Release Notes
Polycom® Video Border Proxy (VBP™) VOS Version 9.1.5.3

9.1.5.3 | October 2010 | 3725-78301-003B

POLYCOM

Topics

3725-77600-001D7 (October 2009)
1765 West 121st Avenue
Westminster, CO 80234-2301 U.S.A.

Introducing the Polycom VBP System Version 9.1.5.3

This document describes the enhancements and fixes provided by the Polycom Video Border Proxy (VBP) VoIP Operating System (VOS), version 9.1.5.3. It includes all modifications made since VBP VOS version 7.2.2

What's New in the Polycom VBP System Version 9.1.5.3

The Polycom VBP system version 9.1.5.3 is a full all platforms release that resolves customer issues found in the field. This release also includes new features to the VBP-E, VBP-ST and Access Proxy but are not limited the following.

- VBP-E
  - Security – Whitelist/Blacklist added to the user interface
  - H.323 – Support for FACILITY messages
  - H.323 – The ability to change the Q.931 port
  - H.323 – Call Status – The ability to view active calls and disconnect calls
  - License key – The ability to disable the systems encryption applications – required for shipping into certain countries
  - License key – Support for 200Mbps of video on the 6400 platform only
- VBP-ST
  - H.323 – The ability to change the Q.931 port
  - H.323 – Call Status – The ability to view active calls and disconnect calls
  - H.460 – continuing to enhance multi vendor scenario's
  - Authentication – Support for TACACS
  - Security – Whitelist/Blacklist – this feature will be primarily used on the VBP-E system
  - License key – The ability to disable the systems encryption applications – required for shipping into certain countries
  - License key – Support for 200Mbps of video on the 6400 platform only
- Access Proxy
  - GUI – added new options to enable debugging
  - Added basic syslog support for client add/delete and Access Proxy start/stop
  - Continuing to enhance support for clients in complex NAT scenario's

Out of the Box Installation notes

When installing the VBP-E system for the first time, the systems DHCP server is enabled and serving out an IP address range of 192.168.1.150 – 192.168.1.199 to your computer dynamically. By default the systems DHCP server does NOT assign default DNS server information. After configuring the Network parameters e.g WAN IP Address, Default gateway, Primary and Secondary DNS servers the system will now assign these DNS server IP addresses to the DHCP server. If you're configuring the VBP system for a dynamic WAN type, check the DHCP server page after you have configured the Network parameters for the presence of DNS server IP addresses received from the provider's server.

For testing Internet connectivity you will need to renew your computers DHCP address to receive valid DNS server information. You can disable/enable your network adapter, disconnect and reconnect your Ethernet cable, or from a command prompt on a Windows OS type ipconfig -release then ipconfig -renew.

After you verify your computer now has valid Primary and Secondary DNS server IP addresses you will now be able to open a web browser and verify Internet browsing.

Interoperability

- Polycom CMA 4000/5000 server v4.01.02 or higher (see note)
- Polycom V and VSX Series v8.7.1 or higher
- Polycom ViewStation SP/MP/512/H.323 v7.5.4
- Polycom PVX v8.0.2 or higher
- Polycom ViewStation FX/EX/4000 v6.0.5
- Polycom HDX systems v2.0.3.1 or higher
- Polycom QDX 6000 (all versions)
- Polycom MGC v8.0.2 or higher
- Polycom RSS2000 v3.0.2 or higher
- Polycom RMX 2000 v3.0 or higher
- Polycom RMX 1000 (all versions)
- Polycom DMA 7000 v1.0 or higher

Note: The following issues, which may impact VBP functionality exists in CMA 4.01.02. These issues are addressed in CMA version 4.01.04

- Duplicate Aliases – When a CMA Desktop or HDX in VC2/dynamic mode moves from an internal CMA connection to an external VBP Access Proxy connection you might experience a scenario where the endpoint cannot connect to the CMA Server. An HDX endpoint is likely in this state if it displays an indicator stating that the gatekeeper service is down. A CMAD client is likely in this state if cannot progress beyond the "signing into the media server" message. In some cases, gracefully logging out of the internal location and waiting at least 10 minutes before an external login can reduce the chances of experiencing this issue.

- Dual Redundancy – When deploying 2 VBP systems and 2 CMA server's for what is called Dual Redundancy, if the MASTER CMA server fails, this forces the BACKUP CMA server to have control of all services, it is possible when this CMA failover happens, this CMA server may NOT send responses from the VIP (virtual IP) causing messages to be sent from the physical IP, the VBP is expecting messages to come from the VIP and will not be forwarded to the remote client. When deploying Single Redundancy 2 VBP systems and 1 CMA server, if the MASTER VBP fails, the BACKUP VBP will take over and function as expected.

Known Issues

- In VOS 9.1.5.3 the Polycom VBP-E series does not support the Access Proxy feature, although the feature is present in the GUI. VBP-E series platforms will support this feature in a future release. Access Proxy feature support is fully functional in the VBP-ST series.

- 5233 – ESCVIU-43 – Firewall - Management Interface - LAN side management still active – VBP-E only - There is a work around to this issue; When the system is configured to use the Management Interface on a different subnet than the WAN or LAN and you have all the management protocols unchecked, management from the WAN or LAN is still active. When you select or check all the management protocols and Submit the changes the system will now only respond on the Management subnet, WAN and LAN access will be dropped.

- H.460 – NAT router issue - When deploying H.460 device behind a 2 Wire NAT router calls will fail – there is no stable work around at this time for deploying a H.460 device behind a 2 Wire system that is running a factory default configuration. It may be possible to configure the 2 Wire NAT system which will allow the H.460 device to have successful calls. 4670 outlined below is an attempt at bypassing the 2 Wire ALG by assigning an alternate Q.931 port, however has not proven 100% successful at this time. 4670 has proven success in other scenarios where H.460 calls using the default TCP 1720 port where failing. Polycom engineering is continuing to investigate a solution for this issue.

- 5479 - VIU-183 – ViewStation FX and H.460 clients. With the FX and H.460 client registered to the same VBP-ST, one way media may occur in either direction.

Installation Recommendation

Platform	Upgrade Recommendation	Comment
All Platforms	All Platforms	This release will replace any Polycom hox fix version with a version string greater than 9.1.5.1. VBP-ST Access Proxy systems running version 9.1.5.1 should be updated. There are numerous fixes and enhancements to increase successful CMA Desktop or HDX deployments. VBP-E systems upgrade is also recommended This release includes an SSH daemon security update introduced in VOS 9.1.3.

New Features introduced in VOS 9.1.5.3

- 4699 - VIU-102 - Upgrade Firmware - Logging enhancement - The upgrade firmware page now displays more detailed error messages if an upgrade fails, e.g. Download Server DNS resolution failure, no route to host, connection refused, login failed, file permissions. Added download percentage display to the 5300, 5300LF, 6400, 6400LF, 6400LF2. The 200x, 4300, 4350x platforms already display the download percentage.

    - **Upgrade error: Could not connect to download server, no route to host**
    - **Upgrade error: Could not connect to download server, connection refused**
    - **Upgrade error: Could not connect to download server, network is unreachable**
    - **Upgrade error: Could not connect to download server, connection timed out**
    - **Upgrade error: Could not log in to download server, credentials incorrect**
    - **Upgrade error: Could not find file on download server, check the file name**
    - **Upgrade error: Was not allowed to download file, check server permissions**
    - **Upgrade error: Failed to resolve Download Server DNS name. Verify the Download Server DNS name and the DNS settings on the network page are valid.**

- 5279 - Disable Encryption - License Key - Added the ability to disable encryption based applications for shipping VBP platforms into countries that do not allow certain applications to be encrypted, e.g. PPtP, Site to Site VPN, Access Proxy. Encryption to the system for management is allowed and still enabled, e.g. HTTPS, SSH. When these applications are license key disabled the items are removed from the user interface.

- 5108 - Security – Whitelist/Blacklist - Added a user interface menu under VoIP ALG -- > H.323 -- > Whitelist/Blacklist. This feature allows the user to create IPv4 firewall rules to allow or deny specific source IP address or subnets from creating TCP port 1720 call SETUP connections to the VBP. This feature has been added to the VBP-E and VBP-ST platform, the feature will have more useful functionality on the VBP-E platform for allowing or blocking calls from remote H.323 systems. The feature is also enabled on the VBP-ST platform.

- 1463 – ESCVIU-27 – H.323 – Support for FACILITY messages – The VBP will now responds to FACILITY messages to redirect a call setup, i.e. routeCallToGatekeeper, routeCallToMC, and callForwarded. The system also translates the H.245 address for FACILTY messages with reason startH245.

    - 5297 - Alias Manipulation - When the VBP-E system is configured as LAN-side gatekeeper mode and the CMA is set to use this VBP-E system as its SBC/ALG. When a user dials an IPv4 address to the destination system the CMA inserts an @ character i.e. @1.1.1.1. The insertion of the @ symbol was introduced by the gatekeeper team to work around the issue described in Bug: 4765. With this issue resolved the gatekeeper team can now remove this dependency in future gatekeeper releases. With the new support for FACILITY messages as described in 1463 – ESCVIU-27 the below rules to remove the @ symbol from the redirected SETUP message is needed in certain cases for the destination system to route the call correctly.

      When calling a system that supports FACILITY redirects, the VBP redirects the SETUP as destinationAddress - url-id: h323: @1.1.1.1 some systems won't route the call correctly to the destination with this string.

      Adding the following Alias Manipulation rules to remove this symbol solves this issue in the FACILITY redirect scenario;

      ^@
      ^h323:@

      These rules will not be inserted on system upgrades, you will need to enter them manually. The rules will be present for new shipping systems or performing a factory default.

      The help file on the Alias Manipulation page was update to include these new expressions.

- 4794 – EXT-2715 - TACACS support on the VBP-ST platform - TACACS is now enabled on the VBP-ST platform. TACACS authentication will be preformed on all management protocol to the system, if the remote TACACS server is unavailable the system will authenticate with the local system credentials.

- 4670 - ALG – H.323 – Alternate Q.931 port – Added the ability to change the Q.931 listening port of the system from the standard TCP port 1720 to a non-standard port. This feature was added to help work around SoHo NAT devices that either block this standard port, or manipulate the Layer 5 headers that can cause the call SETUP to fail. During this feature testing in proof of concept trials in the field it has proven to help solve CMA Desktop connectivity related issues. When setting this port it will change it for all users on the system. No modifications are needed on the H.323 client. The alternate Q.931 port will be assigned to the calling client in the ACF message when using a VBP-ST platform. This field is also present on the VBP-E platform. When changing the VBP-ST or VBP-E platforms to use a non-standard Q.931 port, the system will listen and respond to Q.931 setup requests on the GUI configured Q.931 port and the standard well known 1720 port.

When changing the Q.931 port on the VBP-ST platform to solve a remote CMA Desktop's connection issues behind a NAT router you may try a few well known ports e.g. 80, 110, 25, 21, 20. If you are planning to use port 80 for the Q.931 port, you must reassign the HTTP port for managing the VBP. If you have not reassigned the HTTP port on the Firewall page for management and assign port 80 as the Q.931 port and click Submit to save the changes the system will warn you;

Error: Port 80 is currently used by the Web management GUI and cannot be used as the Q.931 port. You can remap the HTTP port on the Firewall Page

When changing the Q.931 Port on either platform the active registered clients in the systems H.323 Clients List will be removed, you will need to wait for the clients to re-register before making test calls. If you are testing this feature on a VBP-ST platform with H.460 enabled the H.323/H.460 remote client will reregister to the system as half the period of the configured Keep-Alive Time (s) value. The default time of 45 (s) will cause the remote client to re-register in approx 22 (s). The H.323 clients list may not display the client for up to a minute even though the remote client reports that it is registered. If the remote client reports it is registered calls will now be possible using the new Q.931 port.

The default setting on a VBP-E system registered client can take up to 300 seconds or 5 minutes to re-register.

- 4996 – Access Proxy - Added Access Proxy client add and delete syslog messages without the need to enable any debug options on the system. This feature will be useful in diagnosing Access Proxy client issues when configuring the system for external syslog under the Services Configuration page setting Enable Remote System Logging. Local syslog files are limited to 2 x 32k files that wrap in a circular manner in the /var/log/ directory, messages and messages.old.

- 4995 – Access Proxy - Added Access Proxy start and stop syslog messages without the need to enable any debug options on the system. This feature will be useful in diagnosing Access Proxy issues when configuring the system for external syslog under the Services Configuration page setting Enable Remote System Logging. Local syslog files are limited to 2 x 32k files that wrap in a circular manner in the /var/log/ directory, messages and messages.old.

- 3880 – License Key – 200Mbps – Added the ability to support up to 200Mbps of video on the 6400 platform only.

- 4227 – VIU-97 – GUI – Call Status – The VBP-E and VBP-ST systems now have a new GUI menu under Voip ALG -- > H.323 to view active calls, details about the call and the ability to disconnect the call.

Help

H.323 Call Status

Current time: **Wed Jul 28 18:03:02 2010**
Current payload bandwidth: **256**
Estimated total bandwidth: **320**

The H.323 call status shows currently ongoing H.323 calls.

Refresh Status

H.323 Call Status

Start-Time	Source	Destination
Jul 28 18:02:40	**8885** 192.168.1.50:5557	**5551000@12.48.270.1** **12.48.270.1**:1720
Terminate Call	Duration: 0:00:22 Bandwidth: 256 kbps Route Decision: AnnexO style alias Call-Status: H.245 signaling received and forwarded	

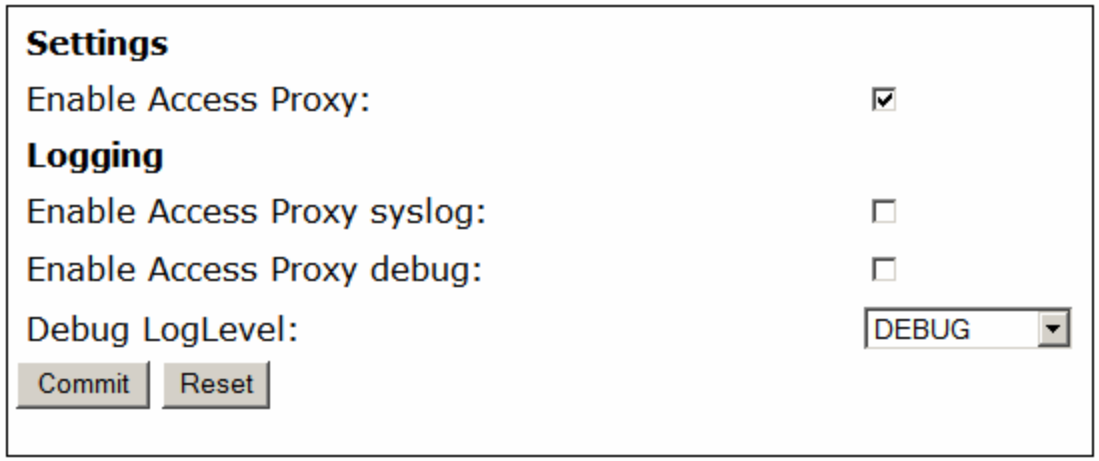
Fixes and Enhancements in VOS 9.1.5.3

- 4596 – Access Proxy – Continuing to enhance the support for multiple clients that are installed behind SoHo or enterprise NAT devices. Issues have been found in the field in previous versions that cause the Access Proxy to not correctly track clients that are installed behind devices that can NAT a single client as multiple IPv4 addresses and may cause the client to display “Can’t connect to Presence server” Added syslog message for deleting client when iptables rules are not added.
    - 5530 – Modification made to the access proxies add client, delete client and the clients list clean up process which allows the mobile user to switch network interfaces immediately without experiencing re-authentication issues.
- 4599 – AccessProxy - Logging enhancement - Access Proxy now has a GUI item to enable debug messages for advanced troubleshooting.

  The output of this debug will be only accessible from the CLI interface in the /var/log/ directory as accessproxy.log which is the active file, when this file reaches a 250K size it will be rotated to accessproxy.log.1. The logs will continue to rotate up to accessproxy.log.7 and then be rotated out and non recoverable. Depending on the log level selected and the amount of users trying to connect these logs can fill up and rotate within 1min.

  Added basic Access Proxy message decode to syslog; this feature will provide some information to help solve connection related issues. By enabling Access Proxy syslog the system will send limited messages to the systems logging application; you can access these files on the CLI in the /var/log directory as messages and messages.old. Local syslog files are limited to 32k. If you wish to capture syslog on a remote syslog server configure the Remote Syslog Host and Enable Remote System Logging in the Service Configuration page on the GUI.

  Added help text for new logging options.



- 5291- H.323 – Embedded Gatekeeper – VBP-E replies with LCF for an alias it does not know This was a side effect of feature request 4765. We now do not attempt to do a DNS lookup on an alias in an LRQ.

- 4409 – Network - DHCP WAN type – When the WAN type was set to DHCP and the network DHCP server replied with an Infinite IP address lease time the DHCP client daemon would exit. The DHCP client daemon was configured to restart if the application exited; this caused the system to continually restart. The DHCP client exiting behavior is correct when receiving an Infinite lease time, the system now will not attempt to restart if the network DHCP server sends an Infinite lease time.

- 5234 -H.323 - H.460.19 not working when NAT device in the path rewrites H.245 messages. Modified the H.460.19 logic to create symmetric RTP streams which avoids the NAT device rewriting the OLCAck port numbers. This issue can cause H.460 devices installed behind some NAT devices to receive RTP media “sometimes”. This intermittent issue was observed in endpoints behind Netgear NAT devices (WGR614v9 – firmware V1.2.2_14.0.13NA) with no replication pattern.

- 4998 – Access Proxy - Firewall is required to be enabled before enabling the Access Proxy. The Access Proxy secures the application through firewall rules and therefore the firewall must be enabled. This issue was found in the field that some customers didn’t enable the firewall and remote clients could not log into the system. The Access Proxy will not start if the firewall is not enabled and will warn the user to enable the Firewall.

- 4283 – Route page - Removed the 20 route entry limitation. The new limitation is 75 entries.

- 4328 – ESCVIU-26 - Tandberg interoperability - Inbound calls with DST H323-ID sent with user@VBP_WAN_IP failed in LAN/Subscriber-side gatekeeper mode or Peering-Proxy mode. There is an existing work around by adding an Alias Manipulation rule to strip @VBP_WAN_IP. The system did parse this message correctly in Embedded Gatekeeper mode. The system previously only stripped the '@OUR_WAN_IP' part for the internal call routing logic. The system now removes this from the actual SETUP message as well before forwarding to the LAN side device.

- 4765 – H.323 – Embedded Gatekeeper mode - ARQ message handling – The VBP now attempts to resolve an FQDN even if no @ sign is present in the alias. This issue was present if the user dialed e.g. hd.polycom.com as a DNS name, the system attempted to look for a registered H.323-ID alias and then failed the call. The system now attempts to resolve the string as a H.323 alias, if no alias is found, attempt a SRV h323cs lookup, then A record lookup.

- 3918 – Access Proxy – Help file change - Committed new help text.

- 4309 – ESCVIU-24 – NAT – In previous VOS versions it was possible to enter duplicate entries. The system now verifies the protocol, source port, and WAN IP when checking for duplicate entries. If these 3 fields match an existing entry, the new entry is not added and the following warning message is displayed

    - **The source already exists.**

- 4718 - GUI - User Commands page - Edgewater KB reference – Modified Help page language.

- 4745 - GUI - SIP page - Help file - language change - remove or replaced references to EdgeMarc and EdgeProtect with VBP-E and VBP-ST.

- 4955 - DHCP Server – Disabled the DHCP server on VBP-ST platforms. The DHCP server is now always disabled on VBP-ST platforms.

- 4937 – ESCVIU-40 -H323 - Codian MCU dialing IP only – When configuring the VBP-E system with a default alias the inbound call did not route correctly. When the Codian MCU dialed the VBP with a IP only the Codian would configure a destination alias as a transported with the WAN IP of the dialed VBP IP address. The VBP default alias logic saw this as a valid alias and did not route the call correctly. A work around is available by dialing user@VBP_WAN_IP. The VBP now checks whether it understands the destinationAddresses passed in the Setup, If it does understand them, it leaves them alone, otherwise it removes them and adds a default alias.

- 4418 – ESCVIU-29 - NAT page - Wording change Fixed – The wording read “For static NAT to function, WAN NAT must be enabled” the changed language is now “For static NAT to function, LAN NAT must be enabled

- 4718 - GUI - User Commands page - Edgewater KB reference.

- 4775 – Access Proxy – Removed a system call which caused the Access Proxy not to start after factory default. This issue was only present in an intermediate Polycom hot fix, version 9.1.5.1 did not have this issue.

- 4679 - H.323 – call looping caused the ALG to exit – In certain calling cases when the called endpoints SETUP message is looped back to the same VBP-ST the ALG will exit and restart. This exit was due to a second H.225 connection being received with the same Call-ID as the previous call. We now detect and prevent these loops. An example of this is; when a call is received on a CMA Desktop client from the system and the call completes and the call ends, the receiving client now selects the recent call history and redials the previous call, the CMA Desktop client stores the VBP-ST IP address that its registered to as the last received call. When the user dials this IP address the CMA server can route this call to a VBP-E system that provides off net dialing for the enterprise. The VBP-E system now routes this call back to the VBP-ST and creates a call loop.

Introducing the Polycom VBP System Version 9.1.5.2

This document describes the enhancements and fixes provided by the Polycom Video Border Proxy (VBP) VoIP Operating System (VOS), version 9.1.5.2. It includes all modifications made since VBP VOS version 7.2.2

What's New in the Polycom VBP System Version 9.1.5.2

The Polycom VBP system version 9.1.5.2 is primarily a maintenance release too include the new 200E hardware to the VBP product family. This VBP release support's all legacy H.323 video scenario's and adds support for SIP audio. For more information on SIP audio supported scenarios visit the Polycom Support web site for the configuration guide.

Out of the Box Installation notes

When installing the VBP-E system for the first time, the systems DHCP server is enabled and serving out an IP address range of 192.168.1.150 – 192.168.1.199 to your computer dynamically. By default the systems DHCP server does NOT assign default DNS server information. After configuring the Network parameters e.g WAN IP Address, Default gateway, Primary and Secondary DNS servers the system will now assign these DNS server IP addresses to the DHCP server. If you're configuring the VBP system for a dynamic WAN type, check the DHCP server page after you have configured the Network parameters for the presence of DNS server IP addresses received from the provider's server.

For testing Internet connectivity you will need to renew your computers DHCP address to receive valid DNS server information. You can disable/enable your network adapter, disconnect and reconnect your Ethernet cable, or from a command prompt on a Windows OS type ipconfig -release then ipconfig -renew.

After you verify your computer now has valid Primary and Secondary DNS server IP addresses you will now be able to open a web browser and verify Internet browsing.

Interoperability

- Polycom CMA 4000/5000 server v4.01.02 or higher (see note)
- Polycom V and VSX Series v8.7.1 or higher
- Polycom ViewStation SP/MP/512/H.323 v7.5.4
- Polycom PVX v8.0.2 or higher
- Polycom ViewStation FX/EX/4000 v6.0.5
- Polycom HDX systems v2.0.3.1 or higher
- Polycom QDX 6000 (all versions)
- Polycom MGC v8.0.2 or higher
- Polycom RSS2000 v3.0.2 or higher
- Polycom RMX 2000 v3.0 or higher
- Polycom RMX 1000 (all versions)
- Polycom DMA 7000 v1.0 or higher

Note: The following issues, which may impact VBP functionality exist in CMA 4.01.02. These issues are addressed in CMA version 4.01.04

- Duplicate Aliases – When a CMAD or HDX in VC2 mode moves from an internal CMA connection to an external VBP Access Proxy connection you might experience a scenario where the endpoint cannot connect to the CMA Server. An HDX endpoint is likely in this state if it displays an indicator stating that the gatekeeper service is down. A CMAD client is likely in this state if cannot progress beyond the “signing into the media server” message. In some cases, gracefully logging out of the internal location and waiting at least 10 minutes before an external login can reduce the chances of experiencing this issue.

- Dual Redundancy – When deploying 2 VBP’s and 2 CMA server’s for what is called “Dual Redundancy” if the MASTER CMA server fails, this forces the BACKUP CMA server to have control of all services, it is possible when this CMA failover happens, this CMA server may NOT send responses from the VIP (virtual IP) causing messages to be sent from the physical IP, the VBP is expecting messages to come from the VIP and will not be forwarded to the remote client. When deploying “Single Redundancy” 2 VBP’s and 1 CMA server, If the MASTER VBP fails, the BACKUP VBP will take over and function as expected.

Known Issues

- In VOS 9.1.5.2 the Polycom VBP-E series does not support the Access Proxy feature, although the feature is present in the GUI. VBP-E series platforms will support this feature in a future release. Access Proxy feature support is fully functional in the VBP-ST series.

- 1463 – ESCVIU-27 – Facility messages are now supported on the VBP-E platforms

New Features introduced in VOS 9.1.5.2

- 200E hardware platform introduced in VOS 9.1.5.2

Fixes and Enhancements in VOS 9.1.5.2

- 3546 - Added 200E hardware ID support
- 4213 - VIU-94 - Access Proxy - NTLM string longer than 512 is not being forwarded: Increased buffer size to 2048 to handle longer NTLM authorization messages. This issue was found after the production release of 9.1.5.1, some Windows system platforms received service updates to their NTLM libraries which caused the NTLM authorization string to be longer that 512.
- 4314 – ESCVIU-25 – Gatekeeper neighboring in LAN/Subscriber-side gatekeeper mode with a CMA gatekeeper – When gatekeeper neighboring to a providers network for ISDN offnet dialing, the providers gatekeeper was re-writing the destination alias in the LCF, when the call SETUP arrived with this modified alias the VBP's ALG did not track the original LRQ and modified LCF correctly resulting in a ALG restart. Bug 4320 was also addressed as a direct cause on Bug 4314 – an incorrect source port was assigned as port 0 for transparent LCF responses.
- 3598 – SIP – The system by default is configured with a SIP Server of 0.0.0.0, after an unknown time period the ALG will restart.
- 4690 – Access Proxy – Change the default session timer to 30 mins from 60 mins. This timer is used to clean up Access Proxt clients that have disconnected from the system without logging out.
- 4689 – VIU-101 – Access Proxy – Authorizations for clients using Network credentials or cached network credentials could not login. The Access Proxy was not updating the content length of the authorization fields be forwarded to CMA. The CMA server was rejecting the authorization as a bad request.
- 4599 – Access Proxy – Logging cleanup
- 4596 – Access Proxy – Supporting multiple clients behind a SoHo NAT device was not functioning correctly. The client tracking logic only allowed for 1 device behind a SoHo NAT, when this device logged out the remaining clients experienced a loss of Presence and LDAP directory services.
- 4600 – Access Proxy – Configuration file cleanup.

- 2874 – Access Proxy – Access Proxy configuration files not saved with the “ewn save” command – accessproxies.conf and accessproxy.conf now saved correctly.

- 2961 – Access Proxy – Access Proxy UI configuration allowed a duplicate “Subscriber port” to be configured.

New Features introduced in VOS 9.1.5.1

- None

Fixes and Enhancements in VOS 9.1.5.1

- 4074: Log rotation fix for iptables logging - log rotation capability has also been added to Access Proxy, the system will now have 8, 250K ap-iptables.log files located in /var/log that track the dynamic “add” or “delete” firewall rules for authenticated VC2 based endpoints. This file also tracks VC2 endpoints that have become unavailable that indicates they have been “deleted”.
    - ap-iptables.log
    - ap-iptables.log.1
    - ap-iptables.log.2
    - ap-iptables.log.3
    - ap-iptables.log.4
    - ap-iptables.log.5
    - ap-iptables.log.5
    - ap-iptables.log.6
    - ap-iptables.log.7

- 4075: Fixed accessproxyrc startup problem with multi cores, 6400, 6400LF, 6400LF2

New Features introduced in VOS 9.1.5

- Copied key/cert to /usr/local/ssl/certs
- Access Proxy
    - Added support for HDX. Changed handling of the incoming authentication message from the HDX client.
- Allow LAN side E/P's to dial ANNEX O If an incoming call used an AnnexO dialing string where the IP address was the address of the system itself, we would not forward the call. Now we strip of the IP address from the alias if it is matching the address of the system itself, and completes the call using the alias part of the AnnexO string.

Fixes and Enhancements in VOS 9.1.5

- 2298 - Annex-O LAN->LAN calls are GK routed.
- 3883 - VBP incorrectly assigning RTP ports We now attempt to match the RTP forwarding entries according to the signaled session IDs so that the forward and reverse stream gets the same port number.
- 3857 - Access Proxy - Enable Logging. Default Access Proxy.conf file has been copied to /etc/default/ for reference. Additional enhancements to the log messages to provide before information.
- 3858 - Access Proxy - Added Log Level support. Access proxy can now print out logs of varying levels by modifying /etc/config/Access Proxy.conf. Update LOG_LEVEL with either LVL_INF, LVL_DBG, LVL_DAT.
- 3867 - Access Proxy - HTTPS access to the system on alternate port. Firewall rules in config_ep_fw.sh and config_em_fw.sh have been updated. Text/Warnings has also been updated on the Firewall page, HTTPS Certificate page and the Access Proxy page.
- 3873 - Access Proxy - VRRP Support. Access proxy will start via /etc/Access Proxyrc if VRRP is enabled and is in MASTER state. Access Proxy will self-terminate if the state changes to BACKUP.
- 3873 - Access Proxy - VRRP Support. Modified config_vrrp.sh to insert the appropriate allow iptables rules when the system is running in VBP-ST mode.
- 3859 - In Embedded Gatekeeper mode, not all the aliases are display this limitation has been removed.
- Message of the Day" configured or not; a longer than 8 characters password will now be rejected.
- 3929 - bandwidth tracking problem for h.460 nat'd endpoint initiated calls, this is a result of the fix for bug 2217 and is now resolved.

New Features introduced in VOS 9.1.4

- Access Proxy Secure ALG functionality: In secure mode, the Access Proxy will have the following functionality:
  - Automatic AdapterProbe message response.
  - Automatic UpdateCheck message response with xml: <appUpdate>NONE</appUpdate>
  - Default iptables rule for blocking ALL traffic to XMPP (5222) and LDAP (389) ports.
  - Authentication message validation.
  - Dynamic addition / deletion of iptables access rule per user based on authentication 200OK response from CMA Server.
  - Addition of internal client list for tracking client access.
  - Log out handling → removes client from internal ap-client.list, iptables access rule removal.
  - Heartbeat handling → updates the session time for client in internal list.
  - Session time expiration handling (60 minutes) → Removes expired clients from the list and iptables.
  - Access Proxy now runs in Secure mode as a default.
  - Debug log rotation capability has also been added to Access Proxy, the system will now have 8, 250K accessproxy.log files located in /var/log note: debug is NOT enabled by default and must be enabled in the /etc/config/accessproxy.conf file please contact Polycom technical services for the correct instructions
    - accessproxy.log
    - accessproxy.log.1
    - accessproxy.log.2
    - accessproxy.log.3
    - accessproxy.log.4
    - accessproxy.log.5
    - accessproxy.log.6
    - accessproxy.log.7

- Bug 4383 Added the option "Supports Additive RRQ" in the RCF response from our embedded GK. This should allow our downstream VBP-ST to register more than 25 endpoints.

Fixes and Enhancements in VOS 9.1.4

- 3483 - Added the option "Supports Additive RRQ" in the RCF response from our embedded GK. This should allow our downstream VBP-ST to register more than 25 endpoints.
- 3053 - Inconsistent GUI password login length when you have "HTTP Short System Message" The behavior is now the same whether there is a "Short System Authorization

- 2542 - "?" is not allowed as the first character in the password It is now possible to use "?" in GUI passwords, as the first character or any other character.

New Features introduced in VOS 9.1.3

- Access Proxy functionality was added to the VBP-ST system which can be accessed through the menu. In addition, you will also see the “Access Proxy” configuration on the VBP-E series appliances, the feature is not fully supported on the E series system in this version, please do not attempt to configure this feature in this version. The E series Access Proxy feature will be supported in a future Polycom VBP VOS version.
- Security update: Upgrading openssh-4.0p1 to openssh-5.1p1

Fixes and Enhancements in VOS 9.1.3

- Enhancement: Polycom private / public security keys were added to ST and E models.
- 3426 - When HTTPS management is enabled, an attempt to add an HTTPS proxy server will now result in a message instructing the user to disable the HTTPS management from the Firewall page. If after the addition of the HTTPS proxy server, the HTTPS management is enabled, a message stating that HTTPS proxy and HTTPS management will be using different ports will be displayed.
- 3293 - NAT GUI: leading and/or trailing spaces in the port fields cause SNAT rule to not be applied in iptables. Leading and trailing spaces in the port fields caused parsing problems in the scripts. When saving the NAT rule, spaces are now stripped out of the rule before it is saved.
- 3257 - Re-enable MPPE support in kernel for PPTP server.

New Features introduced in VOS 8.11.1

- 6400LF2 platform was introduced in VOS 8.11.1

Fixes and Enhancements in VOS 8.11.1

- 0899: “Erase” button did not function on 5300LF. The button now works the same as on all the other devices which is as follows:
  - Pressed once: Nothing happens.
  - Pressed twice: The CLI password is reset.
  - Pressed three times: The device is set to the factory defaults
- 3191 - Default gateway was not being set on the subscriber eth0 interface of “ST” devices.
- 2929 - Removed Test UA from GUI.
- 3546 - VBP system reports a 200AW hardware type but actual hardware is a 200EW, the issue is now resolved.
- 3012 - ALG crashes with a LifeSize Express endpoint places call, the issue is now resolved.

New Features introduce in VOS 8.9.1

- Support for VBP 200EW and VBP 4350W was added.
- DHCP options 67 (boot file), 150, 151, 159, & 160 were added to DHCP GUI page for better interoperability with Polycom phones.
- H.323 activity log is now written to a separate log file with a maximum of 25 entries and with newer entries on top of the file. This prevents the H.323 activity log from being overwritten by other syslog activity.
- Added more feedback and controls to the upgrade page. Added a checkbox that displays the output from the upgrade command. Added the platform name to the upgrade page. Added a checkbox to enable/disable the FTP server ping check. Improved error feedback when an upgrade fails.
- Message of the Day (MOTD) is now displayed on VBP-ST systems.
- Feature/Bugfix: Improved reliability of VRRP. Numerous fixes: + Re-applied patches for multiple race-conditions. + Modified VRRP to only advertise on LAN link. WAN link status is still monitored but only the LAN has advertisements. This should prevent ping-ponging of state due to conflicting advertisements on different links. + Re-enabled revertive mode and made it user configurable. + Modified keepalived's script notification to be synchronous to fix a state issue race condition + Added VRRP state check in ALG causing ALG to self-terminate if we're in backup mode to prevent a situation where ALG is running even though we're in backup mode. + Increased default advertisement interval to 3 seconds to prevent VRRP state from going from FAULT to BACKUP to MASTER when recovering from a fault.

Fixes and Enhancements in VOS 8.9.1

- Enhancement: Capability was added to function in a router only mode.
- 2832 - PPoE was not coming up on WAN after the execution of “ewn load” command. This problem is now fixed.
- 2558 - Multicast gatekeeper requests were not being answered by VBP. This problem is now fixed.
- 2733 - LAN to LAN call using prefix routing was failing. This problem is now fixed.
- 2560 - VBP was not forwarding LRQ on the WAN side. This problem is now fixed.
- Bug fix: ALG was failing if a call came on a shared call appearance phone. This problem is now fixed.
- 2806 - All references to V2IU were converted to VBP in 200 and 4350 series.
- 2810 - SIP UA and GW were removed from 200 series GUI. Test UA, however, has not been removed since no analog ports are needed to run Test UA.
- 2808 - (200 Platform) A video call would terminate by itself after a certain amount of time.
- 2582 - One way audio was observed on certain H.460 endpoints. This problem is now fixed.
- 2267 - Q.931 was not being blocked when H.323 was enabled. TCP port 1720 is now blocked by firewall when H.323 is enabled which blocks Q.931 traffic.

- Bug - H.323 - Transparent LRQ in LAN GK mode was not working.
- Bug - ALG was failing while receiving an incoming WAN call in LAN side gatekeeper mode. This problem is now fixed.
- 1288 - H.460.18 traversal was not working when used with a RadVision GK and a Tandberg endpoint.
- Bug - ALG was failing when endpoints were registering with multiple aliases containing the same string.
- Bug - SIP stale RTP deletion feature was incorrectly deleting active H.323 calls which would cause ALG to malfunction.
- 2217 - LAN side prefix routing is counting bandwidth, the issue is now resolved.
- 2496 - Removed the Route GUI page and renamed the VoIP subnet routing page to Route. VoIP subnet routes are not limited to the ALG so the two pages were redundant.
- 140 - ADSL-PPPoE is displayed in the GUI for the following platforms 5300, 5300LF, 6400, 6400LF, 6400LF2, this is not a support WAN type for these platforms. Removed ADSL-PPPoE network option from the 5300, 5300LF, 6400, 6400LF, and 6400LF2.
- 1848 - 6400 and 6400LF does not have HTTPS as an option in the GUI. Added support for HTTPS on 6400, 6400LF. Added of the certificate link and the HTTPS firewall check box for these platforms.

Upgrade Instructions

This version of software is available on the Polycom Support FTP site: ftp.support.polycom.com

It is recommended you reboot the Polycom VBP Series appliance prior to doing the upgrade. This will ensure there is enough dynamic memory available to handle the upgrade process.

When you update your software all services will be unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when VoIP traffic can be interrupted.

Upgrade procedure

1) Use a web browser to connect to the **VBP** appliance.
2) Click on the **Upgrade firmware** link. Use the page defaults.
3) Press **Submit**.
4) Follow the progress of the upgrade using the "refresh the upgrade status" link.
5) When the Write process begins, please heed the warning:

WARNING!!! Do not change the configuration or power off the device until the write is 100 percent complete. The device may become unusable if the write is interrupted.

6) The system will automatically restart after the new image has been loaded. After the upgrade process has completed, check that the new version number is displayed on the main System page.

Obtaining Further Assistance

Please contact the Polycom Technical Services for assistance.