

# iPassConnect 3.65 Release Notes

Version 1.0, November 2008

## Version History

Version	Date	Notes
1.0	October 2008	General release availability document

## Introduction

This document contains the latest information on iPassConnect 3.65, including:

- New Features
- Technical Requirements
- Resolved issues
- Known issues

## New Features

### PEAP-GTC Support

iPassConnect 3.65 now supports PEAP-GTC protocol thereby ensuring secured private enterprise network connectivity. In the client, this is being established with the support of One Time Password (OTP) tokens.

All these parameters are supported in:

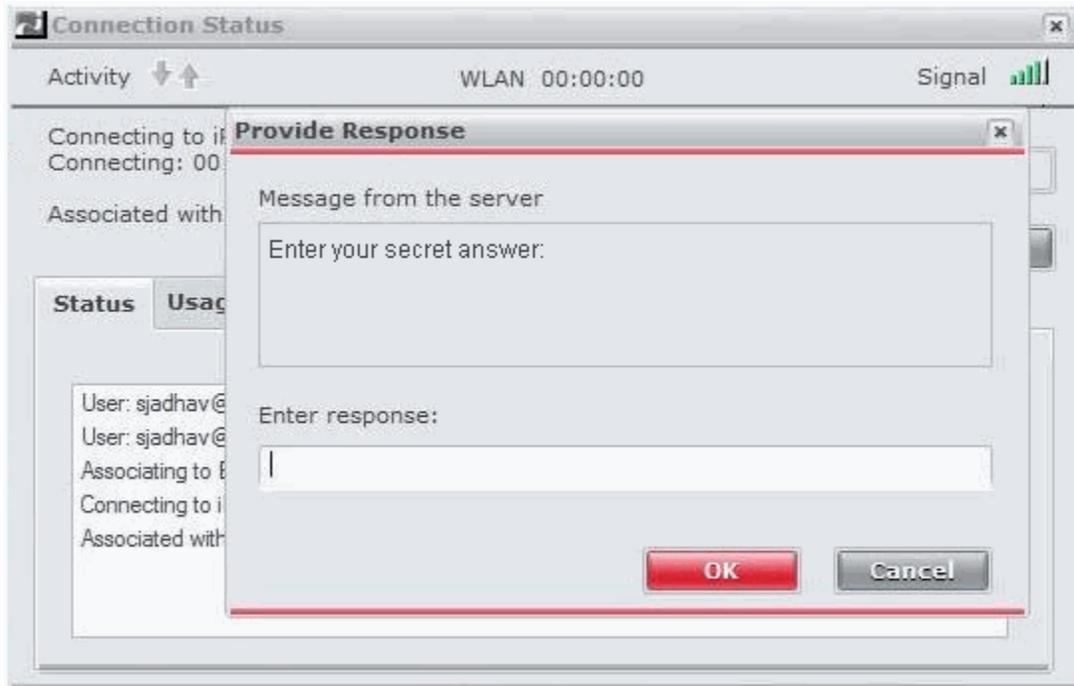
- Windows XP (Professional) Service Pack 2 and Service Pack 3.
- Windows Vista (All versions) Service Pack 1

**Note:** *RSA Next Token is not supported in Vista platform only.*

*Testing involved validation on both Standard and Administrative user account privileges. The authentication parameters have not been validated for Windows Vista Home edition.*

While connecting to a PEAP-GTC enabled hotspot, the server challenges the user with a response window. The user interface of iPassConnect client has been enhanced with this **Provide Response** dialog.





Here, the challenge message is sent by the server and user is required to enter the response. Based on the response, the user is re-authenticated for valid credentials.

**Note:** Please contact **iPass Technical consultant** for any clarifications with respect to the server message settings.

## EAP-TLS

EAP-TLS protocol provides secure certificate-based authentication for connectivity to private enterprise networks. This is now supported on both Microsoft Windows XP and Vista Operating Systems.

**Note:** Previous releases of iPassConnect supported EAP-TLS on Windows XP platform.

### Summary of 802.1X protocols supported in iPassConnect

The following table contains list of 802.1X protocols supported by iPassConnect 3.65:

8021X Protocol	Mode			
	Live-Logon		Win-Logon	
	Windows XP	Windows Vista	Windows XP	Windows Vista
8021X_MD5	Yes	No	Yes	No
8021X_TLS	Yes	No	Yes	Yes
8021X_LEAP	Yes	No	Yes	No
8021X_PEAP_MSCHAPV2	Yes	No	Yes	Yes
8021X_PEAP_TLS	Yes	No	Yes	No
8021X_PEAP_GTC	Yes	No	Yes	Yes
8021X_TTLS_MD5	Yes	No	Yes	No
8021X_TTLS_PAP	Yes	No	Yes	No
8021X_TTLS_GTC	Yes	No	Yes	No
8021X_TTLS_CHAP	Yes	No	Yes	No
8021X_TTLS_MSCHAP	Yes	No	Yes	No
8021X_TTLS_MSCHAPV2	Yes	No	Yes	No
8021X_FAST_MSCHAPV2	Yes	No	Yes	No
8021X_FAST_TLS	Yes	No	Yes	No
8021X_FAST_GTC	No	No	No	No

### Token Authentication

In order to ensure that the enterprise network access is secure, this release includes the feature of Token Authentication. Enterprise user's credentials would be authenticated with the use of tokens, thereby enhancing the overall security of the corporate network login process.

#### Token Integration<sup>1</sup>:

Corporate Networks supporting One Time Password (OTP) authentication, will now be able to use the Token Integration feature provided by iPassConnect 3.65.

iPassConnect 3.65 allows for this authentication to be performed, using hard tokens (includes RSA token).

The user interface of iPassConnect 3.65 client is enhanced to provide this desired functionality.

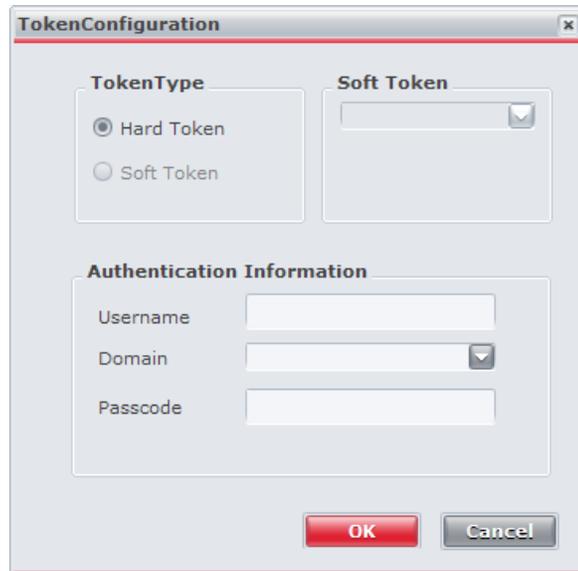
---

<sup>1</sup> Enabling Token Integrations requires iPass Professional Services assistance. Please contact your Account Manager for more information.

## Enable Hard Token and Specify Authentication Parameters

Perform the following steps to select Hard Token as the Token type.

1. On the **Settings** menu, select **Token >Token Configuration**. The **Token Configuration** dialog is displayed.

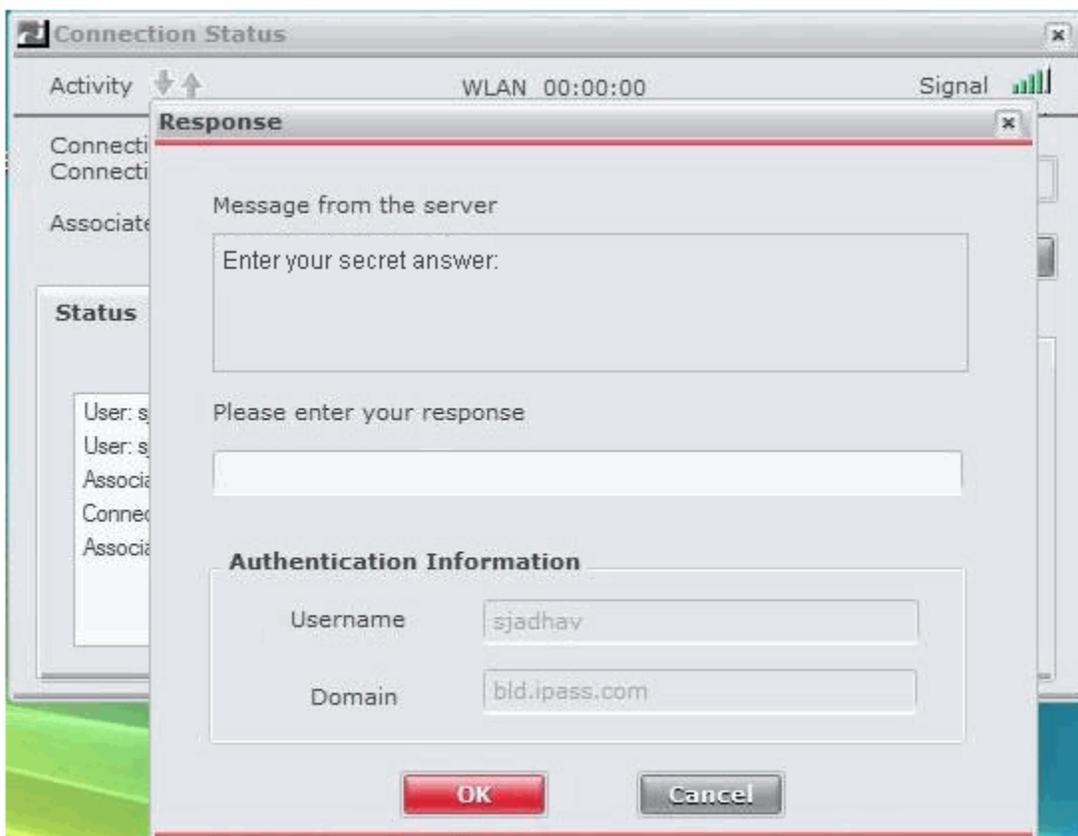


2. You can then select **Hard Token** as the token type by clicking the radio button.
3. In the **Authentication Information** section, specify the Username, choose the Domain and enter your password in the Passcode field.
4. Then click the **OK** button.

**Note:** The **Software Token** feature will be available in a forthcoming release of iPassConnect.

If the user tries connecting to a PEAP-GTC enabled hotspot with hard token enabled, then the server challenges the user for a response. Based on the response specified, the user is re-authenticated by the server.

iPassConnect client user interface has been enhanced by introducing the **Response** dialog



The Username and Domain is displayed as non-editable fields on this window.

### ***New Splash Screen***

iPassConnect 3.65 introduces a new "Unified Mobility" corporate message on the splash screen.



## Technical Requirements

### Minimum Hardware Requirements

- Pentium III processor or equivalent
- 512MB RAM for Windows2000 and XP, and 1GB RAM for Windows Vista
- 500MB free disk space (the typical installer file size is currently around 29MB; a typical installation will occupy around 245MB)
- 16-bit color mode display

### Connectivity Device Requirements

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

- Wi-Fi - an NDIS v5.1-compliant 802.11b/g device and appropriate software drivers.
- Mobile Data - a supported Mobile Data device plus appropriate driver software. A complete list of supported Mobile Data cards can be found in the *Mobile Data Configuration Guide*, available from the iPass Portal.
- Ethernet adapter
- 56K v90/v92 modem
- GSM modem
- ISDN terminal adapter
- PHS 2.1 device

### Operating Systems Supported

iPassConnect 3.65 is supported on the following platforms:

- Windows XP (Professional) Service Pack 2 and Service Pack 3.
- Windows Vista (All Editions) Service Pack1.  

Please **note** that the 802.1X authentication parameters have been validated for Windows Vista Ultimate, Enterprise and Business editions..
- Win2000 Service Pack 4
- iPassConnect is supported only on 32-bit operating systems. iPassConnect is currently not certified for use on 64 bit machines.
- Microsoft Internet Explorer 6 or 7 must be installed.
- iPass strongly recommends installation of all Microsoft-recommended updates for your Operating System.



## Languages

iPassConnect 3.65 supports the following languages:

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

Please **note** that iPassConnect 3.65 has been validated for English, German and French languages.

## Location of Log Files:

Note the location of the iPassConnect log files; this conforms better to Microsoft guidelines and avoids problems associated with management of log files within the %PROGRAMFILES% folder structure:

- Windows XP and Windows 2000
  - C:\Documents and Settings\All Users\Application Data\iPass\log
- Windows Vista:
  - C:\ProgramData\iPass\log

In both cases, the log files are located in "hidden" folders and so, depending on the configuration of Windows Explorer, the user may not see them while browsing the file system.

To view these folders, perform the following steps:

1. Open **Windows Explorer->Tools->Folder Options->View** (for windows Vista this step will be **Windows Explorer->Organize -> Folder and Search Options->View**)
2. Select **Show hidden files and folders** option.

## Limitation

- The phonebook is not getting updated when the system date is modified to a future value. It happens due to the periodic update process which runs in the background, irrespective of whether the user exits the client or launches it. Note, the user is informed about this process by "Phonebook Update is already running" message.

## Resolved Issues

The following issues have been resolved in this release. The numbers in parentheses indicate relevant bug numbers where applicable.

## Installation

- iPassConnect now informs users without administrative privileges that they cannot perform the product installation with relevant messages.
  - In Windows XPP platform, if the user is logged in the normal mode, then the following



message is displayed

*"Setup cannot continue because you do not have local administrative privileges".*

- Similarly, in Windows Vista platform, if the user with incorrect administrator credentials tries installing iPassConnect then any one of the following messages are displayed.

*"Unable to logon Failure: unknown username or password".*

*"Logon Failure: unknown username or password".*

- Un-installation of iPassConnect now deletes all the registry entries.
- Previously, it was observed that un-installation of iPassConnect, did not delete `iPassConnectEngine` entry from Microsoft Windows Services. With this fix, the required entry is being deleted as expected.
- While installing the client in standard mode, on Windows Vista, even with the right administrative credentials provided, application was displaying the error *"registration of Periodic Update failed"*. In this release, this issue has been resolved.

## Connectivity

- If the user tried connecting to the same Wi-Fi network repetitively, and then cancelled, the application previously remained in an unresponsive state. This fix now allows the application to connect successfully to the same Wi-Fi network repetitively.
- On Windows Vista, users can now initiate a new Wi-Fi connection even if a prior Wi-Fi connection made through the OS is still active.
- Client does not display engine module error on trying to re-connect to a modem connection, after decreasing the system time (time zone related change).
- In the phonebook control, Sniffed Ethernet services no longer display as "identifying" indefinitely. The required status messages, with respect to the connection, are now being displayed as expected.
- iPassConnect now correctly detects and terminates the Internet connection, in response to the user unplugging the Ethernet cable.
- Post-connect actions are no longer displayed twice, for user defined connect actions, while connecting to Personal Wi-Fi or WPA access points.
- Memory leakage issues related to `iPassConnectEngine.exe` and `iPassConnectGUI.exe` files which were observed in previous releases have been fixed in this version of iPassConnect.
- The iPass client has been configured to allow SSIDs of a maximum of 32 characters.

## Third Party Applications

- iPassConnect now successfully connects and logs on to the system when the **Sygate Personal Firewall** (v5.5) or **McAfee Antivirus** (v8.0i) services are stopped in Live Logon mode.



## Updates

- iPassConnect can now read the Proxy Auto Config files, defined locally in the system with Internet Explorer 7. The issue is resolved on installing the KB933566 security update for Internet Explorer 7 from Microsoft support site.

For more information please visit any one of these URL's:

<http://support.microsoft.com/kb/933566> or  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=c2191703-8cbd-4959-9f84-e13f21173926&displaylang=en>

- While performing software upgrade the client was not displaying appropriate error message when
  - the user clicked on iPassConnect desktop icon or
  - launched iPassConnect (98079)

With this fix, the following warning message - *Please do not re-launch iPassConnect while update is in progress* is displayed



- The iPCCheck software update utility now runs in the user context; this enables the utility to read the IE proxy settings required to upgrade the iPass client software.
- Erroneous warning messages are no longer displayed when the user does a Phonebook update on iPassConnect.

## Alternate Credentials

- iPassConnect configured with Alternate Credentials works as expected, when the user tries to connect to the Internet by double-clicking on one of the available SSID<sup>2</sup>s.

---

<sup>2</sup> SSID: Service Set Identifier

- Enabling Alternate Credentials Policy does not prevent the iPassConnect client from using USER-DEFINED actions.
- iPassConnect client configured with Alternate Credentials uses different authentication parameters for authenticating inner and outer tunnels.

Kindly **note** that the Alternate Credentials feature set has **Limited Availability**. Please contact your **iPass Technical Consultant** for any further information regarding the availability and applicability of this feature.

## User interface

- The following button labels have been abbreviated in Portuguese (Brazilian) to accommodate them within the button boundary limits:
  - Palavra-chave to Pal-chave
  - Propriedades de Discagem to Prop. de Disc.
  - Adicionar Marcacao to Adic. Marc.
- The dial string is now disabled, if the user selects **Smart Redial** checkbox in **Dial-up Connection settings** dialog.
- Changes to the Default Country option in the **Login Information** dialog are automatically updated in the iPassConnect main dialog. The default country name is now visible in the main dialog.
- The time counter option for PEAP-GTC enabled hotspots of iPassConnect is working as expected.

## Localization

- The **Home Broadband** option is displayed properly on the iPassConnect main dialog for all the countries. This option was not working as expected, for the Korean version of Windows XP Service Pack2 and Service Pack3.

## Known Issues

The following are the known issues in this release. The numbers in parentheses indicate relevant bug numbers where applicable.

### Connectivity

- In **Provide Response** dialog, currently it is observed that the client succeeds to connect even when the same One Time Password (OTP) token is entered twice. This occurs if the password is entered after 30 seconds of the dialog launch.
- In **Provide Response** dialog, if the user enters invalid password multiple times, iPassConnect fails to connect to the internet. However, the **Connection status** dialog pops up and the user is not able to close this dialog by clicking on “**Close [X]**” button.
- iPassConnect does not connect to an EAP-TLS enabled POP on Microsoft Vista, with



machine certificates.

- iPassConnect does not connect to an 802.1X Ethernet POP using EAP-TLS on Vista.
- In Live Logon mode iPassConnect currently fails to connect to PEAP-TLS enabled hotspot, since it is not using the appropriate certificate credentials.
- iPassConnect is displaying the message “*Connection established*” in the **Connection status** dialog multiple times for **PEAP-GTC** enabled hotspots. This happens, when the user connects to the internet and leaves the system idle for 30-40 minutes.
- For **PEAP-GTC** enabled hotspots in Windows Vista **Connection Status** messages are not in the correct sequence. However, all the other messages related to the Connection status are being displayed as expected.
- On specifying incorrect password in the **Provide Response** window of a PEAP-GTC enabled hotspot, the client is currently not displaying an error message indicating that the connection attempt has failed. However, Windows immediately displays the message “*Windows cannot connect you to SSID*” for this failed connection.
- If the client tries to connect to a PEAP-GTC enabled hotspot, wherein there is no server certificate installed in the Trusted root store and `VerifyServerCert` setting in `config.ini` file is set to “`yes`”, “*Server Certification failed*” message is not being displayed.
- Altering the focus of the tab, in the Connection Status window from “Cancel” button to “Disconnect”, and then hitting the “Enter” key on the keyboard, is resulting in - “*An invalid argument was encountered*” error message.
- Custom actions are being fired incorrectly while connecting to a customer (C-book) Wi-Fi POP (Customer Trusted Wi-Fi), using Flex VPN, on Microsoft Vista.

## Application Updates

- The phonebook is not getting updated when the system date is modified to a future value. On trying to update manually, the message “*Phonebook update is already in progress*” is displayed but, the phonebook does not actually get updated.
- Software update is not happening if iPassConnect is configured with secure proxy settings.
- When iPassConnect client installed, does not have a connection to the phonebook update server (pb.ipass.com), and the user selects the option **Update iPassConnect – Software**, the message “*The Software is up to date*” is being displayed incorrectly.

## GUI

- The **Provide Response** Window does not timeout (as per the default setting) and return to the “Response” window dialog, while connecting to a PEAP-GTC enabled hotspot.

E N D O F D O C U M E N T

