

Frequently Asked Questions: iPassConnect 3.50

Version: 1.0, August 2006

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065 USA



www.ipass.com
+1 650-232-4100
+1 650-232-0227 fx

TABLE OF CONTENTS

| | |
|--|-----------|
| Overview | 5 |
| When will iPassConnect 3.50 be available? | 5 |
| What is the business need for iPassConnect 3.50? | 5 |
| What are the key new features and benefits of iPassConnect 3.50? | 5 |
| Which languages are supported? | 6 |
| Which operating systems are supported? | 6 |
| Is this an opt-in release? | 6 |
| Automatic Connection to Preferred Networks (AutoConnect) | 7 |
| What is AutoConnect and how does it work? | 7 |
| Can I configure multiple AutoConnect networks? | 7 |
| Are there situations where AutoConnect will not work? | 7 |
| Is AutoConnect limited to Wi-Fi networks? | 7 |
| Will iPassConnect AutoConnect to iPass public (chargeable) Wi-Fi networks? | 7 |
| How does a user enable AutoConnect? | 7 |
| Is AutoConnect suspended in response to an authentication failure? | 8 |
| Ethernet Detection | 9 |
| What is Ethernet detection and how does it work? | 9 |
| Will iPassConnect disable Wi-Fi when connected to the LAN? | 9 |
| Why show Open Ethernet? | 9 |
| Why show both Home Broadband and Open Ethernet? | 10 |
| How do I configure Ethernet detection? | 10 |
| Windows Live Logon (Formerly Prelogon) | 11 |
| What is Windows Live Logon and how does it differ from prelogon? | 11 |
| Can I use this feature with other GINA applications? | 11 |
| How are user credentials handled? | 11 |
| How secure are my Windows credentials with Single Sign On? | 11 |
| Is VPN integration essential for Windows Live Logon? | 12 |
| What VPNs and connection modes are supported? | 12 |
| Can I upgrade to a Live Logon profile? | 12 |



TABLE OF CONTENTS

| | |
|---|-----------|
| Are there any features I cannot use with Windows Live Logon?..... | 12 |
| Is Nortel Logoff on Connect (LOC) still supported?..... | 12 |
| Flexible VPN Launch (FlexVPN) | 13 |
| What is FlexVPN?..... | 13 |
| What are the supported network types?..... | 13 |
| Is FlexVPN limited only to VPN integrations?..... | 13 |
| Can I use FlexVPN Launch with VLaunch?..... | 13 |
| What does the discontinuation of VLaunch mean for me?..... | 13 |
| Authentication and Wireless Security | 14 |
| What new authentication modes are available in iPassConnect 3.50?..... | 14 |
| What wireless security modes are available?..... | 14 |
| Will iPassConnect automatically use a certificate if it is the only certificate in the cert store?..... | 14 |
| Other New Features | 15 |
| What is the Standby/Hibernate Feature? | 15 |
| Are the Wi-Fi drivers different in this release?..... | 15 |
| How does iPassConnect 3.50 interact with the Wireless Zero Configuration Service? | 15 |
| What is the IE Proxy Manager option? | 15 |
| What else is new in the User Interface? | 15 |
| Updates and Provisioning | 17 |
| How has the update process changed in iPassConnect 3.50? | 17 |
| Are all IE proxy features supported? | 17 |
| What happens when iPassConnect encounters a proxy requiring authentication? | 17 |
| Are all updates performed through Background Update? | 17 |
| Will Background Updates work with a 3rd party connection manager or supplicant such as Funk Odyssey, Intel Proset or ThinkVantage Access Connections? | 17 |
| Has the CBook format changed? | 17 |
| What is the process to upgrade to iPassConnect 3.50? | 18 |
| What applications and traffic types do I need to configure in my firewall in order for iPassConnect to be able to connect and update successfully? | 18 |
| Can personal Wi-Fi be transferred when upgrading to 3.50?..... | 18 |
| How do I start using these new capabilities?..... | 18 |



TABLE OF CONTENTS

Other Documentation **19**

What other documentation is available on iPassConnect 3.50?19

Copyright © 2005, iPass Inc. All rights reserved.

Trademarks

iPass, iPassConnect, and the iPass logo are trademarks of iPass Inc. All other brand or product names are trademarks or registered trademarks of their respective companies.

Warranty

No part of this document may be reproduced, disclosed, electronically distributed, or used without the prior consent of the copyright holder.

Use of the software and documentation is governed by the terms and conditions of the iPass Corporate Remote Access Agreement, or Channel Partner Reseller Agreement.

Information in this guide is subject to change without notice.

Every effort has been made to use fictional companies and locations in this manual. Any actual company names or locations are strictly coincidental and do not constitute endorsement.



Overview

When will iPassConnect 3.50 be available?

iPassConnect 3.50 will be available in August, 2006.

What is the business need for iPassConnect 3.50?

Universal Client Solution. There is no need to purchase and deploy one product for campus use and another for roaming; iPassConnect 3.50 is a fully featured client connection manager equally at home whether connecting to public or private networks.

What are the key new features and benefits of iPassConnect 3.50?

| Feature | Description | Benefits |
|--------------------|--|--|
| AutoConnect | Automatic connection to preferred Wi-Fi networks and 802.1X Ethernet | User quickly gets connected to preferred Wi-Fi networks with minimal interaction when iPassConnect determines this is appropriate. 802.1X over Ethernet capability brings iPassConnect up to par with Windows XP and is one less use case requiring maintenance of an alternate supplicant. |
| Ethernet Detection | Ethernet detection is a feature to sense an active Ethernet connection so that it can be offered as an "Available Network" in iPassConnect alongside existing detected wireless services, such as Wi-Fi or Mobile Data | <ul style="list-style-type: none"> ■ User is alerted to presence of iPass services that might otherwise be overlooked. Extends the universal connection model into new space by facilitating connections to non-iPass Ethernet. ■ Detection process enables iPassConnect to make intelligent decisions about when to AutoConnect. |
| Windows Live Logon | Presents a new Windows logon screen containing the option to Logon with iPassConnect in place of the Log on using Dial-Up Networking option in the regular Windows logon dialog. This is achieved by replacing the default Windows GINA module. | Live Logon gives remote users the same functionality they're accustomed to using at the office. Windows 2000 and XP users can benefit from domain logon scripts, Windows Policy application, user-defined drive-mapping capabilities and domain password expiration notification. |
| Background Updates | This module will periodically look for Phonebook and configuration updates and SQM data to upload using any connection available at that time, even those not made using iPassConnect and it will automatically discover proxy settings when they are needed. Updates are performed in the background using trickle download technology with bandwidth throttling and support for interrupted downloads. | <ul style="list-style-type: none"> ■ Enables automatic updates over the LAN so user's Phonebooks will be updated when users go on the road. No more need to do a manual Phonebook update before you leave for a trip. ■ Runs in the background so user will not need to wait for the Phonebook update to occur. ■ iPassConnect is nearly always up-to-date, even if it hasn't been used recently. Failed session records are uploaded to IOQ over any network connection allowing true diagnostics for user connection problems. iPassConnect profiles no longer tied to a single unauthenticated proxy server. Administrator no longer needs to provide proxy settings to iPass. Allows for more |

| | | |
|--|--|--|
| | | flexible software deployment options in future. Highly configurable for fine tuning |
| Support EAP-TLS and PEAP-TLS for On Campus Roaming | EAP-TLS and PEAP-TLS 802.1X are certificate authentication modes for secure authentication on campus networks. Certificates from the user's personal certificate store (in Microsoft Internet Explorer) are available for selection; and in Windows Live Logon, from the local machine store are used. | <ul style="list-style-type: none"> ■ Use iPassConnect for On Campus connections to provide secure and easy to support Wi-Fi campus connections as well as when users are outside of the office. ■ No need to use a separate connection client for campus connections. Works with existing certificate management infrastructure. |
| WPA2 for secure enterprise and personal networking | WPA2 support for both personal (pre-shared key) and enterprise (802.1X) use. | Enterprise grade data encryption, especially for 802.1X networks but also for small businesses who wish to use on site PSK in lieu of a full scale VPN and AAA service. |
| Flexible VPN launch | Fine grained control necessary for determining when a VPN should be invoked according to the network type used for the connection | Powerful integration options to enable VPN suppression for 802.1X campus networks but also to allow a wide range of custom integrations e.g. no policy remediation on mobile data or SSL VPN only on dialup. Provides a migration path from legacy integrations (for example, VLaunch) without breaking existing deployed base. |
| Standby / Hibernate support | iPassConnect 3.50 detects when its host is about to enter a suspended mode and takes appropriate action. When resuming from a suspended state, iPassConnect will re-start network detection including scanning for AutoConnect networks. | iPassConnect is always ready to use on resume with the GUI and device states matching the current network environment. |
| Internet Explorer proxy management | Gives an administrator the option to have iPassConnect apply the IE LAN proxy settings to all connections. | Eases management of the appropriate proxy settings for each type of connection |

Which languages are supported?

iPassConnect 3.50 is supported in English, Brazilian Portuguese, French, German, Japanese, Korean, Simplified Chinese, Spanish and Traditional Chinese.

Which operating systems are supported?


Microsoft Windows 2000 SP4, XP Professional SP1 and SP2. and XP Home SP 1 and SP2 are all supported. Limited testing has been performed with Windows XP Professional SP1, but to guarantee the best experience iPass strongly encourages the use of SP2 with Windows XP.

Is this an opt-in release?

Some customers have been notified previously that iPass will be automatically upgrading their iPassConnect 2.x client to 3.50 on September 1, 2006, in line with the iPass End of Life policy. However, in general, customers will not receive iPassConnect 3.50 automatically. Customers who want to upgrade an existing profile to iPassConnect 3.50 must order the upgrade by submitting a Support Ticket.

Automatic Connection to Preferred Networks (AutoConnect)

What is AutoConnect and how does it work?

AutoConnect is a configurable option that simplifies the Wi-Fi connection process by automatically initiating a connection attempt to networks configured for this feature. The feature can be configured in the CBook or as a Personal Wi-Fi service (indicated by the  icon). iPassConnect also AutoConnects to customer-defined 802.1X Ethernet services.

Can I configure multiple AutoConnect networks?

Yes, you may configure any number of your Personal and Customer Wi-Fi networks for AutoConnect although only one can be connected at a time. Note that all services with a common SSID must be configured with the same AutoConnect behavior.

Are there situations where AutoConnect will not work?

AutoConnect will only commence when iPassConnect detects an eligible network and when the current state of the client indicates a connection would be appropriate. For example, iPassConnect will not AutoConnect if an Ethernet connection with open Internet access is detected, nor will it connect if an explicit disconnect has occurred since the last connection or restart of iPassConnect (for example, a user disconnect or VPN teardown).

Is AutoConnect limited to Wi-Fi networks?

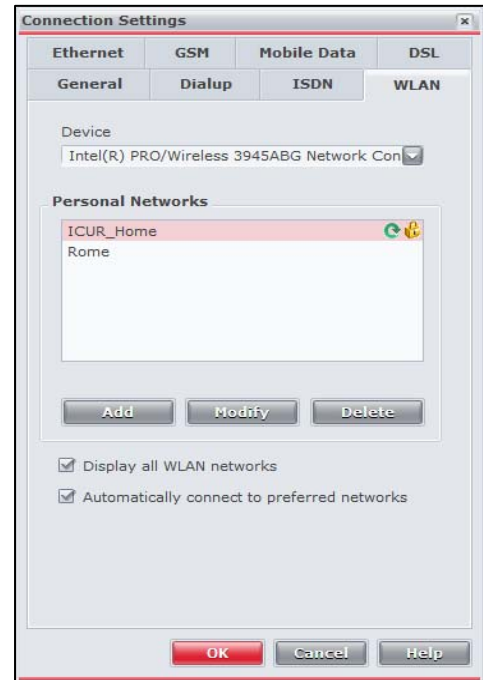
In general yes, although AutoConnect to 802.1X over Ethernet is also provided to match the feature set of the Windows XP Zero Configuration Service. AutoConnect to Mobile Data services has not been implemented in this release.

Will iPassConnect AutoConnect to iPass public (chargeable) Wi-Fi networks?

No. The AutoConnect feature can only be applied to campus and personal Wi-Fi and 802.1X Ethernet services. iPass may extend the scope of the feature in the future.

How does a user enable AutoConnect?

To enable AutoConnect, select **Connection Settings > WLAN**, and then check **Automatically connect to preferred networks**.



Is AutoConnect suspended in response to an authentication failure?

No. This decision was taken to keep the client behavior simple, and in recognition of the fact that not all connection failures reported to the client as authentication failures are necessarily because of the user credentials (or the certificate) supplied. If the Cache Password feature is disabled the client will prompt for a password on each AutoConnect attempt. The retry attempt rate will progressively slow down in response to repeated connection failures and AutoConnect will be suspended if the user cancels a connection attempt.

Ethernet Detection

What is Ethernet detection and how does it work?

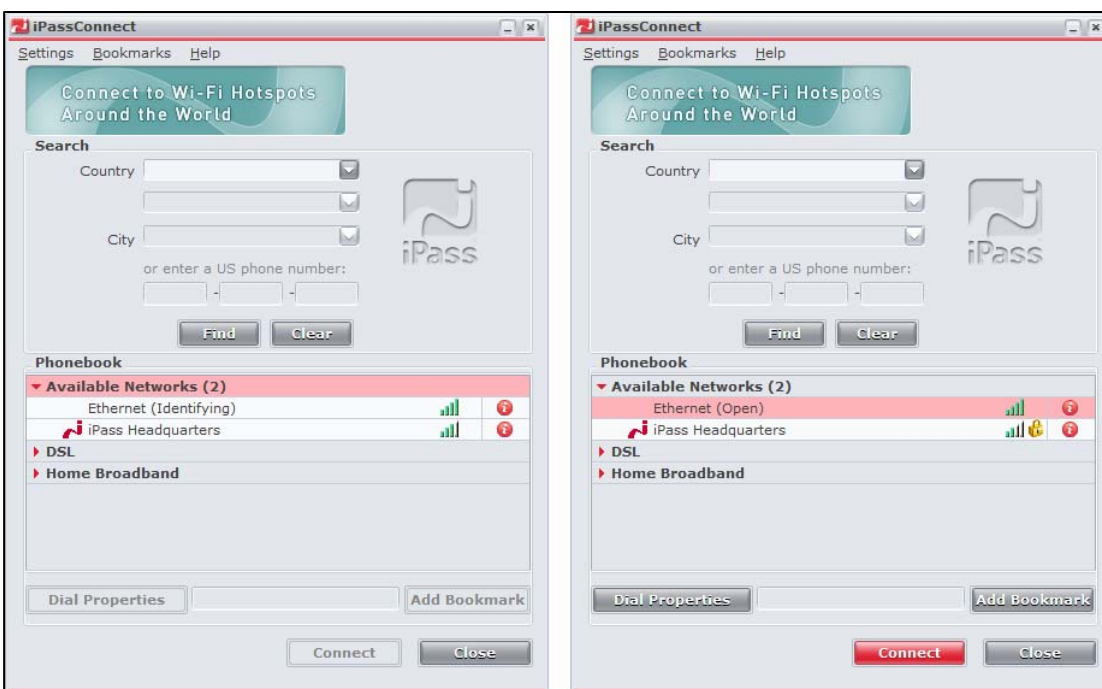
Ethernet detection will sense an active Ethernet connection so that it can be offered as an available network in iPassConnect alongside existing detected wireless services, such as Wi-Fi or Mobile Data. (**Available Wireless Networks** on the main interface has now changed to **Available Networks**, with Ethernet always shown at the top of the list when available.)

When an active Ethernet cable is attached to the PC, iPassConnect quickly performs a series of tests to identify whether the connection represents an open Internet connection, an iPass-enabled walled garden, a non-iPass walled garden, or an 802.1X service.

In some instances, iPassConnect will recognize the access procedure (such as GIS) but will not be able to definitively identify the service as an iPass location. In these instances, iPassConnect will ask the user whether or not to use iPass credentials in the connection attempt.

Will iPassConnect disable Wi-Fi when connected to the LAN?

No, although AutoConnect will be suspended if an open Ethernet connection is detected. iPass is planning to implement a feature to disable unwanted interfaces in a future release of iPassConnect.



Why show Open Ethernet?

When a user is connected to open Ethernet, the user already has Internet connectivity. However, in many instances, for example, when at home or when visiting customer premises, the user may still need to launch a VPN or to run other network services. The iPassConnect open Ethernet option provides a convenient way to achieve this with a single click.

A hotel room Ethernet service may initially require authentication but will then remain open for the remainder of the stay and iPassConnect 3.50 can accommodate this situation by dynamically updating the Available Networks entry as needed.

iPassConnect 3.50 uses the availability of open Ethernet as a factor when deciding whether to initiate an automatic connection to an available Wi-Fi network.

Why show both Home Broadband and Open Ethernet?

A user connected to Open Ethernet can generally achieve the same connection experience with Home Broadband, but Open Ethernet is superior as it is dynamically detected, is associated with a specific interface and is pre-qualified for Internet access. However, Home Broadband is a very popular method of connecting and so is retained in iPassConnect 3.50. iPass will continue to solicit feedback on the future interface design.

How do I configure Ethernet detection?

Ethernet Detection is automatically enabled on any iPassConnect 3.50 profile configured with the Wired Broadband option. In some instances, iPassConnect will detect multiple Ethernet interfaces and the user must select the appropriate interface from **Connection Settings > Ethernet**.

Windows Live Logon (Formerly Prelogon)

What is Windows Live Logon and how does it differ from prelogon?

iPassConnect 3.50 offers the Windows Live Logon option in place of the legacy prelogon service. This option inserts a new GINA (Graphical Identification and Authentication) module at the start of the Windows logon sequence which includes an option to logon with iPassConnect (in place of the Log on using Dial-Up Networking option in the regular Windows GINA). When this option is checked, iPassConnect will be launched before the Winlogon sequence, to allow a live Windows domain logon without further user input.



The major improvements from prelogon are that this is a fully-featured GINA, rather than a GINA “stub”, and offers fully configurable credential handling, including Single Sign On. In addition, it is compatible with a wider range of VPNs (see page 12).

Can I use this feature with other GINA applications?

No. At this time, the iPassConnect GINA can only chain to the MSGINA, although the architecture allows for the possibility of extensions to chain to other GINAs in future. iPass will consider other integrations in response to customer demand.

For this release, iPassConnect will only recognize and interact with the Windows MSGINA. To protect the system environment, the iPassConnect installer will not proceed if another GINA is detected. When upgrading to a Live Logon profile it is essential that the administrator ensures none of the upgrade recipients users has another GINA in place otherwise they could become stranded without any iPassConnect client.

How are user credentials handled?

The iPass GINA collects the Windows credentials and passes them to the Windows GINA (no longer seen by the user) using standard GINA chaining. If desired, the administrator can specify that these credentials also be passed to iPassConnect and/or the VPN, allowing for a full range of Single Sign On options including the ability to have the same set of credentials used by iPassConnect, VPN and Windows logon. iPassConnect can also be configured to re-use the Windows username but to prompt separately for a different password.

How secure are my Windows credentials with Single Sign On?

By default, the Windows password is not retained by iPassConnect and is not propagated to the VPN client. If iPassConnect is configured to reuse the password then it will store it in encrypted form and

will decrypt for the shortest possible interval when needed. iPassConnect never writes the Windows password to disk.

Is VPN integration essential for Windows Live Logon?

Yes. There may be some instances where a connection to the domain controller is possible without a VPN but the VPN tunnel should be considered essential for roaming or remote use.

What VPNs and connection modes are supported?

The iPass Windows Live Logon service supports the VPN clients from Cisco, Check Point and Nortel. (The Nortel VPN client must be installed as a service for this mode.) In addition, the Live Logon service also supports connections made through secured private networks where a VPN might not be required (for example, 802.1X encrypted Wi-Fi such as WPA2 with EAP-TLS). Note that the Windows Live Logon feature does not support VLaunch implementations.

Information on the specific VPN releases tested is available on request.

Can I upgrade to a Live Logon profile?

Yes. The upgrade to iPassConnect 3.50 allows for the installation of the iPassConnect Live Logon service. However a full upgrade is required. Windows Live Logon cannot be enabled through a Phonebook update.

Are there any features I cannot use with Windows Live Logon?

Features that could raise security concerns are disabled in Live Logon mode. These include the **Help** and **iPass on the Web** menu items, as well as user-defined Connect Actions, since these all allow the user to browse for files before authentication. Also, connections to non-iPass venues that require a Web browser launch to facilitate authentication are also prohibited (an explanatory message is displayed to the user in this case).

Is Nortel Logoff on Connect (LOC) still supported?

The LOC option has not been tested with iPassConnect 3.50 and this configuration is now deprecated.

Flexible VPN Launch (FlexVPN)

What is FlexVPN?

This feature provides the fine-grained control necessary for determining when a VPN should be invoked according to the network type used for the connection. The most common use for this feature is anticipated as being to launch a VPN in all instances *except* on a private secure Wi-Fi connection (for example, an 802.1X authenticated WPA2 service). The feature defines 8 distinct network types that can be independently configured as required.

What are the supported network types?

iPass Broadband, iPass Dial, Customer Dial, Customer Encrypted 802.1X Wi-Fi, Customer Wi-Fi other, Customer Ethernet, Mobile Data, All Other Networks. Further network types may be added in future releases.

Is FlexVPN limited only to VPN integrations?

No, the same logic can be applied to any iPassConnect connect action integration and also to the AppMonitor VPN monitoring utility.

Can I use FlexVPN Launch with VLaunch?

No, VLaunch is now a deprecated feature and will not be further enhanced. Where possible, customer VPN integrations should be migrated from VLaunch to connect actions or shim implementations. FlexVPN in iPassConnect 3.50 provides customers with a smooth migration path to assist with this transition.

What does the discontinuation of VLaunch mean for me?

iPass plans to remove the VLaunch function from the client in the next 12 months and will not offer any further fixes or enhancements. iPassConnect 3.50 is a great time to migrate your legacy VLaunch VPN implementations.

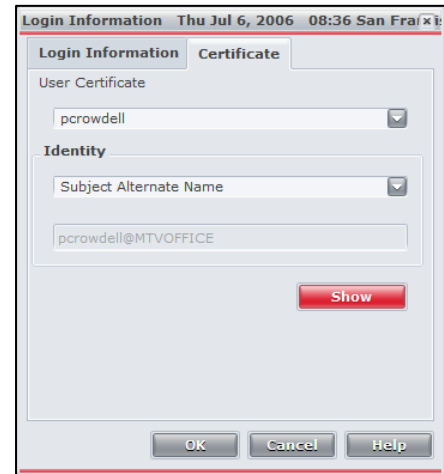
Authentication and Wireless Security

What new authentication modes are available in iPassConnect 3.50?

iPassConnect 3.50 introduces support for the EAP-TLS and PEAP-TLS 802.1X certificate authentication modes for secure authentication on campus networks. Certificates from the user's personal certificate store in Microsoft Internet Explorer are available for selection. In Windows Live Logon, certificates from the local machine store are used.

Available certificates are presented through an optional additional tab on the **Login Information** dialog and the administrator can control how the user (or host) should be identified. In addition, the administrator may elect to trust only a subset of trusted root Certificate Authorities for network authentication.

A new CBook formatting document will be published with iPassConnect 3.50 to describe the configuration process for adding TLS certificate authentication to a client profile.



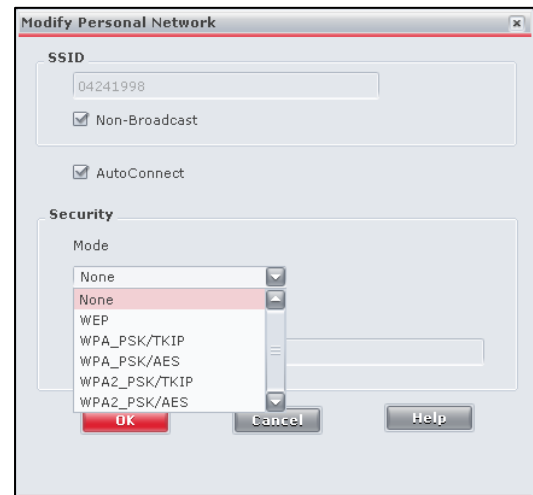
What wireless security modes are available?

iPassConnect 3.50 introduces WPA2 support for both personal (pre-shared key) and enterprise (802.1X) use. Both AES and TKIP encryption modes are supported.

All types of customer WPA2 wireless network can be specified in a CBook entry. In addition, the new pre-shared key modes WPA2_PSK/TKIP and WPA2_PSK/AES are available to users when adding a Personal Wi-Fi network.

Will iPassConnect automatically use a certificate if it is the only certificate in the cert store?

Yes. The client will still prompt for static credentials as needed. This is to cover the requirement for AutoConnect (also known as 1-click) VPN integration.



Other New Features

What is the Standby/Hibernate Feature?

iPassConnect 3.50 detects when its host is about to enter a suspended mode and takes appropriate action. When a connection is in progress, iPassConnect 3.50 will attempt a graceful VPN disconnect before terminating the connection and resetting the user interface. iOQ logs are generated to indicate that disconnection occurred due to the system entering a suspended state.

When resuming from a suspended state, iPassConnect will re-start network detection including scanning for AutoConnect networks.

Are the Wi-Fi drivers different in this release?

Yes. The Wi-Fi drivers built-in to iPassConnect 3.50 represent a significant step forward from previous releases. iPassConnect 3.50 has been designed not to interrupt existing associations made by other connection managers when starting up. This feature includes an enhancement to suspend active detection of non-broadcast networks if an existing association is detected.

How does iPassConnect 3.50 interact with the Wireless Zero Configuration Service?

In response to customer feedback, the wireless interface in iPassConnect 3.50 has been designed to allow users to maintain existing connections made through the Windows XP Wireless Zero Configuration Service (WZC) right up until the point when an iPassConnect connection attempt begins. This will allow users to browse iPassConnect while connected via other means and should also allow users to choose to connect over an existing wireless connection using the Home Broadband option if they choose (although the preferred option would be to use the iPassConnect Personal Wi-Fi feature instead).

When a connection attempt begins, (either manually or via AutoConnect), iPassConnect will disable the WZC service for the selected interface only. The Windows Wireless Networks tab will not be displayed for that network interface for the duration of the session although the WZC service will still show as running in the services list. The WZC service will not be restored to the selected interface until iPassConnect exits.

iPassConnect does not depend on the WZC service and customers may choose to disable it if desired.

What is the IE Proxy Manager option?

Microsoft Internet Explorer 6 stores one set of proxy settings for LAN connections (Ethernet and Wi-Fi) with separate configurations for other types of connection. Management of the appropriate proxy settings for each type of connection can be an issue for a remote access administrator. iPass created the IE proxy manager to handle this task automatically. Typically, this will involve applying the IE LAN settings to all connections made through iPassConnect although other configurations are also possible.

What else is new in the User Interface?



iPassConnect 3.50 contains several new branding items, including a new desktop icon and a new splash screen.

iPassConnect 3.50 also includes a link to the new iPass user portal: <http://connect.ipass.com>. This link is found under **Help > iPass on the Web > iPass Home**.



Updates and Provisioning

How has the update process changed in iPassConnect 3.50?

iPassConnect 3.50 introduces a new update mechanism called Background Updates. This runs as a separate service distinct from the iPassConnect client and periodically looks for Phonebook updates or SQM data to upload using any connection available at that time, even those not made using iPassConnect. In particular, the feature enables automatic updates over the LAN. Updates are performed in the background using trickle download technology with bandwidth throttling and support for interrupted downloads. One key benefit of the periodic update module is that it automatically discovers where proxy settings are needed.

Are all IE proxy features supported?

iPass has designed iPassConnect 3.50 to work with the full range of proxy configurations that might be specified through the IE interface. At this time we believe all valid IE proxy configurations are supported.

What happens when iPassConnect encounters a proxy requiring authentication?

iPassConnect 3.50 will display the following dialog to request the user enters their credentials (There is no way to determine ahead of time if these credentials are the same as the iPassConnect or Windows credentials). The user can provide their credentials for one time use or they can choose to save their credentials to avoid further prompting. They may also defer the update attempt by clicking **Ask me Later**.



Are all updates performed through Background Update?

Background Update is a modular service that can be extended in the future as needed. For the initial release, modules are provided to manage Phonebook update, SQM uploads and the self-update of the Periodic Update module itself. A new Periodic Software Update module (to replace ipccheck.exe) is in development and is targeted for delivery to 3.50 clients later in 2006. The Dialer ID update process (used for SQM, USID and iSEEL) is unchanged from earlier releases and still requires an iPassConnect connection.

Will Background Updates work with a 3rd party connection manager or supplicant such as Funk Odyssey, Intel Proset or ThinkVantage Access Connections?

Yes, the Background Update feature will opportunistically make use of any connection available; it does not need iPassConnect to be connected or even to be running in order to function.

Has the CBook format changed?

The format for dial access points has not changed but the CBook formatting document describes two new fields for AutoConnect on Wi-Fi services. In addition, there are new security modes for WPA2

and new Access procedure modes for EAP-TLS and PEAP-TLS. As with all previous releases, all CBook submissions made after the release of the new iPassConnect client must conform to the new format, even if they are intended for an earlier client.

The Cbook format is outlined in the tech note: *Creating a Customer Access Point List*, available on the iPass Portal.

What is the process to upgrade to iPassConnect 3.50?

iPassConnect 2.20 and later can be upgraded directly to 3.50 using the standard iPassConnect software upgrade process (ipccheck). Customers on releases pre-2.20 should contact their iPass technical representative to discuss alternative deployment strategies.

What applications and traffic types do I need to configure in my firewall in order for iPassConnect to be able to connect and update successfully?

For *updates*, iPassConnect tries establish outbound network sessions to iPass servers using HTTP on port 80 and HTTPS on port 443.

For broadband *connections* (other than 802.1X), HTTP and HTTPS are also used but some providers use redirectors to non-standard ports. iPass therefore recommends outbound access is permitted on all TCP ports for the following iPassConnect service components: iPassConnectEngine.exe, BrowserLogin.exe, iPassPeriodicUpdateApp.exe and iPCCheck.exe. iPass may add other network aware components in the future.

Can personal Wi-Fi be transferred when upgrading to 3.50?

Yes, users on iPassConnect 3.35 and above will have these settings carried forward to 3.50 if they use the iPassConnect upgrade mechanism. The AutoConnect setting will default to off.

How do I start using these new capabilities?

iPass always recommends evaluating new clients and features with a test profile before deploying to all users. If you already have a test profile available then you can submit a standard support ticket to request it be upgraded to 3.50. If you do not have a test profile then you may request one from the iPass Portal or from your iPass Account Manager.

Other Documentation

What other documentation is available on iPassConnect 3.50?

- Release notes
- Technical Guide
- End User Guide
- Upgrading to iPassConnect 3.50
- Creating a Customer Access Point (CBook)

