a version of iPassConnect previous to 2.20 will never receive a prompt to upgrade.

There is no automated method of updating to iPassConnect 3.30 from a version previous to 2.20. A user with an earlier version must contact iPass Customer Care to arrange a new client download, and then perform a new installation of iPassConnect 3.30.

If an installation is attempted on a system that does not meet the minimal install requirements as specified in *System Requirements* on page 12, the iPassConnect installer will present the user with a message that tells the user which of these criteria is not met.

For iPassConnect 2.20 or Later

All customers running iPassConnect clients versions 2.20 and later with the right OS are eligible to upgrade to iPassConnect 3.30. When the customer profile is set to 3.30, the client receives three very small files just like any Phonebook push.

One of these files checks the user's eligibility to upgrade. If the user is not eligible for the upgrade, (meaning the system is using an unsupported version of Operating System or Internet Explorer), the user never sees anything else regarding the update until the system is upgraded to meet the minimum requirements.

If the user is eligible for iPassConnect 3.30, on the next connection, iPassConnect attempts the download of the iPassConnect 3.30 installer. iPassConnect also moves one of the small downloaded files to a run folder. This small file runs the next time the user logs onto the system.

Users having difficulty upgrading from iPassConnect version 2.20 to 3.30 should contact their company help-desk to determine the cause of the failure. iPassConnect logs the exact reason why the user is ineligible and reports it in a new file in the log folder of iPassConnect 2.x named `ipcheck.log`. IT managers should review this log file to identify the specific upgrade problem.

Upgrade Mechanism

Upgrade Files

Once the customer profile has been set to version 3.30, the client will receive three files through a normal Phonebook push. Each file will be placed in the iPassConnect folder and is less than 100kB in size. These three files are:

- `ipccheck.exe`: this executable will run as a post-connect action and verify the client environment. This includes checking for:
 - operating system version
 - Internet Explorer version
 - whether or not the user has administrative privileges
 - correct color settings
 - sufficient disk space
- `ipcdnldr.exe`: this executable is also known as the downloader, and will actually download the iPassConnect 3.30 installer.
- `ipcdnldr.ini`: this is the configuration file for the downloader, and indicates your system's upgrade eligibility. This file is not configurable by the customer.

Upgrade Procedure

To upgrade from iPassConnect 2.20 or later to version 3.30:

1. Start your iPassConnect client
2. If you are not connected to the iPass network, connect to the iPass network as usual. If you are already connected to the Internet through a LAN, you do not need to connect again.
3. On the **Options** menu, select **Update Phonebook**. The three files described above will be downloaded.
4. In iPassConnect 2.x, select **Options > Exit** to exit iPassConnect. In iPassConnect 3.x, right-click the iPassConnect system tray icon and select **Exit**.
5. Start iPassConnect again.
6. Connect to the iPass network using an access point, or through the Home Broadband tab.
7. `ipccheck.exe` will verify whether or not your system meets the requirements.
 - a. *If No*: the upgrade process will be discontinued. iPassConnect records this information in a file in the `log` folder of iPassConnect named `ipccheck.log`. (`ipccheck.exe` will continue to check your system to determine eligibility, although notification ineligibility will only be presented once.)
 - b. *If Yes*: continue to Step 8.
8. If your system is eligible for the installation of iPassConnect 3.30, you will be prompted that there is a new 3.30 client version available. Click **Download Now** to begin the installer download.
9. The installer download process will place the iPassConnect 3.30 installer in the `\Program Files\Common Files\iPassConnect` folder. During this process, an iPassConnect icon will appear in your Windows system tray that indicates that the downloader is running. Double-click the downloader icon in the system tray to show the download status. (The user can cancel the download at any time.) If the download is cancelled, iPassConnect will keep a record of the download progress. This information allows the downloader to recover from the point at which it was interrupted. The downloader will begin again at the next system startup and wait for an Internet connection to continue the download.

10. When the download is complete, you will be prompted with the below message. If you click cancel, the utility will try to upgrade at a later time. If you click Install Now, you will be disconnected and the installation will begin.
11. Follow the installation prompts to complete the installation, including acceptance of the End User License Agreement.
12. The installer will uninstall your current iPassConnect client and install your 3.30 client. When the iPassConnect 3.30 installation is completed, all of the downloaded files (`ipccheck.exe`, `ipdnldr.ini`, and `ipdnldr.exe`) will remain in the iPass folder.
13. After installation is complete, you may now launch and use iPassConnect 3.30.

Upgrade Matrix

The following matrix identifies the upgrade mechanism to upgrade IPC to version 3.30.

<i>iPassConnect Version</i>	<i>SOS Ticket Required?</i>	<i>Upgrade Mechanism</i>
Earlier than 2.20	Yes	Download client and manually install
2.20 or later	Yes	Automated Software Update

Installing iPassConnect 3.30

Installing iPassConnect Software

The installer file for iPassConnect 3.30 is approximately 7.4 MB. Currently, iPass only provides .exe versions of the installer.

By default, the installation program will install iPassConnect into the folder: C:\Program Files\iPass\iPassConnect\

Additional Files

The following files are installed in non iPass directories:

File Name	Folder	Description
ipgina.dll	C:\Windows\system32	.dll for using iPass prelogon
mdc802.1x.sys	C:\Windows\system32\drivers	drivers for automatic Wi-Fi network detection and card configuration

Supported Languages

iPassConnect 3.30 is supported in all the following languages:

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

Please see the Installation options below for information on how to receive iPassConnect in these languages.

User Rights

In order to install iPassConnect, a user must have the ability to write to the HKEY_LOCAL_MACHINE portion of the registry. Typically, this will require write access to the registry or administrative rights. These rights are necessary because iPassConnect installs drivers for the automatic wireless network and configuration functionality. This is a Microsoft limitation, not an iPass limitation.

Restricted and power users will be able to operate iPassConnect 3.30 normally, once an administrator installs it.

In previous versions of iPassConnect, admin rights on the local system were required to install and operate iPassConnect. This has been changed in iPassConnect 3.30 with the advent of a Windows service, called iPCAgent, which enables users with restricted rights to fully access iPassConnect functionality.

System Reboots

iPassConnect may require a system reboot after the installation completes. The table below identifies reboot scenarios which is dependent on Operating System and iPassConnect configuration. If a reboot is required, the user is prompted by the iPassConnect installer.

Operating System	Prelogon Enabled?	Reboot Required?
Windows XP	No	No
Windows XP	Yes	Yes
Windows 2000	No	No
Windows 2000	Yes	Yes

Installation Options

Installation Bundling

If requested, iPass can provide a bundled installer of iPassConnect and another customer-provided program such as a VPN client and or a personal firewall. The installer must be an .exe and must support a silent install. Customer can make this request through an SOS ticket.

EULA Suppression

iPassConnect 3.30 presents the End User License Agreement (EULA) when the software is installed. iPass also 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. This is a legal requirement. There are no exceptions to this requirement.

Running at System Startup

By default, iPassConnect runs at system startup and resides in the system tray. Optionally, iPassConnect can be configured to not run at system startup. Running at system startup allows for quicker launch of the client as well as faster automatic network detection. Customers who use iPass Wireless LAN Roaming (iWLANR) should always have iPassConnect run at system startup so the internal Wi-Fi network will be easily accessible.

Language Installation

iPassConnect can be configured for one of three language installation options:

- *Automatic:* The locale setting on the end user's PC will be used as the language for installation.
- *User select:* allows the end user to determine which language to use for installation.
- *Force language install:* the application will force the user to install in a chosen language.

General Functionality

Profiles

Each build of iPassConnect has a unique profile number and may have different customization settings selected. This allows a customer a customization options for a particular user group and designate 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 group user profile and provide Toll-Free access points in the executive user profile to help keep costs down.

A customer may have multiple iPassConnect profiles. (Please note that a fee may apply for multiple profiles.)

Viewing Client Customizations

iPass has made seeing iPassConnect customization options simple by providing a providing a Profile Viewer on the iPass Portal. Customers may view customization options by profile ID.

Changes to Customizations

Making changes is just as simple as viewing them. Customers may request changes made to their iPassConnect profile by submitting a ticket on the secure Web site.

Connectivity

Dial-Up Networking (DUN)

iPass uses DUN, a standard part of the Windows operating system, to ensure consistent functionality across different modems. iPassConnect creates and uses a dial-up networking connectoid named *iPassConnect* for all modem, ISDN and PHS connectivity.

TAPI

iPassConnect overrides Microsoft Telephony Application Programming Interface (TAPI) dialing rules, because dialing rules such as US 7, 10 and 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.

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. The original settings are restored after the connection is ended or cancelled.

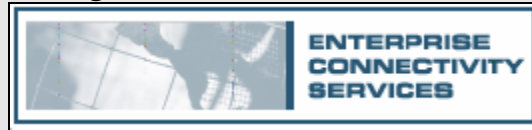
Administrator-Controlled Policies

GUI

Customized Logo

iPassConnect can support a customized corporate look. The customer can submit a corporate logo to replace the blue Enterprise logo on the left side of the main interface in iPassConnect. The iPass watermark logo on the right side will still be present. This logo should be submitted as a Windows bitmap (.bmp) file 267 pixels wide by 59 pixels high.

Default Setting: This is the default logo:



Exit, Not Close

iPassConnect can be configured to change the label on the **Close** button in the bottom right-hand corner of main interface to read **Exit**. By changing it to **Exit**, a user would not only close the GUI but also exit the application with a single action.

Default Setting: The interface has a **Close** button.

Domain

The domain name field (or realm) is used to uniquely identify a user with a specific customer or group within an enterprise. Customers may choose to have multiple domains to segment user communities or to get extra information in Call Detail Records (CDRs).

Empty Domain Name

iPassConnect can be configured with no domain present on the **User Info** dialog. This allows a corporation the flexibility to allow users to fill in a domain.

Pre-set Domain

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. 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 for the character limit is $(1024 - (N - 1))$ where N equals the number of domain names.

Non-editable Domain

iPassConnect can be configured to make the domains non-editable. This feature may prevent a user from accidentally changing or deleting their domain and having difficulty connecting. The domain will appear disabled. The customer can only have one pre-set domain if using this feature.

Domain Hidden

iPassConnect can be configured to completely hide the domain. This feature requires one valid pre-set roaming domain name. This feature can be used to avoid confusion when a user's e-mail address is not the same as iPass logon information.

Default Setting: The default domain setting is an empty domain.

Administrator Settings: An IT administrator may preset a domain name or names. If a domain name is set, by default, it is not editable by a user. An IT administrator can give users the ability to edit the domain or make the domain not present.

Department/Project Code

iPassConnect can be customized to support the use of *department/project codes*, sometimes referred to as *billing codes*. Some companies use these codes to uniquely identify departments or subsets of users, such as “sales” or “product marketing,” especially when billing back charges to individual departments.

At the end of the month, iPass will provide call detail records (CDRs), indicating connections used by the various billing codes to allow for easy segmentation and dissemination (for example, *user@sales.domain.com*). iPass will not use the portion that indicates the department/project code that is “sales” for authentication.

The department/project code is not mandatory.

Each billing code can be a maximum of 16 one byte alphanumeric characters.

Empty Department/Project Code

iPassConnect can be configured with a blank department/project code so that users have the flexibility of entering any alphanumeric text as a department/project code.

Pre-set Department/Project Code

iPassConnect can be configured to include multiple department/project codes and will present them in a drop-down menu of all domains. A total of 1024 characters for all of the department/project codes may be used. Character space is taken up by commas which need to be placed between each department/project code. The formula for the character limit is $(1024 - (N - 1))$ where N equals the number of department/project codes names. Customers may choose to have department/project codes to segment user communities or to receive extra information in CDRs.

Default Setting: By default, the department/project code is disabled.

Administrator Settings: If an IT administrator chooses to enable department/project codes, it can be empty or preset with a series of codes. By default, it is not editable by a user. An IT administrator can give users the ability to edit the department/project code.

Session Management

Idle Timeout

The idle timeout feature helps to control connection costs by automatically disconnecting the user if the system is idle. Idle Timeouts are only available for modem, ISDN and PHS connections. Idle Timeouts are typically used to control costs to keep inactive users from accidentally prolonging a session.

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, iPassConnect will disconnect.

Idle Timeout Traffic Threshold

iPassConnect can be configured with a threshold which needs to be reached to prevent the idle timeout from terminating the connection. 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 specified in terms of bytes per second (bps).

Default Setting: By default, the idle timeout is disabled.

Administrator Settings: If an IT administrator chooses to enable idle timeouts, the default setting for the warning message is 0 – meaning no warning message will be presented to a user. The default setting for traffic threshold is 0 – meaning that the connection must be very idle in order for the idle timeout to take effect. IT administrators need to submit the warning message in the form of minutes for the message to appear. IT administrators need to submit the traffic threshold in terms of bps.

Maximum Session Length Timeout

The maximum session length timeout feature helps to control connection costs by automatically disconnecting the user after a given amount of time has elapsed. Maximum Session Length Timeouts are only available for all connections types.

Maximum Session Length Timeout Duration

iPassConnect can be configured to include a maximum session length timeout. The duration should be submitted in terms of minutes.

Maximum Session Length Timeout Warning Message

The maximum session length timeout can be configured to include a dialog box which gives the user the option to remain connected. If the user takes no action within the time period specified, the user will be disconnected. If the user does decide to remain connection, the timer for another maximum session length begins.

Default Setting: The default setting for maximum session length timeouts is to not enable it.

Administrator Settings: If an IT administrator chooses to enable maximum session length timeouts, the default setting for the warning message is 0 – meaning no warning message will be presented to a user. If a warning message is desired, it must be submitted in the form of minutes.

Redial Settings

General Redial Settings

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. Also, redial settings only affect modem, ISDN and PHS connections.

Attempts

If value “x” exists in the attempts area, iPassConnect will attempt to redial the same number again “x” times if not successful the first time. 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

The Connection Timeout setting is for how long to wait before attempting to connect to another access number.

Default Setting: The default setting for attempts is 2 and for connection timeout limit is 120 seconds. By default, users can not modify these settings.

Administrator Settings: An IT administrator can choose to alter either of these settings and can also give users the option to change them. It is not recommended to change these settings.

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. Smart Redial settings override the redial settings in the previous section.

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. The **Connection Settings** dialog of iPassConnect has two places for Smart Redial, one on the **Modem** settings tab and another on the **ISDN** settings tab. It is not possible to enable or disable these settings separately for each connection type. If this is desired, the Allow User to Enable Smart Redial setting should be enabled so the user can properly enable the appropriate setting.

Default Setting: The default setting for user control of Smart Redial is off.

Administrator Settings: An IT administrator can give a user the ability to turn on or off Smart Redial.

Password Settings

Save Password

The Save Password feature can save the user time as there is no need to input their password with each connection attempt. iPass does not recommend saving passwords on any device due to the risks involved. iPass does make this feature available, but the default setting is to disable it. If Save Password is enabled, the password is stored in an encrypted fashion in the client using a proprietary algorithm. Save password is NOT available in prelogon mode as iPass uses a portion of the user’s domain logon credentials to encrypt the iPass user credentials and since the user has not yet logged into the domain, those credentials are not available for use to encrypt the iPass user credentials.

Allows User to Change Save Password Setting

iPassConnect can be configured allow the user to save or not save the password based on personal preference.

Default Setting: The default setting for Save Password is off.

Administrator Settings: If enabled, the default method is to not allow the user to change the setting, but an IT administrator can give a user the ability to turn on or off Save Password as well.

Cache Password

The Cache Password allows the password to be retained by iPassConnect so if another access point is automatically attempted, the user does not have to enter a password again during that session.

Turn off Cache Password

iPassConnect can be configured to turn off Cache Password. This feature is needed if customers use time-sensitive passwords such as Rosa's SecurID for iPass authentication since the password entered for the first connection attempt will be either out of date or not able to be used a second time.

Default Setting: The default setting for Cache Password is ON.

Administrator Settings: An IT administrator can request that cache password is turned off.

iPass End-to-end Encrypted Login (iSEEL)

iSEEL uses public key cryptography to protect passwords. iPass encrypts the user password before it is ever transmitted over a link. This thwarts an eavesdropper who records the message because they cannot decrypt the password. The password is not decrypted until it reaches the iPass Transaction Center. Not all iPass access points support iSEEL as some providers do not support the password lengths and special characters generated by iSEEL. Please note that iSEEL is a fee-based service.

iSEEL can be configured in three different fashions: None, Mandatory or Mixed Mode.

- *No iSEEL:* This configuration means that iSEEL is not used on any access point.
- *Mandatory Mode:* Mandatory Mode means that only access points which support iSEEL are displayed in iPassConnect and iSEEL is used for every authentication attempt. If the customer has ALL realms in mandatory mode, and does not have a PDA client or Mac client using the domain, the customer can request that the entire domain (not just the profile) is set in mandatory mode. This will effectively force all users to use iPassConnect to gain access using iPass as non-iSEEL passwords will be rejected.
- *Mixed Mode:* Mixed Mode means that iPassConnect will use iSEEL on access points which support iSEEL and will not use iSEEL on access points which do not.

Default Setting: The default setting for iSEEL is off.

Administrator Settings: If enabled, the customer must specify mandatory or mixed mode. Customers must have special approval to set the entire domain to mandatory mode, as this will force iPassConnect usage for all profiles using the domain.

Pricing Settings

Display Modem/ISDN/PHS Pricing

iPassConnect can be configured show modem, ISDN, and PHS pricing for each particular access point.

Display Wi-Fi/Wired Broadband Pricing

iPassConnect can be configured show Broadband pricing for each particular access point. This feature is not allowed at this time. Please consult your iPass account manager for more information.

Currency

iPassConnect can be configured to show pricing in any currency symbol, including but not limited to dollars (\$), pounds (£), euros (€), or yen (¥)

Multiplier

Some corporations want to mark up the pricing displayed to their users to more accurately reflect the amount being charged back to particular department. The multiplier can also be used for currency conversion rate.

Default Setting: The default setting for Display Pricing is Off.

Administrator Settings: If enabled, the IT administrator must specify currency type and currency multiplier.

Proxy Settings

Many customers use proxy servers to help secure Internet access for users. iPassConnect can be configured to work with a customer's proxy server to facilitate Phonebook and configuration updates over a customer's LAN. Please note that these settings are not used to configure a DUN entry or Internet Explorer for a user. They are ONLY used for Phonebook and configuration updates. Also, iPassConnect can not work with a proxy server that requires authentication.

Static Proxy Servers

Proxy Server Address

If a customer wants to enable any of the proxy services for updates using iPassConnect, the first setting is to provide the proxy server address and port. This should be provided in the form of a DNS name or IP addresses and port number.

LAN Updates

If the proxy server needs to be used for LAN updates, this setting needs to be enabled. A simple yes or no is all that is needed for this setting.

Proxy for Customer-Owned Access Points

If a customer has added its own access points into iPassConnect and they require a proxy server to gain Internet access, the administrator should indicate that this setting is changed to yes.

Proxy for iPass Access Points

If a customer requires a proxy server for LAN updates AND is using a VPN (either 1-click or 1.5-click) and is using the SQM/Phonebook delay feature, the administrator should indicate that this setting is changed to yes.

Proxy with Authentication

If a customer uses a proxy server that requires authentication, iPassConnect should be configured to include these user credentials. A new dialog under the **Settings** menu will store a username and password for the proxy server to facilitate a Phonebook update.

Default Setting: The default setting is that all proxy settings are Off.

Administrator Settings: An IT administrator must request that each of these settings is enabled individually.

Proxy Scripts

Some customers with multiple proxy servers within an organization may use proxy scripts in Internet Explorer to manage Internet access in multiple offices. Rather than having a different iPassConnect profile for each proxy server, iPassConnect can work with an automatic proxy script in Internet Explorer (also known as a .pac file.) Please note that this feature is only available for users using Windows 2000 SP3 or later and Windows XP. The functionality is not available in other operating systems, but if configured is ignored by those other systems.

Use Proxy Script

The customer simply needs to indicate a simple yes to the proxy script and it will be configured to get the script from the user's Internet Explorer. It will use this script to roll through multiple addresses until the correct proxy server is found. If this setting is enabled it applies to all access types: LAN updates, iPass access points and customer-owned access points.

Default Setting: The default setting is that all proxy scripts are Off.

Administrator Settings: An IT administrator must specifically request "scripts" with the proxy request for this setting.

Local Number Lookup

Local Number Lookup assists end users with determining the local number to dial in the United States. 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 phone number 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. Access points are sorted by distance, meaning the access point at the top of the list is always going to be the closest to the originating number. If no access point is local, the Toll-Free numbers will appear for the user. If the customer has filtered out the Toll-Free numbers, the user will be told that no local access is available.

Customer-owned Access Points

If a customer has added its own access points to iPassConnect and the access point falls within the local area, it can be presented at the top of the list even if it is farther away than other iPass access points.

Default Setting: Local Number Lookup is On.

Administrator Settings: An IT administrator may disable Local Number Lookup. If an IT administrator leaves Local Number Lookup enabled, customer-owned pops can be requested to be at the top or bottom of the list.

Phonebook Filtering

Removal

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, and price or access type. Filtering can not be done by individual access point or provider. A Phonebook filter should not be used to suppress a specific connectivity type. A connection norgy filter is discussed later in this document.

City Level Dialing

iPassConnect has an option to suppress the numbers under the city name when a user does a search for modem access. This option is helpful if a corporation finds the number of access points in each city to be overwhelming for users. This option is only available for modem access. For all other types of access, it is important to understand the actual access point. (Note that if this feature is selected, Smart Redial should be enabled as well.)

Default Setting: All access points are included and All-cities are shown.

Administrator Settings: An IT administrator may make the specific requests as indicated above.

Customer-owned Access Points

Access Methods

Customers may submit their own modem, ISDN and PHS numbers to be included in iPassConnect. Customers may also add their own wireless networks as part of iPass Wireless LAN Roaming. These access points must use the user credentials from the **User Info** dialog for authentication. Typically, these access points provide direct access to a customer's internal network, which implies that no VPN client is required. (iPassConnect can be configured to take different actions based on whether the connection is being made from a customer-owned access point or an iPass access point – or can take the exact same actions) 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.

Please be aware that the same post-connect actions are used for iPass Wireless LAN Roaming too.

Lastly, please note that there is a contractual limit to the number of customer-owned 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. Please note that if a department/project code is used, it too will be sent as part of the authentication request.

Default Setting: No customer-owned access points are included.

Administrator Settings: An IT administrator may request customer-owned access points be requested. If so, by default, the roaming domain is not included in the authentication request. This setting can be added. Also, iPass Wireless LAN Roaming requires an Additional Services Order Form to be completed.

Help Settings

There are no customizations to the standard Help within iPassConnect. However, customers have two methods to add customized help information. Documentation explaining how customers can create their own custom help for inclusion in iPassConnect is available on the iPass portal.

Customer-Specific Help

Customer can submit a .chm 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 types, iPass and their VPN. See the *Tech Note: Creating a Custom Help File*, on the iPass portal, for more information.

Technical Support Message

iPassConnect can be configured with a custom support message, which is accessed from the main interface of iPassConnect by selecting **Help > Technical Support**, telling users where to call for assistance. See the *Tech Note: Customizing the iPassConnect Technical Support Message*, on the iPass portal, for more information.

Default Setting: The default setting is to not include Customer Specific Help or a Technical Support Message.

Administrator Settings: An IT administrator can include either of these files.

Connect Actions

iPassConnect can be configured to launch programs based on actions taken by the iPassConnect. Administrators must specify the exact path name of the program. An administrator can specify multiple actions to take place at the time in the session (for example, multiple post-connect actions) but must specify whether they are to be made synchronously or asynchronously.

Pre-dial Actions

A pre-dial action takes place just after a user clicks connect but before an access attempt is made, and despite its name, it does work on all connection types. This functionality is typically used to ensure that certain programs are running before a user connects.

Post-connect Actions

A post-connect action takes place just after a user makes a successful authentication, but after a Phonebook/configuration update. These actions are typically used to launch a VPN that does not have specific integration with iPassConnect or is using a CLI (Command Line Interface) from the VPN vendor.

On-error Actions

An on-error action takes place just after a user receives an error message. An example of an on-error action is a customer-written batch program which pops up a support phone number when a user gets an error message, so the user does not have to search for it.

On-cancel Actions

An on-cancel action takes place just after a user clicks **Cancel**.

Disconnect Actions

A disconnect action takes place just after either the user clicks **Disconnect** or a policy disconnects the user. This action does complete before the disconnect takes place. Disconnect actions are typically used to ensure that many online programs are shut down before the disconnect takes place.

Default Setting: No connect actions are set by default.

Administrator Settings: An IT administrator must specify the connection type, the exact path for the installation and if multiple actions are needed at the same stage must state if they are synchronous or asynchronous.

User-defined Actions

iPassConnect can be configured to allow users to enter their own post-connect actions. These actions take place regardless whether a user accesses a customer-owned access point or an iPass access point. Furthermore, the action takes place regardless of the connection type.

Launch Programs

A user can enter their own post-connect action by browsing to the executable for the program. A short wizard takes the user through setting it up.

Default Web Browser

If checked, iPassConnect will launch the default Web browser as a post-connect action.

Default Setting: Both settings are blank and users can edit the information.

Administrator Settings: An IT administrator can disable the either of these services. An IT administrator can also check the Launch Default Web Browser checkbox and make it editable for users.

Updating Functionality

Phonebook/Configurations

A key feature in iPassConnect is the ability for it to automatically receive Phonebook and configuration updates. An administrator cannot turn off automatic Phonebook and configuration updates for a user or profile.

Delay Phonebook

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 users always have the most current Phonebooks.

Size and Frequency of Phonebook Updates

iPass generally publishes a new version of the Phonebook on a weekly basis. iPass may do this less or more often, based on the rate of changes to the iPass network configuration, but weekly is a typical frequency. If a user is two or fewer Phonebook versions behind the newest Phonebook, the user will receive a small file with only the changes. The size of this file will vary based on the number of changes. If a user is more than two Phonebook versions behind, the user will receive a full, replacement Phonebook in a compressed format. The current iPass Phonebook file is about 500 kB compressed.

Local Number Lookup Updates

iPassConnect has a separate file which manages Local Number Lookup. This data is updated on a quarterly basis or more often if major changes are made in local calling rules. This data is compressed is also about 500 kB and is downloaded as part of the regular iPass Phonebook updates process.

Default Setting: No delay is set.

Administrator Settings: An IT administrator can set a delay and must specify that the Phonebook update should wait "x" seconds and try "y" times.

Software Updates

Core software update functionality has been built into iPassConnect 3.30. When later versions of iPassConnect are made available, 3.30 will have a more integrated update to the later version (when specified by the customer administrator). For users upgrading to iPassConnect 3.30 from an earlier version, the software update will include an automatic uninstall of the old version and install of the new one.

LAN Prioritized Update

This feature will allow iPassConnect to take advantage of the times when the user is connected over a broadband connection, to optimize the update experience. If enabled, iPassConnect will only perform a software update when the user is connected to a high-speed connection, typically a LAN or broadband connection.

Default Setting: The default threshold for LAN speeds is 128 kbps.

Administrator Settings: An IT administrator can set a number of attempts to detect a LAN, the LAN poll frequency, and whether or not the user will be prompted to download the software.

Integrated Service Quality Management (SQM)

Description

Service Quality Management (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 through the iPass intelligent Online Quality (iOQ) service to identify user issues for troubleshooting and monitor usage.

SQM Timing Settings

SQM sends data of the current connection, the last disconnect of a successful connection and all failed attempts in between just after a successful authentication to the iPass Virtual Network.

SQM Delay

This feature (which must be used in parallel with the Phonebook Update Delay feature) makes iPassConnect wait x seconds before attempting to send the quality data if the first attempt fails. iPassConnect will attempt to send the data 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 users always have the most current Phonebooks.

Default Setting: No delay is set.

Administrator Settings: An IT administrator can set a retry and must specify that the sending of SQM should wait "x" seconds and try "y" times.

Connection Types

Overview

The IT administrator can configure iPassConnect to any number of the connection types available in iPassConnect. The connection types appear in the client at two different times: when the client is first launched, it will display Home Broadband and an Available Wireless Network if one is automatically detected. A user can also put in location search criteria and the networks types available in the region fitting the location search criteria will be displayed.

Modem

The **Modem** norgy is used most often by iPass users. It is for any connection attempt using a standard modem. iPassConnect is compatible with all modem types, including 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

The **ISDN** norgy is used to facilitate ISDN connections. iPass has both single-channel and dual-channel ISDN access points. Depending on the configuration of the ISDN Terminal Adapter, the user may need to select the ISDN terminal adapter twice in the ISDN settings area of iPassConnect to make a dual-channel connection. Users should consult the documentation of their specific ISDN Terminal Adapter to determine the proper configuration.

Available Wireless Networks

The **Available Wireless Networks** norgy is used to display all wireless networks, including Wi-Fi and Mobile Data, which have been automatically detected by iPassConnect.

For Wi-Fi

Access Points Displayed

iPassConnect will only display the following Wi-Fi access point types:

- iPass-enabled access points
- Personal wireless access points, described below.
- Customer-owned Wi-Fi access points added to iPassConnect as part of iPass Wireless LAN Roaming.

By not displaying other Wi-Fi access points, users and IT managers can be assured that all Wi-Fi access through iPassConnect is trusted.

If iPassConnect detects an SSID that belongs to a single venue, it will display the venue name. If iPassConnect detect an SSID that belongs to multiple venues, it will display *iPass-enabled Access Point*.

Personal Wireless

Personal Wireless gives a user the ability to enter a single SSID (in broadcast mode) and 40/128-bit WEP key and iPassConnect will auto-detect and configure the Wi-Fi card for access. This access point can be set to not require any user authentication. Personal Wireless allows iPassConnect to be the primary interface for using Wi-Fi networks whether the user is at a hotspot or in their home.

Windows XP Zero Configuration Utility

iPassConnect disables Windows XP's Zero Configuration Utility (ZCU) when it starts up. This ensures that the ZCU and iPassConnect are not both trying to use the Wi-Fi card at the same time. Please note that iPassConnect restores the ZCU when iPassConnect exits, so the user does not have to do this manually.

Default Setting: All Wi-Fi functionality is On.

Administrator Settings: An admin can shut off all Wi-Fi functionality, but not individual pieces.

Disconnecting from Wireless Broadband

iPassConnect 3.30 adds a new feature which will help a user properly disconnect from iPass Broadband networks connections. If a user connects to a Wi-Fi or Wired Broadband location and exits iPassConnect or shuts down the computer without disconnecting, iPassConnect will attempt to send a logoff request to the Wi-Fi or Wired Broadband network on behalf of the user.

Wi-Fi Devices

While iPass does not endorse any specific manufacturer's products, the following Wi-Fi devices have been successfully tested for connectivity on the iPass Virtual Network.

Wi-Fi PCMCIA Cards

Vendor	Model	Name	Driver	Firmware
Cisco	AIR-PCM352	Aironet 350 Series WLAN Adapter	8.01.06	4.25.30
Cisco	AIR-PCM340	Aironet 340 Series WLAN Adapter (EOL)	8.01.06	4.25.30
Compaq	WL100	Compaq Wireless PC Card	3.6.7.0	0.8.0
Intel	WPC2011BWW	Intel Pro/Wireless 2011 LAN PC Card	3.0.18.10	F3.00-18
Intel	WCB5000AM	Intel® PRO/Wireless 5000 LAN CardBus Adapter	1.0.1.33	N/A
Orinoco	PC24E-H-FC	IBM/Lucent/Orinoco	7.14.01	N/A
Nokia	C110/111	Nokia Wireless Adapter	0,0,104.0	N/A
D-Link	DWL -650	D-Link Air	N/A	2.0.10.0

Wi-Fi Compact Flash Cards (CF)

Vendor	Model	Name	Driver	Firmware
Netgear	MA701	Netgear MA701 CF Card	N/A	N/A

Built-in Notebooks/Laptops

Vendor	Model	Name	Driver	Firmware
Toshiba	Tecra 9000/9100	Tecra 9000/9100	7.16.0.189	N/A
Toshiba	Portege 4010	Portege 4010	N/A	N/A
Various Centrino-based devices				

USB Devices

Vendor	Model	Driver	Firmware
--------	-------	--------	----------

Microsoft	Wireless USB Adapter	4.10.2222	1.31.9.0
Linksys	Wireless USB Adapter	N/A	2.5

For Mobile Data

The customer is responsible for provisioning and activating a Mobile Data account with a supported card before using the Mobile Data service with iPassConnect. It is important to understand that unlike existing iPassConnect access services, the Mobile Data service is not a connection to the iPass network. Instead, iPassConnect *facilitates a connection* to a carrier network, which provides the actual connection. However, the iPass Mobile Data service adds the security and policy envelope delivered by iPassConnect and related iPass services.

The Mobile Data service is not measured and billed by iPass in the same manner as existing remote access services, such as dial-up connectivity. Instead, connections are measured and billed by the network operator directly to the user or contracting organization. For network integration and connections with the iPassConnect client, iPass charges a monthly fee based on the number of active users.

Networks Displayed

When iPassConnect detects a Mobile Data network, it will display the network name under **Available Wireless Networks**.

Connecting

When the user clicks **Connect**, the Mobile Data card passes carrier authentication credentials to the carrier network. Upon authentication, the user is connected to the Internet through the carrier network and is assigned DNS and an IP address.

Mobile Data Devices

Supported Cards

iPassConnect Mobile Data Services have been tested on the following PCMCIA cards:

GPRS

- Option Globetrotter
- Sierra Wireless AirCard® 750
- Sony Ericsson GC-82 GPRS/EDGE
- Vodafone Mobile Connect 3G/GPRS data card

CDMA

- Sierra Wireless AirCard® 550
- Sierra Wireless AirCard® 555D

Tested Locations

Devices were tested in the San Francisco Bay Area, London, Paris, Munich, Stockholm and Amsterdam.

Tested Networks

Testing was performed on the following networks: Vodafone, T-Mobile, Verizon Wireless, SprintPCS, Cingular, Telecom New Zealand, and Telstra. (Roaming networks may be supported if home carrier has roaming relationship.)

Supported cards listed may work on networks that iPass has not tested. However, we cannot necessarily offer support on every network. If the service provider is not listed here, then iPass cannot offer support.

Wireless Broadband

The **Wireless Broadband** norgy is used to facilitate Wi-Fi connection if the access point was not automatically detected. A user will need to use this if the Wi-Fi card is not NDIS 5.1-compliant. It can also be used as a search mechanism to determine where iPass has Wi-Fi access.

Wired Broadband

The **Wired Broadband** norgy is used to facilitate wired Ethernet connections which are typically found in hotel rooms.

GSM

The **GSM** norgy is used to make connections to GSM-compatible networks. The iPass network has a subset of access points that will allow access through a GSM phone or data card. The speeds of these connections are typically 9.6 Kbps.

PHS

PHS is a mobile phone standard which is currently only available for iPassConnect in Japan, and is mostly used for data communication. DDI Pocket and NTT DoCoMo are the two major service carriers. The user is required to have an account with either DDI or NTT, and a PHS phone. The **PHS** norgy is used to make connections to Japanese PHS (Personal Handyphone Service) networks. A user may connect a PHS phone to a laptop to connect to the Internet.

- *PHS 2.1* is offered by DDI Pocket and allows the phone to move dynamically from 32KBS to 64KBS and back down to 32KBS as demands warrant.
- *PHS 2.0* is offered by NTT DoCoMo and negotiates to either a 32KBS or 64KBS connection and remains at the level for the duration of the connection.

Home Broadband

The **Home Broadband** norgy allows a consistent interface for establishing a secure connection while using an existing Internet 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. Home Broadband connections are treated like customer access point connections for purposes of assigning connect actions.

User Credentials

iPassConnect can be configured to either prompt or not prompt for iPass user credentials. If the customer is using a 1-click VPN, it is strongly encouraged to prompt for user credentials so the user can be passed to the VPN client.

User message

A customized message of up to 56 characters can be displayed under the Home Broadband norgy.

Default Setting: Users are prompted by iPassConnect for user credentials and message reads "Use existing Internet connection."

Administrator Settings: An IT administrator can specify to prompt or not prompt for user credentials as well as customized the message.

Third-party Security Software Integration

Overview

iPass has a very successful strategy of collaborating with leading technology companies to bring comprehensive remote access solutions to the enterprise markets. These partner technologies include Authentication/Authorization/Accounting (AAA) databases, VPNs, personal firewalls and anti-virus applications. Many partners have integrated the iPass technology into their remote networking and security solutions. This integration approach allows iPass to easily support established corporate security policies.

The iPass Solutions Lab in Redwood Shores is available for customers and prospects to see and test the latest third-party software and is used for compatibility and integration testing to always ensure that iPassConnect and the third-party software are working well together.

Default Setting: No third-party VPN software integration is configured in iPassConnect.

Administrator Settings: Each of the individual sections below will outline what information is needed for customization.

VPN Integration

iPassConnect can be integrated with VPN in several different ways.

VPN Integration Types

VPN integration with iPassConnect allows several different types. VPN integration type is described in mouse clicks, which indicate how many credentials are entered into iPassConnect and the VPN client.

Type	Description
1-click	<ul style="list-style-type: none">User enters only one set of credentials into iPassConnect, to establish both the Internet and the VPN connection.The iPass RoamServer authentication and the VPN switch authentication must either point to the same common user database, or else must have the identical active username and password resident in each respective user database.Also called <i>auto-connect</i> integration.
1.25-click	<ul style="list-style-type: none">User enters one set of credentials for iPassConnect to establish an Internet connection. iPassConnect then launches the VPN client, which uses the same username as iPassConnect, but prompts for a different password.1.25-click integration requires that iPass authentication and the VPN authentication use an identical set of usernames for both iPassConnect and the VPN client; however, the passwords can differ.1.25-click integration is valid only for Cisco and Nortel VPN clients.
1.5-click	<ul style="list-style-type: none">User enters credentials into iPassConnect, and then can choose which server to connect to using the VPN client software, but must enter VPN credentials separately. This allows the customer to use separate credentials for iPassConnect and VPN authentication.Also called <i>auto-launch</i> integration.

In addition, VPN integration can include *auto-teardown* and *prelogon* capability.

1-click

Upon successful connection 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. iPassConnect can be configured with 1-click for the following VPN Clients:

- Cisco
- Nortel
- Aventail
- Microsoft
- Check Point

Depending on the VPN product, different information is required, but 1-click can always be configured to work with either iPass access points, customer-owned access points or both.

Cisco

For Cisco, the 1-click interacts with the Cisco .pcf file. The customer must have the Cisco VPN Client version 3.1 or later and a single connection entry name (.pcf file name) common on all users' VPN clients. The .pcf file used for Cisco 1-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 and XP, users must have full registry rights for the Cisco VPN client. For Cisco 1-click, the customer must provide the connection entry name. User credentials for both iPass and the VPN must be the identical.

Nortel

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 1-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).

Aventail

iPassConnect's 1-click integration requires the use of AventailConnect, Aventail's SSL VPN client. It will not function with Aventail's clientless product. The customer must provide the installation path, .exe name and destination IP or network name of Aventail gateway.

Microsoft PPTP

For Microsoft PPTP, iPassConnect supports 1-click for modem/ISDN/PHS when using a PPTP connectoid created by iPassConnect. The iPassConnect-generated PPTP connectoid does not function with Wi-Fi, Wired Broadband or Home Broadband. If the customer wishes to use an existing PPTP connectoid, a script can be run to execute 1-click which will work with all connection types but can only be run on Windows 2000 and XP. See the Tech Note: *Integrating iPassConnect and Microsoft PPTP*, available on the iPass portal.

Check Point

Customer must provide iPass with folder of installation and type of Check Point client being used. 1-click is supported with the following clients:

- 4.1
- NG FP1
- NG FP2
- NG FP3
- AI

1.5-click

Also called *auto-launch*. Upon successful connection to the Internet, iPassConnect will automatically launch the user's VPN client, but the user will be required to enter their VPN credentials and select a VPN gateway or configuration file. Typically, the VPN client will cache the last information entered into the client other than the password so the user will usually only have to click connect and enter the password. iPassConnect can auto-launch any program as a post-connect action, but has done specific testing with the following VPN clients:

- Alcatel
- Avaya (formerly VPNNet)
- Aventail
- Certicom
- Cisco
- Check Point
- Cosine
- Columbitech
- Computer Associates
- InfoExpress
- Intel
- Lucent
- Microsoft
- NCP
- Neoteris
- Netscreen
- Nokia
- Nortel
- Novell
- Secure Computing
- SonicWALL
- Symantec
- V-ONE

Auto-teardown

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 automatically teardown and terminate the Internet connection. This feature ensures that when connected to the Internet the user always has the VPN running, (and, conversely, 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 1-click or 1.5-click VPN integration. Auto-teardown is supported with the following VPNs:

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

No specific information is needed for auto-teardown for any of these VPN clients. The default grace period is 60 seconds and default polling period is 15 seconds. The customer can alter these settings if desired. The customer must specify that whether auto-teardown should be in place for iPass access points, customer-owned access points or both.

Prelogon

Prelogon is the ability to perform operations on a Windows NT-based computer (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 3.30 has the ability to operate on the Winlogon Desktop.

iPassConnect 3.30 has an option to integrate with the Microsoft GINA (Graphical Interactive Network Authentication), 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). When used in conjunction with a 1-click or auto-launched VPN, prelogon for iPassConnect will allow a user to perform a live logon to the NT Domain.

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 does not replace the Microsoft GINA but chains to it. Only one GINA can be installed on a user's machine so if another program has installed a GINA, iPassConnect WILL replace that GINA as the primary GINA. If iPassConnect is uninstalled, it will restore the Microsoft GINA as the primary GINA.

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 antivirus 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 access this folder 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.

See the *Tech Note: iPassConnect and Windows Prelogon*, on the iPass Portal, for more information.

VPN Gateway Selection

If VPN Gateway Selection is enabled (for Cisco or Nortel VPN clients only) then upon connecting to the iPass network, you will be presented with the **Login Information** dialog as usual. You enter your iPassConnect credentials, such as user name and password. Then, under **VPN Gateway**, select the VPN gateway you will use to connect with from the drop-down list. Your VPN client will access the selected gateway as part of your iPassConnect connection process.

Upon first using this feature, iPassConnect will save the selected gateway as the default for all future connection attempts. However, you are free to use a different gateway if the default one is unavailable, by selecting it from the drop-down list.

The list of VPN gateways in the drop-down is determined differently for each VPN client.

- For the Cisco VPN, the gateway list consists of the names of all .pcf files on your computer.
- For the Nortel Contivity VPN, the gateway list is taken from the list of Connection Entries.

Personal Firewall and Anti-Virus Integration

iPassConnect has three different integration types with personal firewalls and anti-virus software: SecureConnect, 1.5-click Integration and Auto-teardown. All of this functionality is supported on the following products:

Personal Firewalls

- ISS RealSecure Desktop Protection Agent (minimum version 3.1)
- Sygate Personal Firewall Pro (minimum version 5.0)
- Sygate Secure Enterprise (minimum version 3.1)
- Zone Labs ZoneAlarm Pro (minimum version 3.7)
- Zone Labs Integrity Desktop (minimum version 2.0)

Anti-virus Software

- McAfee VirusScan Enterprise Edition (minimum version 7.0)
- Norton AntiVirus Corporate Edition (minimum version 8.0)
- Trend Micro (minimum version 5.58)

IT administrators simply need to indicate which product is being used and all three integrations will be activated by default. SecureConnect and Auto-teardown MUST be used together. 1.5-click integration is optional.

SecureConnect

iPassConnect will check and ensure that the anti-virus software and/or personal firewall are running before allowing a user to make a connection. SecureConnect is important as it can help safeguard the device from potentially harmful viruses and software.

1.5-click Integration

Also called auto-launch integration. Used in conjunction with SecureConnect, instead of presenting the user with an error message when the personal firewall or anti-virus software is not running, iPassConnect can automatically launch the personal firewall or anti-virus software to prevent the user from seeing an error message. Of course, if the user does not have the appropriate software installed, the user will see the SecureConnect error message.

Auto-teardown

iPassConnect will poll the personal firewall and or anti-virus software and if the personal firewall or anti-virus software is terminated during the connection, iPassConnect will disconnect the user from the Internet. Auto-teardown ensures that the user always is protected when using iPassConnect.

Configuration Example

All of these integrations can be used effectively together to create a remote access environment which is both secure and easy to use. An example of an ideal iPassConnect configuration can include the following, with the assumption that customer is using a static password for iPass authentication, strong authentication for VPN authentication and has disabled split-tunneling:

- iPass authentication using the same credentials as the user's corporate domain credentials
- iSEEL with no saved passwords
- VPN 1.5-click integration and Auto-teardown
- Anti-virus SecureConnect, 1.5-click integration, and Auto-teardown
- Personal Firewall SecureConnect, 1.5-click integration, and Auto-teardown

The key points that make this a secure and easy-to-use configuration:

Passwords

- Passwords are not stored on the device
- Passwords are encrypted to protect against replay attacks
- Strong authentication is used for VPN authentication.

Data transmission (VPN)

- Auto-teardown forces all Internet traffic to be routed through corporate firewalls – subjected to the same rules as users in the corporate office.
- If a user does not connect to the VPN within a given amount of time, the user will be disconnected.

Device Protection

- SecureConnect and Auto-teardown for anti-virus and personal firewall ensures that the machine is protected whenever the user accesses the Internet and corporate network.

In addition, all this added security is presented to the user in a simple fashion. The customer uses a password for iPass access which is already familiar: the domain password, which is less cumbersome for the user, avoiding the need to enter the same information twice, once for iPass access and once for VPN access.

Auto-launch for VPN access eliminates the need to take action to launch the VPN client; instead, it is automatically presented. And the auto-launch for personal firewall and anti-virus removes the need to remember to launch these products.

About iPass

iPass Inc. delivers enterprises simple, secure and manageable connectivity services for mobile workers as they move between office, home, and remote locations. iPass combines its global network of dial-up, Ethernet and the world's largest Wi-Fi footprint with support for campus wireless LANs and home broadband connections to deliver a unified and comprehensive solution. The award-winning iPassConnect™ user interface, centralized management, leading security features and powerful policy enforcement have made iPass services the choice of hundreds of Global 2000 corporations including General Motors, Dow Corning and Underwriters Laboratories. Founded in 1996, iPass is headquartered in Redwood Shores, California, with offices throughout North America, Europe and Asia Pacific.

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065
United States
Tel: +1 650.232.4100
Fax: +1 650.232.4111
www.ipass.com

Australia
iPass Holdings Pty Ltd.
Level 1, 80 Waterloo Road
Macquarie Park, NSW 2113
Australia
Tel: +612 8876.8700
Fax: +612 8876 8777

United Kingdom
iPass (U.K.) Limited
139 Piccadilly
London W1J 7NU
United Kingdom
Tel: +44 20.7317.4400
Fax: +44 20.7317.4450

Hong Kong
iPass Asia Pte Ltd.
3802A, Lippo Centre
Tower Two
89 Queensway, Admiralty
Hong Kong
Tel: +852.2918.8268
Fax: +852.2918.8278

Germany
iPass EMEA
Region D/A/CH
Wiener Platz 7
D-81667 München
Germany
Tel: +49 89 44 142 - 100
Fax: +49 89 44 142 - 111
infoDach@ipass.com
Netherlands
iPass EMEA
Kingsfordweg 151
1043 GR Amsterdam
Netherlands
Tel: +31 20 491 77 48
Fax: +31 20 491 9090
sales-emea@ipass.com

Sweden
iPass EMEA
Frösundaviks Allé 15
Solna
Stockholm 16970
Sweden
Tel: + 46 (8) 590 041 39
Fax: + 46 (8) 590 041 10
sales-emea@ipass.com

Belgium
Pegasus Park
Pegauslaan 5
1831 Diegem
Belgium
Tel: +32 2 709 29 40
Fax: +32 2 709 22 22
sales-emea@ipass.com

Denmark
South Harbour
Sluseholmen 2-4
Copenhagen South 2450
Denmark
Tel: +45 36 94 45 65
Fax: +45 36 94 45 10
sales-emea@ipass.com

Japan
iPass Japan
Ginko Kyokai Building, 15th Floor
1-3-1 Marunouchi
Chiyoda-ku, Tokyo 100-0005
Japan
Tel: +81 3.3216.7266
Fax: +81 3.3216.7281

Singapore
iPass Asia Pte Ltd.
7 Temasek Boulevard
#23-02 Suntec Tower One
Singapore 038987
Tel: +65 6334.8783
Fax: +65 6337.033

Latin America
Tel: +1 650.232.4186
Fax: +1 650.232.0229
sales-sa@ipass.com