iPass 2.7.0 Release Notes for Windows

VERSION 1.0, JUNE 2016

New Features and Enhancements

iPass 2.7.0 for Windows added the following new features:

- Support for Brazilian Portuguese, UK English, and Mexican Spanish
- Changing company branding from Open Mobile to iPass
- Updating of Terms and Conditions with new iPass branding
- SmartConnect added device location information for network blacklisting

System Requirements

The latest version of iPass has the following system requirements:

Operating System

Any of the following:

- Windows 10 (Win10, WinX)
- Windows XP (SP3) (32-bit only)
- Windows Vista, Vista SP1 or Vista SP2 (32- or 64-bit)
- Windows 7 or Windows 7 SP1 (32- or 64-bit)
- Windows 8 or Windows 8.1 (32- or 64-bit)

Additional Software Components

- For Windows XP:
    - WLAN API and .NET Framework 3.5 SP1 or 4.0 must be installed.
    - 802.1x connections on Windows XP require the Windows hotfix available at http://support.microsoft.com/kb/958071.
    - Com+ Event System, Com+ System Application, and MSDTC services must be installed and running.
- For Windows Vista version earlier than SP1, .NET Framework 3.5 SP1 or 4.0 must be installed

Hardware Requirements

- 1 GHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB of system memory
- 1 GB of disk space
- 512 MB of physical memory
- Support for DirectX 9 graphics and 32 MB of graphics memory
- A recommended screen resolution of at least 1024x768.
- At least one connectivity device installed, depending on your intended connection type:
    - A Wi-Fi adapter for a wireless connection.
    - An iPass -supported Mobile Broadband device, plus appropriate driver software installed.
    - An Ethernet adapter for an Ethernet connection.
    - A 56K v90/92 modem for a Dial connection.
    - A DSL modem for a DSL connection.

Supported Languages

- Brazilian Portuguese, English (US and UK), French, German, Japanese, Korean, Mexican Spanish, Spanish, Simplified Chinese, Traditional Chinese, and Thai.

Resolved Issues

iPass 2.7.0 resolves the following issues:

Issue ID	Description
OMWIN-120	Customer reported multiple exceptions seen in logs.
OMWIN-230	Customer reported error message is shown on Network tab when network is already detected.
OMWIN-286	Customer reported SIM PIN is not saved when pin state is 3.
OMWIN-90	After SW update from 2.5.0 to 2.5.1, client failed to launch automatically.
OMWIN-96	Application name should be same for base msi and bundled msi.
OMWIN-117	Remove client logic to read cookie on every launch to reactivate silently.
OMWIN-229	Old iPass Logo is seen when Juniper VPN is launched.
OMWIN-281	In PLAP Mode, a hotspot login window can be opened with iPass mini-browser. In this window, the external browser can be launched via a button and within the external browser, some file dialogues can be opened for a command line.
OMWIN-283	iPass is now using the selected VPN gateway while connecting.

Known Limitations

This release of iPass includes these limitations:

Mobile Broadband Limitations

Many Mobile Broadband devices, their firmware, and drivers are not currently supported on Windows 8. It is strongly recommended that you thoroughly test any Mobile Broadband devices on Windows 8 prior to deployment.

Issue ID	Description
119787	When there is a Mobile Broadband device connected through ODF integration and another Mobile Broadband device plugged in, the first device is disconnected.
119347	On Windows 7 64-bit machines, Gobi 3000 devices are detected through WWAN instead of the regular full integration.
117414	After a Sierra Wireless AC320U device is plugged out, there should be at least a ten-second delay before it is plugged back in or it may not be detected.
117053	Due to a limitation with the device, Dell 5530 may not connect to a 3G network.
117039	Sierra 875 devices may show up twice in the **Devices** section (**Options > Mobile Broadband > Devices**) due to a device limitation.
116985	On a few devices, switching from regular iPass or ODF integration to WWAN integration may cause the SIM state to change to "Unknown." This does not occur when switching from ODF to regular integration or from WWAN to ODF or regular integration.
116877	When configuring an ODF, do not include the standalone character "-". For example, if the Port name is "Sierra Wireless MC8355 – Gobi 3000 (TM) HS-USB Modem 9013" then configure the Port name in the XML as "Gobi 3000 (TM) HS-USB Modem 9013" or "Sierra Wireless MC8355".
116867	For Gobi 3000 devices, when there is no SIM in the device, iPass will state the SIM status as unknown (instead of no SIM or SIM removed) due to a device limitation.
116272	For 320U devices, if the first connection attempt is canceled, the next connection attempt sometimes fails.
116271	For 320U devices, on 64-bit Windows 7 machines, the device may not be detected after the computer resumes from hibernation mode. If this happens, pull the device out and plug it back in.
116217	Due to a device limitation, Huawei E352 may fail to detect a 3G network because it is reporting it as 2G. You can fix this by manually scanning for the network.
115498 ,115500	For Gobi 3000 devices, occasionally the Wi-Fi radio will turn off after the computer returns from hibernate or sleep (and all of the Wi-Fi networks will disappear from the Available Networks list). If this happen, the Wi-Fi radio can be turned back on manually.
115431	For Gobi 3000 devices using a BSNL SIM, after the PIN is entered, the device may still show as locked, and the PIN will have to be entered in the SIM tab for this status to correct. Enable PIN may also be shown when the PIN is already enabled—this can be fixed by selecting Enable PIN and entering the correct PIN.
115035	For ZTE 633+ devices, iPass may prompt the user to enter the SIM PIN when Flight Mode is turned off due to the SIM powering down during Flight Mode.
114904	For Option Icon 422 devices, when the device is plugged out it may still be shown as plugged in due to a limitation with the devices driver.
114700	For some older Sierra devices, updating the driver or SDK to the latest may cause the device to not be detected properly by iPass. Uninstalling the latest driver and reinstalling the correct driver for these older devices will fix this problem.
114688	On some SIMs, the Sierra 320U may not be able to send SMS messages until you set the correct Service Center number.

114171	For 320U devices, when the user signs off and signs on to Windows the device may not be fully recognized by iPass and the network will not be detected. To fix this, pull the device out and plug it back in.
113468	USB 308 and USB 309 devices may fail to detect some networks (such as Tata DoCoMo) due to a limitation in the device
111280	For the Huawei E180 device, only 2G networks will be detected.
112503, 110580, 110486	For the Sierra 312U device: ● iPass does not save the band if it is set to "3G All." ● The Sierra 312U device firmware will only support 3G enabled SIMs. On a hot plugin of the Sierra 312U device, iPass may not capture the serial number, software version, and hardware version of the device.
110295	Due to a limitation in Windows 7, manual network selection may not work properly (and may be disabled).
109772	In some cases, turning off Flight Mode on a Mobile Broadband device may cause iPass to prompt for the SIM PIN.

Wi-Fi Limitations

Issue ID	Description
115446	In some cases while connecting to a GTC network, the user will be prompted to enter a second passcode even if the connection has already timed-out.
127755	If the network bridge is enabled and users have installed Junos Pulse VPN, they may have trouble connecting to a Wi-Fi network.
112700	When using token authentication, if the user response is delayed for server challenges. iPass may fail to authenticate to some PEAP-GTC 802.1x networks.

Login Assist Limitations

Issue ID	Description
115696	Save Password has to be selected for the account used by Login Assist or the password will not be passed through.
131291	iPass application name does not show up when installing iPass on OMC Windows and OM Touch client from the Send Activation page. Instead of the iPass app launching, the Launch Application prompt says "TWINUI" (for touch) and "EPCmd" (for Windows).
115673	If a security page displays before the login screen, the Login Assistant may not be able to automatically enter credentials.
112739	Login Assistant will not submit login credentials when Internet Explorer is in InPrivate mode.
N/A	The Login Assist feature is not yet supported on any version beyond Windows 7.

VPN Integration Limitations

Issue ID	Description
120396	Because Junos Pulse does not return a specific error code for authentication failure, iPass will not be able to re-prompt the user to enter credentials if incorrect credentials were entered.
120221	When the VPN is configured in the iPass Portal to not send the username and password (1.5 click), then VPN Gateway Selection will not work.
120145	Custom VPN will not send the username and password if those fields contain a '%' character.
119909	Due to a limitation in versions of Cisco AnyConnect later than 3.1.00495, the check box "Always trust this VPN server and import the certificate" may not appear, and if that checkbox is not selected,

Issue ID	Description
	connections to the VPN may fail. We expect this to be corrected in a future maintenance release of AnyConnect.
119749	If configured to send either just the Username or no authentication credentials (1.25 or 1.5 clicks), VPN Gateway Selection will not work for any VPN besides Juniper.
119012	Due to a limitation with Junos Pulse VPN, the user's credentials may not get sent every time and the user will be prompted to enter them (if the VPN is configured to authenticate using the account).
118440	Due to a limitation with Cisco IPsec VPN on Windows 8, iPass may not connect to it in rare cases.
116937 , 116766	Connection attempts made using 1-click integrated Cisco AnyConnect v3.0.5080 and v3.0.07 on Windows XP, and v3.0.07059 on SP3, will fail.
113761	Checkpoint VPN profile names are case-sensitive. The name of the profile must be entered exactly as it appears in the Checkpoint VPN.

Proxy Authentication Limitations

Issue ID	Description
111275	iPass and Internet Explorer will fail to connect to proxy networks if the proxy.pac file contains the following expression: if shExpMatch (url, "http://google.com") return "DIRECT";

Connect Before Logon (CBL) Limitations

Issue ID	Description
117374	If Connect Before Logon is configured with a very short timeout, the connection process may continue in the background after the timeout so that when the user reopens iPass from the pre-logon screen, they may be able to connect and proceed to their VPN and Windows Logon.
117176	A Cisco AnyConnect VPN may display as connected in pre-logon mode when it is not.
116669	On 64-bit machines, Connect Before Logon may not pass credentials through to the VPN and Windows Logon (if configured to do so) after connecting to the network. This can be solved by completely deleting all iPass files and doing a fresh install of iPass 2.2.0.
114999	In pre-logon mode, adding a connection method or campus network in **Options > Wi-Fi > Campus Networks** will not work. The user has to sign in to the computer before adding a connection method or campus network.

Multiple Networks at a Time (MNAAT) Limitations

Issue ID	Description
115137	On a few Mobile Broadband devices (such as Novatel MC 990D), attempting to connect to a Wi-Fi network while the user is connected to a Mobile Broadband network will not work as the device interferes with the connection.
114516	When a user connects to a Wi-Fi network after already connecting to an Ethernet network, the VPN will not auto-connect even if it is configured to do so when a Wi-Fi connection is established. The VPN can still be manually connected by clicking on the VPN switch.

General Limitations

Issue ID	Description
120146	Connecting to a browser login hotspot using Windows 8 sometimes causes Internet Explorer to launch.
OMWIN-223	Application launcher for activations does not have proper Windows name on supported browsers.

118687	On 32-bit operating systems, attempting to connect to a DSL connection may cause the OS to abruptly terminate.
118603	Although Event Actions enable a process to be specified as running in Hidden Mode, this is subject to the limitations of the process itself. Some Windows applications may not actually run in Hidden mode.
118500	In some cases, on Windows 8, iPass may abruptly terminate after the system tray icon is clicked.
117336	When Policy Enforcer is configured with McAfee Desktop Firewall 8.5, this application may cause the system to crash if the latest patch has not been downloaded and installed.
117058	To add Custom Profile Attachments, a 2.1.3 or later profile is required—you cannot upgrade an existing profile.
117036	If a device only has a Modem Port and no additional port that responds to AT commands, the SMS feature will not be supported for that particular device. <SMSSend> and <SMSReceive> tags will have to be set to false.
115541	When the screen resolution is 800x600, some of the user interface, including some buttons, may become inaccessible. It is recommended that the screen resolution be set to at least 1024x768.
113642	iPass may not detect BlackBerry devices running the version 6.1 set of drivers.
112869	Due to an issue with Windows 7, when uninstalling iPass, this message may be displayed and persist: `"Error Opening installation log file. Verify the specified log file location exists & is writable."` To resolve this issue, Microsoft recommends restarting the explorer.exe process. For more information, consult the Microsoft Knowledgebase article, http://support.microsoft.com/kb/2564571 .
112589	Windows UAC must be disabled in order for Login Assist to work, unless Internet Explorer is set to run in the administrator context.
110109	Attempts to connect to DeviceScape access points at Wayport venues failover to local GIS access points.
N/A	There are no Windows 8 specific ODF integration files. Use the Windows 7 files instead.

Known Issues

The following issues are known for this release of iPass:

Mobile Broadband Issues

Many Mobile Broadband devices, their firmware, and drivers are not currently supported on Windows 8. It is strongly recommended that you thoroughly test any Mobile Broadband devices on Windows 8 prior to deployment.

Issue ID	Description
110334	Flight mode is not available for the Sierra USB 306 device.

Wi-Fi Issues

Issue ID	Description
115150	When configuring an Account for a Profile in the iPass Portal, if **Token** is enabled and a **Soft Token** is selected, you have to select **Save Token** or connections to networks requiring token authentication may fail.
	After software upgrade to 2.7.0, desktop shortcut icon text and control panel installed programs listing the app name doesn't change to "iPass" from previous name "Open Mobile."
114825	When using token authentication, the first time a user connects to a FAST-TLS network the connection may fail due to the authentication process, but all subsequent attempts should succeed.

113120	Wi-Fi connectivity may fail on laptops with adapter Intel 5100 AGN, when the Avast Anti-Virus service is running.
113119	When using the NETGEAR WG111v3 Wireless-G USB Adapter, iPass will fail to connect on the first connection. To resolve this, connect using the Windows native Wi-Fi client. After this connection is made, iPass will be able to connect normally.
106801	iPass may not successfully complete some Wi-Fi connections if the latest Intel Wi-Fi drivers (13.2.1.5) are installed without a restart. To resolve this issue, try restarting the computer.

VPN Integration Issues

Issue ID	Description
117084	When Juniper is configured to automatically launch, iPass does not support "Next Passcode" mode. The workaround is to wait for the passcode to change and manually provide the next passcode in the VPN browser. The next passcode can be retrieved either from the RSA SecureID Application or by right clicking the System tray icon and generating the passcode.
116710	If a profile is configured to pass token information to the VPN, and the token is entered in the iPass Portal with Allow End User to Edit PIN not selected, the PIN information will not be saved and the user will not be able to enter it.
113817	After switching networks on a VPN connection, iPass does not always show the correct connection status, even if the connection is successfully switched. As a result, the option Disconnect VPN on Network Switch should be enabled for CheckPoint, NCP, and Cisco IPSEC VPNs.
113764	In some cases, when connected by the NCP VPN and the current network connection is switched; the user is prompted for credentials even if the credentials are saved. Due to this issue, when configuring the NCP VPN, the Disconnect on Network Switch option should be selected.
112541	In some cases, after a software upgrade from iPass 1.4.3 to 2.0, OesisCOM may fail to register, and the VPN button will not be shown in the iPass user interface.
111108	iPass will not correctly report the connection status of Checkpoint VPN or a Custom VPN if the user is on a corporate network.
108234	If Nortel VPN is configured for a connection profile, then iPass will not authenticate for RADIUS and for certificate-based profiles. Attempts to connect with a profile that is configured for an authorization type different from what was configured in the Portal will always fail.

Operating System-Specific Issues

Issue ID	Description
118564	On Windows 8, iPass is unable to connect to a TTLS/FAST MS-CHAPV2 network.
131288	Disabling SSLv3 on web browsers that use the MS IE default browser settings creates OM Browser Login error.
118296	On Windows 8, iPass will fail to authenticate when using a smart card configured for PEAP-TLS.
117927	On Windows 8, when iPass is connected to a Wi-Fi network, if Airplane Mode is turned on and off, iPass continues to show the previous connection as active even if there is no actual connection.
117806	BHOs do not work correctly on Windows 8. As a result, Login Assist will not function as intended on Windows 8.
117738	On Windows 8, iPass is unable to connect to WLAN defined 802.1x networks that require user interaction.
117736	On Windows 8, iPass is unable to convert a WLAN profile that is defined for TTLS-MSCHAPV2/PAP protocol.
110727	When installing iPass on Windows Vista with UAC enabled, OesisCom.dll will fail to register during the installation process. If this occurs, you can resolve this issue in either of these ways: ● Root the computer or restart the iPass services, so the DLL will register. ● Manually register the DLL after installation using this command: `regsvr32 /u "c:\Program Files\iPass \opswat\OesisCom.dll"`

Connect Before Logon (CBL) Issues

Issue ID	Description
118255	On Windows 8 64-bit, iPass configured with Connect Before Logon will fail to launch imobility.exe.
117027	Connect Before Logon may not work with Cisco AnyConnect versions 3.0.5080 and 3.0.07059.
115316	Any preferences or settings that the user enables in iPass **Options** during pre-logon will not be saved and carried over after the user logs on to Windows due to a limitation in what preferences can be accessed in pre-logon mode.
114800	If Connect Before Logon (CBL) is added to a user profile after migrating from earlier iPass version, user will have to reinstall the new version of iPass: Connect Before Logon will not work if a user performs only an iPass software update.

MNAAT Issues

Issue ID	Description
115407	If "Tear down Internet connection automatically when VPN is disconnected" option is selected and the user is connected by Ethernet without a VPN connection then attempts to connect to a Wi-Fi network with the VPN failing to connect, iPass may try to disconnect from the Ethernet connection.
115151	If Multiple Networks at a Time (MNAAT) is enabled for a profile and a VPN launch is configured for multiple media types, the user may sometimes have an unreliable VPN experience.
114718	When a user is connected by Ethernet, they will not be able to connect to a Wi-Fi network that requires a browser log in (because the hotspot will detect that the user is already connected to the Internet).
114387	Multiple Networks at a Time (MNAAT) is not supported on profiles with DSL enabled.

General Issues

Issue ID	Description
131291	Application launcher opened for activations on supported browsers should have proper name for Windows Desktop
131288	Web wizard and browser login-SSL3 SECURITY VULNERABILTIY
131245	Windows_2.7.0.15502: One click activation/Activation by Link is not working with IE 11 when protected mode is enabled
120510	In some cases, when the user sets Limits & Alerts, they may override Administrator-defined Limits & Alerts (created in the iPass Portal).
119548	After connecting using Manual Login, an incorrect SQM record is generated (it will record it as a GIS connection).
118384	On Windows 8, iPass will be unable to connect to a network where a proxy is configured using a .PAC file.
117674	If a profile is configured to auto-detect the language and iPass is installed on Windows 7 using the command line installation for U.S. English (msiexec.exe /qn /i <full path of install.msi> LANGID=1033), then iPass will not launch in English.
115968	If the account settings for Username are changed to **Use the Windows username**, this change will not take effect after a profile update.
115541	When the screen resolution is 800x600, some of the user interface, including some buttons, may become inaccessible. It is recommended that the screen resolution be set to at least 1024x768.
114853	If you enable Wi-Fi Timeout for a Time-Based Session Limit, the timeout may not apply to an iPass network connection that is a fallback from a failed OpenAccess connection.
112644	After a profile update that includes revised Endpoint Security settings, the user's system must be restarted in order for the new settings to take effect.

106851	Sometimes after returning from sleep/hibernate on an Ethernet connection, iPass may erroneously report a state of limited connectivity.