

iPassConnect 3.66 Release Notes

Version 1.0, February 2009

Version History

Version	Date	Notes
1.0	January 2009	Custom release availability document

Introduction

This document contains the latest information about iPassConnect 3.66, including:

- [New Features](#)
- [Technical Requirements](#)
- [Limitations](#)
- [Resolved issues](#)
- [Known issues](#)
- [Appendix](#)

New Features

iPassConnect v3.66 includes the following new features and enhancements:

Localization Support

In iPassConnect user interface, the fields related to **Alternate Credentials** feature are now displayed in the language that the client is configured for, rather than that of the Operating System language.

Alternate Credentials is not a General Availability feature. Please contact iPass Professional Services team for more information about this feature.

PEAP-TLS Support on Windows Vista

iPassConnect 3.66 now supports Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS) protocol on Windows Vista (Win Logon mode).

This 802.1x protocol ensures secure private network connectivity using mutual certificate authentication. iPassConnect authenticates the server and client using digital certificates and then, allows the user to connect to the Internet.



Soft Token Support

To ensure secure enterprise network access, iPassConnect now includes Software Token Authentication. The enterprise users' of the client can be authenticated by using software tokens, the use of these tokens enhances the security provided to the corporate network logins.

The Software Token feature requires iPass Professional Service assistance. So, please contact your Account Manager for more information..

Summary of 802.1X protocols supported in iPassConnect

The following table contains the list of 802.1X protocols supported by iPassConnect 3.66:

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	Yes
8021X_PEAP_GTC	Yes	No	Yes	Yes
8021X_TTLS_MD5	Yes	No	Yes	No
8021X_TTLS_PAP	Yes	No	Yes	Yes
8021X_TTLS_GTC	Yes	No	Yes	Yes
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	To be Supported in the future releases of iPassConnect:			

Technical Requirements

Minimum Hardware Requirements

- Pentium III processor or equivalent
- 512MB RAM for Windows XP, and 1GB RAM for Windows Vista



- 500MB free disk space (the typical installer file size is 30 MB; a typical installation will occupy 250 MB)
- 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 (The *Modem on Hold* feature is not supported)
- GSM modem
- ISDN terminal adapter
- PHS 2.1 device

Operating Systems Supported

iPassConnect 3.66 is supported on the following platforms:

- Windows XP (Professional) Service Pack 2 and Service Pack 3.

*iPassConnect 3.66 and its future versions are **not supported on Windows 2000 platform.***

- 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.*

- 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 3.66 supports the following languages:

- English
- French
- Korean
- Chinese (Traditional)
- German
- Brazilian Portuguese



- Chinese (Simplified)
- Japanese
- Spanish

Please **note** that iPassConnect 3.66 has been validated for English, German Japanese 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
 - 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.

Software Limitation

- iPassConnect displays, "Could not start service- iPassPeriodicUpdateApp" error message, when the user tries to install the client, on a Windows XP system with **McAfee VirusScan Enterprise 8.5.0i** already installed on it.

McAfee Antivirus blocks the installation of iPassConnect. The reason for this is well explained in **McAfee VirusScan Enterprise Setup**, as shown below:

Workaround: Stop any AV or PFW service before installing iPassConnect.

Resolved Issues

The following issues have been resolved in this release.

Connectivity

Improved 802.1X CBook Error Messaging

iPassConnect now displays the error message "Connection request rejected. Please check your credentials or server certificate" in the **Connection Status** dialog for the failed connection attempts, in the following scenarios:

- If the `VerifyServerCert` parameter is configured as `Yes` and there is no server certificate installation in the trusted root location.



- When the domain information in the server certificate, does not match with the value of `Issued_to` field in `certificates.ini` file, then the client no longer connects to the network and displays the error message.
- While connecting to Internet, if the user provides invalid password in the **Provide Response** window.
- When an invalid Server Hostname is specified in the `Issued_to` field of `certificates.ini` file.
iPassConnect no longer connects to an *On-Campus* TLS or Tunneled EAP network with invalid Server hostname.
- If there is a mismatch between the user's Server Certificates and the Root Certification Authority present in `certificates.ini` file.
- When the user specifies incorrect values for `Issued_by_1` and `Issue_to_1` parameters in `Cetificates.ini` file.
- If the user provides invalid login information, while connecting to an 802.1X enabled network on Windows Vista.

All the configuration parameters are enabled or disabled while creating an iPassConnect profile. Please contact your Account Manager for more information.

- iPassConnect now displays “*Please Select Token Type*” message, if the user does not select the Token type in **Token Configuration** dialog.
- The Soft Token passcode is now used only once for establishing a connection and the same passcode cannot be used for the second connection attempt. If the user tries to make a second connection attempt within a minute, “*Error message – Please wait till the next Token code is available.*” is displayed.

*The **Software Token** is not a General Availability feature, Please contact iPass Professional Services team for more information about this feature.*

- On Windows Vista, iPassConnect configured with PEAP or MSCHAPV2 authentication protocols, is now able to connect to the Internet with the correct *Outer* and *Inner* tunnel credentials. Previously, it was observed that the identities of the *Inner* and *Outer* tunnels were interchanged during connection process.
- In an *On Campus* network, iPassConnect stays connected to Internet and displays “*Connected to SSID*” message, when the user shifts between two PEAP_MSCHAPV2 enabled access points with the same SSID.

Software Updates

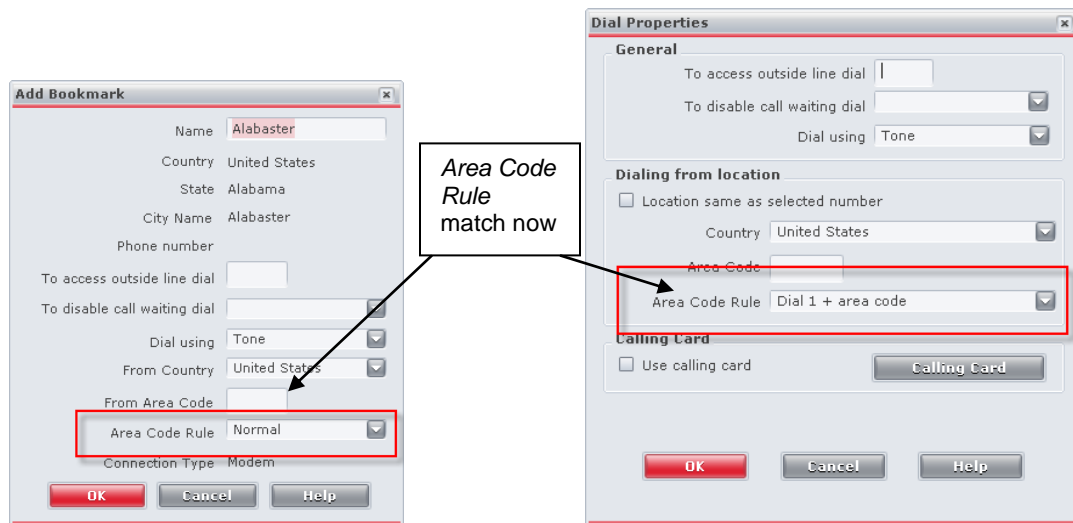
- The iPassConnect software update is now successful, even if the user configures the Internet Explorer (version 7.0) with secure proxy settings.

The software update is supported on Internet Explorer (6.0 and 7.0) on Windows XP SP3 and Internet Explorer (7.0) on Windows Vista.



User Interface

- While creating a bookmark for City level Dial-up access points, iPassConnect now displays the same *Area Code rule*, as selected by the user in **Dial Properties** dialog.



In the above screenshot, the Area Code Rule **Normal** corresponds to **Dial 1 + area code**.

- iPassConnect now displays the cursor in “Please enter your response” textbox in 802.1X Challenge **Response** dialog.



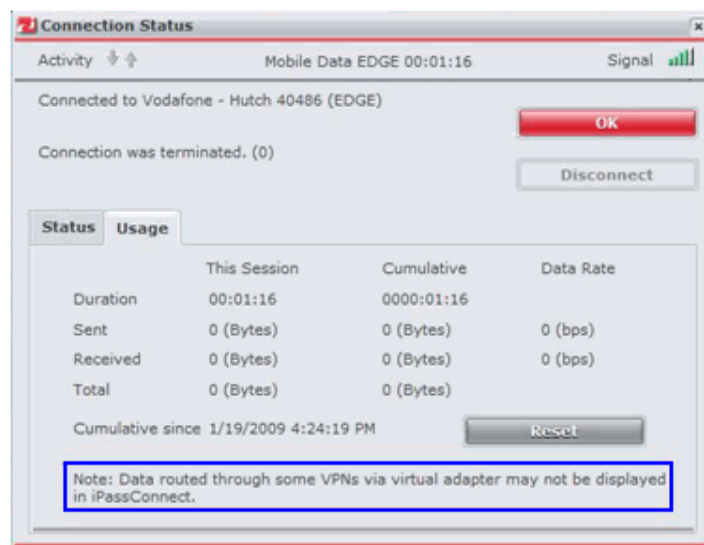
- In the earlier versions of the client, “iPassConnect is required to authenticate via a proxy server in order to check for updates. Please contact your IT support organization for advice if you do not know your account details.” message was truncated in the **Proxy Authentication Required for iPassConnect** dialog. Now, the label boundary limits have been modified to accommodate the entire message.

Live Logon

- On Windows Vista, iPassConnect now updates the *iPass CP Domain List*, if the Windows client changes the Domain.
Previously, it was observed that iPassConnect did not update “Connect with iPassConnect” domain pull-down list, when the windows station changed its domain.

Mobile Data

- iPassConnect now displays the correct **Network Type** for Huawei E270 Mobile Broadband device.
- In the **Connection Status** dialog, iPassConnect displays the **Usage Status** statistics for the connections that are established using the physical adapters. It will not display the usage statistics, for connections which use virtual adapters. A note has been included to inform the user.



The content of the Note in **Connection Status** dialog (highlighted in the image) is not localized. This will be resolved in the future release of iPassConnect.

802.1X Protocols

The following 802.1X issues, for Windows Vista have been resolved in iPassConnect 3.66:

- iPassConnect now displays only the supported connection types in the **Available Networks** list. Previously, the networks that use Wi-Fi Authentication Security Mode 0x04 (Open+802.1X) were also displayed.
- iPassConnect now displays the correct identity information of the *Inner* and *Outer* tunnels in the **Connection Status** dialog, for PEAP_MSCHAPV2 enabled access points.
- While connecting to an 802.1X_TTLS_PAP network, iPassConnect now displays the result of the initial connection along with the reason in case of a failed connection.
- iPassConnect now stays connected (using Fast Reconnect) to an On Campus network, even

if the user shifts between two access points of the same SSID.

Known Issues

The following are the known issues for this release.

Connectivity

- On Windows Vista, iPassConnect does not connect to an EAP-TLS enabled access point with machine certificates.
- iPassConnect prompts for the password, even if the user has already saved the password information. This only occurs when `TokenEnabled=yes` in `config.ini` file.
- iPassConnect is unable to connect to Internet, as the `GlobalUserOffline` value is set to 1 in the system registry. This value prevents the `WinInet` API from contacting the router for establishing the Internet connection.

For more details, see

[iPassConnect - GlobalUserOffline Registry Setting Causes 401 Errors.htm](#)

- It is observed that, when the "Limited Connectivity" balloon pops up after a successful connection to a GIS enabled hotspot, the user interface elements of iPassConnect tend to alter. For instance, the **OK** button is disabled and the **Disconnect** label is altered.

802.1X Protocols

- iPassConnect does not place the cursor in the **Provide Response** text field, while connecting to a PEAP_GTC enabled hotspot.
- EAP authentication methods of iPassConnect are not available in Windows Vista Live Logon mode. According to Microsoft, the WLAN API's do not function appropriately in Windows Vista Live Logon mode.

Alternate Credentials

- The `nad.ini` file has a file size limitation. The sum of all the *Section Name* entries within the `nad.ini` file must not exceed 2000 Bytes.

Dialer

- Users of iPassConnect will not be able to set the "SniffTimeInterval" value in `bb.ini` file.

Live Logon

- After installing iPassConnect from a Terminal Server, it is observed that the client system becomes unresponsive when the user reboots it.



Appendix

GlobalUserOffline Registry Setting Causes and Resolution

Problem Description

Error 401 "Failed to contact router" is generated when iPassConnect is unable to communicate with the broadband service provider's authentication gateway. The iPassConnect Engine is running in the System Context and obtains the Internet settings from Internet Explorer. Some of the settings that affect the processes of the API are stored in the .DEFAULT profile in the system registry.

With the "GlobalUserOffline" registry key set to "1" in the .DEFAULT profile, any HTTP or HTTPS requests sent by iPassConnect are not handled by the API because of this Offline Status.

Cause

This problem occurs when the GlobalUserOffline value is set to 1 under the following registry key:

```
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\GlobalUserOffline
```

When this registry flag is set to 1 it sets the Internet connection to offline mode for the System Context.

Note: This value is not modified by iPassConnect.

Symptoms of this issue are as follows:

- User encounters 401 errors when attempting to connect with iPC via Wi-Fi. All subsequent Wi-Fi connections via iPC fail.
- Association completes successfully and a correct IP address is assigned to the network interface.
- User is able to establish a functional Internet connection via iPC using a Dial-up connection.
- User can connect to Wi-Fi via means other than iPC (such as Windows Zero Configuration Utility - as an example).

If an iPC Debug Log is available, you can confirm this issue by the presence of the following entry in the iPass_GIS debug log:

```
CUTIL::WinInetErrorOut: error=Non-SSL HttpSendRequest() failed (ErrorCode:
2) for:http://sniff1.i-pass.com WinInet error code:2 - No Error message
found!
```

NB: A Windows System Error code 0x2 can be interpreted as ERROR_FILE_NOT_FOUND (The system cannot find the file specified.)



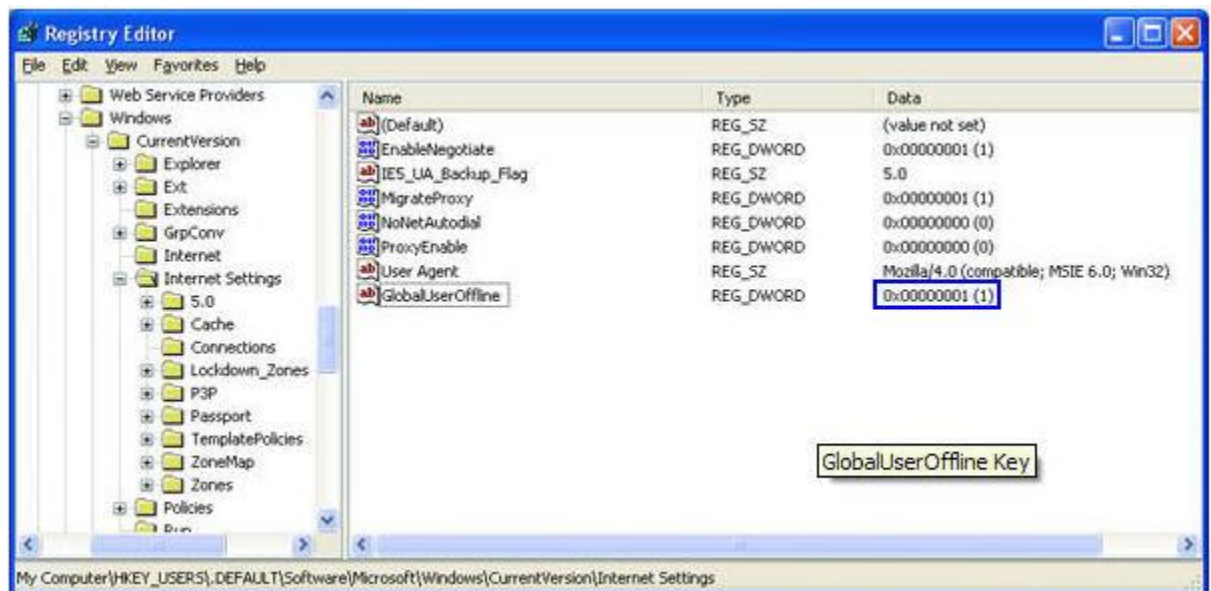
Resolution

Set the GlobalUserOffline registry key value to 0 for the .DEFAULT account:

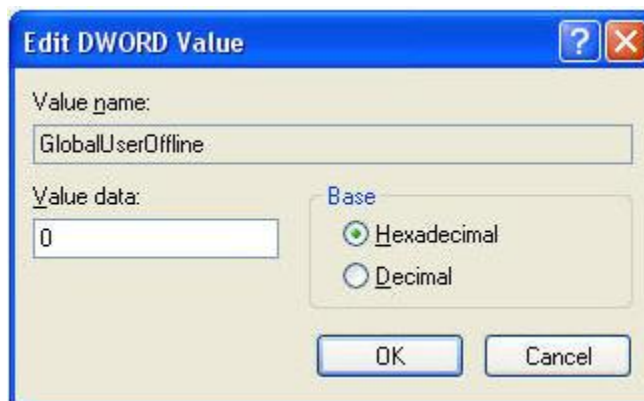
Note, if the following key is not presented in the registry or the key is already set to "0" (zero), then there is another problem causing the 401 error. Move forward with other 401 troubleshooting procedures.

To Set the GlobalUserOffline registry key

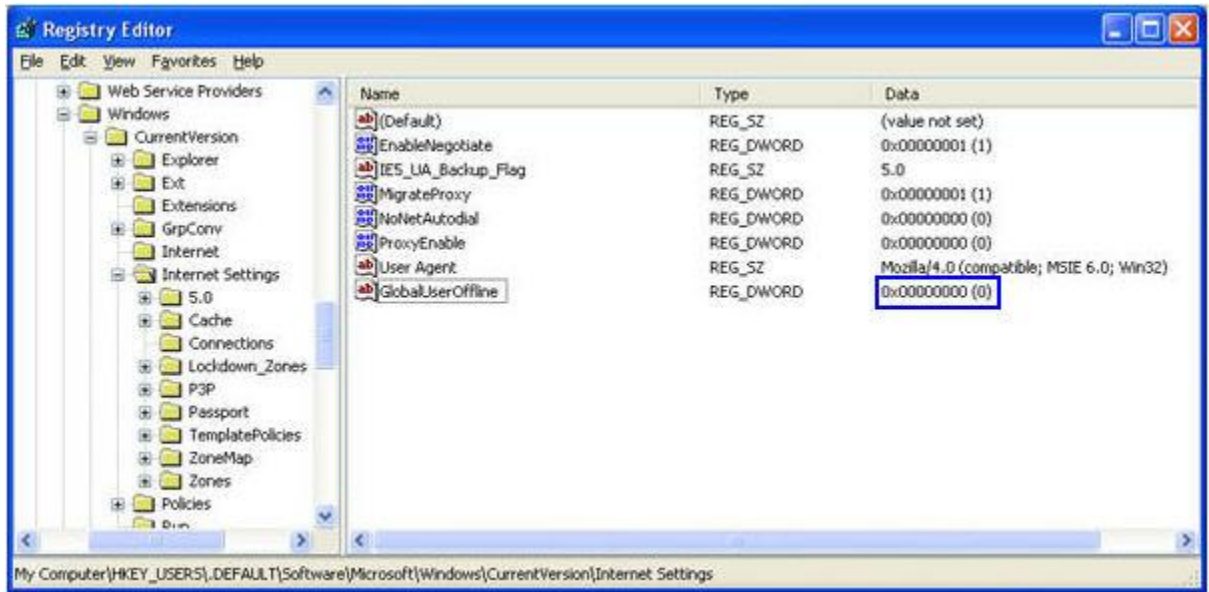
1. First, exit **iPassConnect** from the system tray
2. Navigate to the following registry key
3. HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\GlobalUserOffline
4. Observe the value for the **GlobalUserOffline** key as below. In this example, the registry key is presently set to "1".



5. Double click the registry key to change its value. Enter a 0 (zero/zed) as shown below. Click **OK**.



6. Review of the registry key after the change, it should now show the value of "0".



7. Re-launch **iPassConnect** to establish an Internet connection.
8. Done.

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