

iPass 3.8.0 Release Notes for iOS

VERSION 1.0, JANUARY 2016

New Features and Enhancements

- Network can be secured via VPN Backend servers:
 - targaryen.cloakvpn.io - gslb - This will select the nearest StrongSwan VPN Server based on Geo tag
 - baratheon.cloakvpn.io - This will select the US StrongSwan Server
 - arryn.cloakvpn.io - This will select the UK StrongSwan Server
 - tyrell.cloakvpn.io - apac - This will select the apac StrongSwan Server
- Demeter implemented and activated
 - Collects connection activity data

System Requirements

- iOS 7.0 or later
- iOS multitasking support. Examples: iPhone 3GS or later, iPod Touch third generation or later, or iPad second generation or later.
- Users need an iPass account in order for the service to function as well as be connected to the Internet (by Wi-Fi or Mobile Broadband) to activate iPass

Supported Languages

- English, Simplified Chinese, Traditional Chinese, French, German, Italian, Japanese, Korean, Russian, Spanish, and Thai

Resolved Issues

Issue ID	Description
OMI-261	Demeter records now contain the validating and required "ss" fields for scans
OMI-262	Demeter records now contain the validating and required "assoc","dv" fields for creating active records
OMI-263	Empty Scanlist no longer creates invalid Demeter records



Issue ID	Description
OMI-40	Dialer id supported through Activation Server

Known Limitations

Issue ID	Description
OMI-105	The hotspot preview is saying "No hotspot here" although the balloon help shows that hotspots are available.
OMI-99	In Hotspot Finder panel in main dashboard, client shows nearby network name instead of location information.
OMI-82	More Info page is blank under About settings for iOS WhiteLabel clients.
OMI-76	Branded clients crash on launch.
129208	If users upgrade from IPass 3.3.0 to 3.8.0, their credential information may not be saved in Account Settings. If this is the case, users should re-enter their credentials.
129187	Due to a software limitation, users on iOS 7.1.1 (or later) may not see the Signal Strength message displayed on the IPass main screen.
126745	A gateway page may appear when a user is connecting to IPass with an AT&T device. If this is the case, a user should cancel or exit this page and continue connecting to IPass.
123066	Due to a limitation in iOS, IPass does not support a Session Timeout Limit less than five minutes (even though this is configurable in the Portal).
122868	Wi-Fi Roaming Alerts require a user's device to be running on iOS 6.0 or higher.
120049	Due to a limitation on iOS 6.0 or later, if a user is signed in to a network that they add to the Manual Login list, signing off and signing back in right away through IPass will work as if the network were still an iPass network (and not a Manual Login network). The user can fix this by disconnecting from the network directly through iOS (Settings > Wi-Fi) before trying to reconnect.
117751	On branded clients with iOS versions 5.0 or earlier, the app navigation bar does not reflect the modified Navigation Bar Color of the branded client.
117543	The PIN field does not support entry using a non UTF-8 keyboard.
117522	When IPass is installed on an iPad, location services are enabled in the device Settings.
115964	If IPass is running in the background and the device is switched off, data usage that occurred while IPass was running in the background will not be counted correctly.
N/A	IPass will cache a DHCP-assigned IP address. However, when later attempts to connect are made, no attempt is made to determine if the IP address is valid. As a result, some connections may fail unless the DHCP address is manually refreshed.

Known Issues

Issue ID	Description
----------	-------------

Issue ID	Description
123579	Although Manual Login Settings functions properly by not allowing IPass to sign into specified networks, the annotation "Use iPass Here" may accompany a network whose SSID has been entered in Manual Login Settings (due to a limitation in iOS).

Copyright ©2016, iPass Inc. All rights reserved.

Trademarks

iPass, iPassConnect, ExpressConnect, iPassNet, RoamServer, NetServer, iPass Mobile Office, DeviceID, EPM, iSEEL, iPass Alliance, Open Mobile, 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 document is subject to change without notice. Every effort has been made to use fictional companies and locations in this document. Any actual company names or locations are strictly coincidental and do not constitute endorsement.