

iPassConnect 3.50 Release Notes

Version 1.1, August 2006

This document contains the latest information on iPassConnect 3.50, including:

- New features
- Technical requirements
- Resolved issues
- Known issues

New Features

iPassConnect 3.50 includes the following features and enhancements:

- **Windows Live Logon:** Windows Live Logon enables the user to log on to the corporate domain from a remote device that is not directly connected to the corporate network, through Ethernet or wireless. iPassConnect intervenes in the login process by connecting the device first to the Internet and then to the corporate domain. Live Logon may be helpful when startup processes that require network connections need to be run on the user's system as part of the logon process, such as access to a file or policy server.
- **AutoConnect to Preferred Networks:** AutoConnect allows the user to connect automatically, with little or no intervention, to any WLAN or Ethernet access point from a list of trusted access points.
- **Ethernet Detection:** Upon connection of an Ethernet access point to a user's laptop, iPassConnect will automatically identify the Ethernet network and present it under **Available Networks**.
- **FlexVPN:** FlexVPN allows fine-grained control over which access point types will trigger integrated VPN launch. You can choose to not launch the VPN for connections to trusted on-campus sites, which can reduce the costs of maintaining a VPN server.
- **Background Updates:** Background updates allow non-intrusive iPassConnect software and Phonebook updates, making optimal use of user bandwidth.
- **Standby/Hibernate Support:** When a laptop is set into Standby or Hibernate power saving modes, iPassConnect will now respond correctly after the Windows session resumes.
- **EAP-TLS and PEAP-TLS:** Support has been added for the EAP-Transport Layer Security protocol.



- **WPA2:** Support has been added for WLAN Protected Access 2 (WPA2), an enhanced version of the 802.11i WPA encryption standard.

Technical Requirements

Minimum Hardware Requirements

- Pentium III processor (or equivalent AMD processor)
- 256 MB RAM
- 100 MB free disk space
- TCP/IP Protocol
- 16-bit color mode

Connectivity Device Requirements

iPassConnect requires one or more connectivity devices installed, depending on your intended connection type:

- A supported WLAN adapter for a WLAN connection. (any NDIS-compliant 802.11b and 802.11g Wi-Fi device)
- A supported Mobile Data card for a Mobile Data connection. (A complete list of supported Mobile Data cards can be found in the *Mobile Data Configuration Guide*, available from the iPass Portal.)
- Ethernet adapter for a Ethernet connection
- 56K v90/92 modem for a dial-up connection
- GSM modem for GSM connections
- ISDN terminal adapter for an ISDN connection
- PHS phone for PHS connections

Operating System Requirements

- iPassConnect 3.50 is supported on Microsoft Windows 2000 SP 4 or later, and Windows XP Home or Professional (Service Packs 1 and 2). iPass strongly encourages the use of Windows XP SP 2. In addition, you should install all Microsoft-recommended updates for your operating system.
- Microsoft Internet Explorer 6 is required. At the time of publication Microsoft Internet Explorer 7 is not supported with iPassConnect 3.50. iPass is committed to full support for IE7 from its general release date. Further details will follow in a future communication.

Supported Languages

iPassConnect supports the following languages:

- Brazilian Portuguese
- English



- French
- German
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

Resolved Issues

This release of iPassConnect resolves the following issues.

General

- **Web Access Not Available Before Prelogon:** A security issue has been closed that allowed users of prelogon/Live Logon access to the Web through the **iPass on the Web** menu item before login.
- **Obsolete Access Points No Longer Causing iPassConnect to Terminate:** iPassConnect will no longer abruptly terminate if a Phonebook update removes the last searched access point from the Phonebook.
- **Roaming Profiles:** Windows roaming profiles are now uploaded correctly.
- **Bookmark Deletion:** You can now delete two Bookmarks that have the same name without causing iPassConnect to abruptly exit.
- **Disconnect on System Tray:** You can now disconnect correctly using the System Tray menu **Disconnect**, without disabling the other menu items.
- **Update Sequencing:** An issue has been resolved that would cause iPassConnect to abruptly terminate after performing a full Phonebook update which was quickly followed by a manual software update.
- **Supported Software:** iPassConnect will now correctly inform the user whether or not a software update meets the system requirements.
- **Removal of Last Searched Dial Access Point:** iPassConnect would terminate if the last searched dial access point was removed by a Phonebook update which completed while iPassConnect is not running. This issue has been resolved.

WLAN

- **Non-Broadcast Access Point Detection Caused Existing WLAN to Disconnect:** iPassConnect will no longer disconnect any existing WLAN connections made outside of iPassConnect if non-broadcast WLAN access points are detected.
- **Renaming non-iPass WLAN Access Points:** You can now rename Bookmarks for non-iPass WLAN access points.



- **WLAN Disconnects Correctly When User Moves:** An issue has been resolved where iPassConnect was showing some WLAN users as connected even if they physically moved away from a local WLAN hotspot. They will now correctly show as disconnected.
- **Non-Broadcast Networks Not Shown as Available:** An issue has been resolved that was causing some non-broadcast WLAN networks to be displayed in **Available Wireless Networks**.
- **Non-Broadcast Access Points Not Shown:** iPassConnect will no longer detect non-broadcast access points when they are filtered from the Phonebook.
- **Persistent WLAN Connection Even if Interrupted:** For some WLAN connections, if iPassConnect was used to make the connection, but the connection was terminated outside of iPassConnect (such as the access point going down, or the WLAN radio being switched off), then iPassConnect would still show the connection as active. WLAN connections will now correctly show the connection status if interrupted outside of iPassConnect.
- **Redial Action Failure and WLAN:** iPassConnect will now correctly stop the connection if a synchronous, monitored, redial action fails on a WLAN connection.

PHS

- **Last Searched PHS and Home Broadband Access Points:** iPassConnect will now store the last searched PHS and home broadband access points. 85902
- **PHS City Level Bookmarks:** PHS city-level Bookmarks now work correctly.
- **PHS Redial and Smart Redial:** Smart Redial and redial attempts will now work correctly for PHS access points. (86087, 86088)

Known Issues

The following issues are known for iPassConnect 3.50.

General

- **Not Compatible With DeviceID Verify Calling Process:** Customers wishing to use DeviceID in conjunction with iPassConnect 3.50 should configure their DeviceID server with `Verifying Calling Process = 0`.
- **Rapid Login/Logoff:** iPassConnect may abruptly terminate if a user logs in and then quickly logs off without allowing iPassConnect to properly initialize. Always allow iPassConnect login attempts to time to complete properly.
- **USID for non-iSEEL Access Points:** iPC does not properly generate an SQM Unique Session ID SQM for connections made using non-iSEEL-enabled access points.
- **Same Install_ID on Cloned Systems:** When a system is cloned (either re-imaged or a hard drive image is copied to a new computer) iPassConnect sends the same value for `install_id` as part of SQM data. This can cause faulty SQM data for users on the cloned system with the same windows login credentials but different iPassConnect credentials.



- **Proxy Authentication Window Inactive:** When the **Proxy Authentication** window is displayed, it will be inactive and be displayed in the background.
- **Incorrect Phonebook Update Messages:** Occasionally, when a user performs a manual Phonebook update, a message reading “Initializing” may be displayed for a few moments, before displaying “Operation timed out.” However, information in the update.log will confirm that the update was completed successfully. The problem can be temporarily suppressed by restarting the Periodic Update service.
- **Uninstall Fails:** Sometimes the file `backup\uiconfig.ini` is not deleted on uninstallation.

WLAN

- **Shared SSIDs:** it is possible to have a common SSID shared between both CBook and PBook entries with different characteristics defined. (For example, one SSID could be set to AutoConnect, and the other would not be.) This can lead to unpredictable connection behavior because iPassConnect will attempt to use the characteristics of the first matching SSID.
- **Pop-Up Doesn’t Display SSID for AutoConnect:** When AutoConnected to a local WLAN network, the SSID will not be displayed in the bubble pop-up in the System Tray.
- **Some Failed WLAN Connections Not Timing Out:** On some failed WLAN connection attempts, iPassConnect does not time out the connection attempt. Restart iPassConnect to cancel the attempt.

Mobile Data

- **Unable to Use Mobile Data After Phonebook Upgrade Without Software Upgrade:** When a profile is upgraded to version 3.50, users who update their Phonebooks but refuse the software upgrade will not be able to connect with Mobile Data. To re-enable Mobile Data connectivity, the user must complete the pending software upgrade.
- **Sierra Wireless AC 750:** The Sierra Wireless AC 750 card, a Mobile Data device, will be displayed by iPassConnect as an Ethernet device under **Settings > Connection Settings > Ethernet**.
- **Mobile Data Requires Dynamic IP Assignment:** iPassConnect does not support the use of Mobile Data networks that require static IP addresses. (For example: This includes Vodafone in Spain, Malta and Egypt.)
- **Mobile Data Interruption:** On some Mobile Data connections, initiating a connection but clicking **Cancel** before completion can cause iPassConnect to freeze. You will need to close iPassConnect using the Windows Task Manager and then re-start it.
- **Mobile Data Fails to Connect After Hibernation:** After some computers are brought back from hibernation, some Mobile Data cards may fail to connect to any detected Mobile Data networks. You will need to reboot the laptop in order to reconnect.

Automatic Ethernet Detection

- **Multiple Network Adapters and Ethernet Detection:** When a laptop has multiple network adapters, Ethernet Detection may not correctly characterize networks.
- **USID for Auto-Detected Ethernet:** iPassConnect does not use USID for automatically detected Ethernet, except when part of an iSEEL login for a profile with Mixed Mode disabled.

Windows Live Logon

- **Windows Live Logon Completes Even if Tunnel Creation Fails:** Even if the VPN tunnel is not successfully created, the Windows Logon process will still proceed.
- **Sygate PFW and McAfee AV:** If a user with an iPassConnect profile configured for both Windows Live Logon and either Sygate PFW or McAfee AV SecureConnect integration logs off their PC while either service is stopped, then iPassConnect will freeze at the Initializing state if a Live Logon is attempted.
- **Password Encryption Based on Hardware:** In Live Logon mode, a saved password is encrypted with reference to the computer's hardware characteristics only and does not take account of the Windows user logon credentials, because no Windows user credentials are available until after login. This results in a slightly lower level of encryption for saved Live Logon passwords than for passwords saved following desktop login.

