RELEASE NOTES
Windows HipLink 4.7 RC 19

Supported Platform

- Win 7, 2008 (R1 and R2) - 32/64 Bit, Win Server 2012 (R1 and R2)

System Requirements

Low-End/Training System:
- Intel® Core™ i5 or Core™ i7 processor
- 2 to 4GB RAM
- High-speed HDD
- Gigabit Ethernet Card
- High-speed Internet connection
- Windows Server 2008 operating system

Minimum Production System:
- Intel® Xeon® processor 3000 series
- 4GB RAM
- High-speed HDD
- Gigabit Ethernet connectivity
- High-speed Internet connectivity
- Windows Server 2008 operating system

Recommended Production System:
- Intel® Xeon® processor 6000 or later series
- 8GB RAM or more
- High-speed Enterprise grade HDD
- Gigabit Ethernet connectivity
- High-speed Internet connectivity
- Windows Server 2008/2012 operating system

High-Performance Production System:
- Intel® Xeon® processor of 8800 series
- 32GB RAM or more (extensible)
- Two High-speed Enterprise grade HDD.
- Implement RAID Level-1 for mirroring.
- Gigabit Ethernet connectivity

System Requirements for HipLink Mobile

Minimum Production System:
- Intel® Core™ i5 or Core™ i7 quad-core processor
- 4GB RAM
- High-speed HDD
- Gigabit Ethernet connectivity
- High-speed Internet connection
- Windows Server 2008 operating system

Recommended Production System:
- Intel® Core™ i7 8-cores processor
- 8GB RAM or more
- High-speed Enterprise grade HDD
- Gigabit Ethernet connectivity
- High-speed Internet connectivity
- Windows Server 2008/2012 operating system

High-Performance Production System:
- Intel® Xeon® processor of 8800 series
- 32GB RAM or more (extensible)
- Two High-speed Enterprise grade HDD.
- Gigabit Ethernet connectivity

Deployment

Installation Steps

For upgrading from previous version:

- The build can be upgraded on Windows HipLink 4.5.197 OR Windows HipLink 4.6.181 with SP 5.6 OR Windows HipLink 4.7.247 with Patch 8.4 OR Windows HipLink 4.7.439 OR Windows HipLink 4.7.452 OR Windows HipLink 4.7.524 OR Windows HipLink 4.7.533 OR Windows HipLink 4.7.728 OR Windows HipLink 4.7.913 OR Windows HipLink 4.7.965 OR Windows HipLink 4.7.1009 OR Windows HipLink 4.7.1019 or Windows HipLink 4.7.1060 or Windows HipLink 4.7.1106 OR Windows HipLink 4.7.1170 OR Windows HipLink 4.7.1125 OR Windows HipLink 4.7.1169 or Windows HipLink 4.7.1299.
- Log into HipLink with admin credentials.
- Stop all running services.
- Terminate all user sessions.
- Using Task Manager, make sure no hiplink.csx or hiplink.gui is running. If so, kill them using Task Manager.
- Logout of HipLink.
- Stop the web server service (either Apache or IIS)
- Make a copy of the HipLink directory and save it in a safe location as a backup. This is typically found at C:\Program Files\HipLink Software\HipLink or C:\Program Files(x86)\HipLink Software\HipLink
- Open the latest HipLink build directory (WIN_HipLink_4_7_1368). Run the setup.exe file and select the upgrade option. Location of installation directory must be the same as previous.
- Login to the server and start the services. Make sure everything is working fine.

After Upgrade:

- Finally, advise your Users to change their login password.
- Edit and Save GIS Settings (For GIS only).

For a fresh install:

- Execute installer for WIN_HipLink_4_7_1368.

For Servers on HTTPS

- Follow the same steps for upgrade
- After upgrade, replace your server certificate with a new one.
- Finally, advise your Users to change their login password.

Removal Steps

If needed, the installed build can be uninstalled as follows:

- Stop all running services.
- Terminate all user sessions.
- Using the Task Manager, make sure no hiplink.csx or hiplink.gui process is running. If so, kill the process.
- Logout of HipLink.
- Make a copy of the Hiplink directory and save it in a safe location as a backup. This is typically found at C:\Program Files\HipLink Software\HipLink or C:\Program Files(x86)\HipLink Software\HipLink
- Execute installer for WIN_HipLink_4_7_1368 and select Uninstall from the options. OR
- Go to Windows -> Control Panel -> Add/ Remove Programs.
- Select HipLink 4.7 from the list of installed programs, and uninstall.

New Features

- Add secure flag in carrier profiles
    - In carrier profile (add/edit panel), we need a new multi-valued configuration parameter below the "Backup carrier 2" option.
    - It will be shown as a drop down parameter. We will not be showing the parameter "Enable Web-Based Confidential Dispatch".
    - The name of the new parameter will be "confidential message dispatch type".
    - The possible values will be:
        - Allowed (carrier is secure)
        - Web based dispatch (only if web based confidential dispatch is enabled in global settings)
        - Blocked
- Updated Cascaded carriers work flow for Confidential Messaging.
- Server side work related to Consolidated Inbox in mobile clients.
- Detect and remove XMPP ghost connections in HNP manager
- Updated OpenSSL version to 1.0.1m
- Updated Apache to version 2.4.12 (Note: This build will no longer run on Windows Server 2003 and Windows XP)
- Build is preconfigured to be used on HTTPs on apache. For IIS certificated needs to be added in IIS manager.

- Removed Complete on Confirmation check from HNP Carrier Add/Edit. It will be always enabled behind the scene. After upgrade all HNP carrier will have it enabled.
- Sender Name Description will not be suppressed for HNP Messages now.

Defects Fixed in this Release

- SNPP Two Way Old Messenger is crashing.
- [Time Stamp] Time Stamp is also included in HNP message if "user description as signature" is enabled in Global Settings and user checks Time Stamp check box on send panel.
- [User Description as Signature] "User Description as Signature" is truncated from a message if user also includes TIME STAMP in the message.
- [Receiver] On failure of primary carrier, message file is not jumped to the alternate carrier.
- [Carrier] On failure of primary carrier, message file is not jumped to the alternate carrier.
- If Confidential Mode is Disable from Global Settings then Confidential Message Dispatch Type field must not be shown in carriers.
- Secure Web Dispatch option must not be available for following carriers: OAI OAP SIP.
- [Upgrade][SIP Text One Way][SIP Text Two Way][OAI][OAP][CAP] SWD disabled carriers become SWD enabled carriers after upgrade from 4.7.1299 to 4.7.1355.
- Replace "Web Based Dispatch" with "Secure Web Dispatch" in Confidential Message Dispatch Type.
- Replace Normal with Allowed in Confidential Message Dispatch Type.
- Except SMTP Carrier, all carriers when set to Normal in Confidential Message Dispatch Type, then on edit the Confidential Message Dispatch Type becomes disabled.
- Except SMTP Carrier, all carriers when set to BLOCK in Confidential Message Dispatch Type, then on edit they are shown Secure Web Dispatch.
- [OAI]: Receiver PIN with decimal range of 0000-9999 is only allowed.
- [Send Panel]: Change the warning prompt when user switches to Confidential messaging mode.

Outstanding Defects in this Release

- [HNP Receiver] Message is NOT sent by alternate carrier if it fails to be delivered by Primary HNP carrier.
- Delivered: Read node is not sent to the device even the status is updated on server reports panel.
- [User Description as Signature] "User Description as Signature" is not appended in a message sent from HNP device to another receiver.
- [IE Utility] Facebook and twitter carriers are not exported using IE Utility.
- [Global Settings]: There must be an option that asks users to Allow or Block Confidential Mode in Global Settings Email Server Settings.

- [Global Settings]: Rephrase the Confidential Messaging warning prompt.
- Secure Icon filter (Lock Icon) must now also be shown if Confidential Mode is On in send Panel.
- If hnp receivers does not have message (alert or chat) view permissions on device, than the message is shown as delivered on reports panel.
- Device filter does not working for OAI and OAP receivers.
- [REST SAND BOX] The Confirm Message operation does NOT confirm / refuse a message
- [CLI] Message file is not getting created from Command prompt. (Because of ca-bundle.crt)
- hnp_users.log file replaced with the new one on HNP Manager service restart
- White space ping receiver count is not equal to hnp receivers active sessions, shown under HNP Manager Sessions tab
- [Hnp Manager] Permissions by downgrading a hnp activation key are not getting applied
- [SWD] Assigned Owner name is shown in 'From' field on hiplink session-less message view screen
- Detect and remove XMPP ghost connections in HNP manager.
- Secure Web Dispatch module needs to have a common same across all HipLink.
- [Quick Send]: Server must perform redundancy check on receivers PINS if messages are send from Quick Send panel or from HNP client.
- Default Confirm/Refuse response choices are not added into the secure web dispatch message if message is sent from HNP client without adding custom response choices.
- [HNP Manager] Carrier for text message is showing hnp carrier in drop down.
- Login page is possibly vulnerable to SQL Injection attacks.
- No message file is created on server for unregistered receivers if To field contain invalid receiver.
- Location URL does not shown as hyperlink on secure message web view.
- 2 High Alerts are shown for cross site scripting during ovs security scan .
- Add new line or space in web dispatch URL if advanced messaging is enabled in unsecure SNPP and WCTP receivers.
- [HNP Carrier] If "Complete on Confirmation" is not enabled then "Completion Timeout" field must shown disabled.
- [Global Settings]: Maximum Filtered queue size and Days in Filtered queue remains in edited mode when the settings are saved.
- Schedule messages displays the created time on device time, whereas it should display the current message sending time.
- Message Dispatch URL must be the part of Secure Web Dispatch functionality.
- [HNP Carrier]: "Complete on Confirmation" check does not remove on first try.
- HNP Manager crashes on sending message to multiple (i-e more than 20-25) receivers from device
- Crash page occurs after session timeout, if user switches between networks.
- [HNP Manager]: HNP Manager is taking more than a minute to remove Stale Connection.
- [Remote Administration]: Push Settings under Remote Administration are not working.
- [FT Manager]: File Transfer Manager service is available even if License Key does not support HNP Manager.
- [Recipient User]: Same Receiver can be set a Cover By of the same receiver.
- [Recipient User]: Voice Type Receiver must not be allowed to define Alternate Carrier and Voice Enable option.

- [Recipient User]: Some specific receivers give DB exception when they are assigned in Recipient User Device.
- If a Receiver is assigned in Recipient User Device List from admin panel then its Not Available schedule is not imported.

Contacting Customer Support

You can contact HipLink customer support at the following times and with the following methods:

Time	Monday through Friday 8:00 a.m. to 5:00 p.m. Pacific Standard Time (PST) Excluding U.S. holidays.
Email	support@hiplink.com
Phone	408-399-6120
Fax	408-395-5404
Customer Support Portal System	http://portal.hiplink.com

We recommend that you review the following documentation to become familiar with the product.

- Installation and Administration Guide
- User Guide
- Programmer's Guide

To open all guides, log on to the HipLink application through GUI. Click on "Help" button on the top right corner. It opens up a pop up window rendering the HipLink Help Index. Click on required link to open help guide.

Send Us Your Feedback

We always appreciate suggestions from our customers. If you have comments or suggestions about our product or documentation, send an email message to support@hiplink.com

Also visit our website www.hiplink.com for general information.